ICAEW KNOW-HOW
AUDIT AND ASSURANCE FACULTY

Assurance reports on internal controls of service organisations made available to third parties

TECHNICAL RELEASE 01/20 AAF

icaew.com/auditandassurance

The ICAEW Audit and Assurance Faculty is the professional and public interest voice of audit and assurance matters for ICAEW and is a leading authority in its field. Internationally recognised as a source of expertise, the Faculty is responsible for submissions to regulators and standard setters and provides a range of resources to professionals, providing practical assistance in dealing with common audit and assurance issues.

There are over 1.8m chartered accountants and students around the world – talented, ethical and committed professionals who use their expertise to ensure we have a successful and sustainable future. Over 181,500 of these are ICAEW Chartered Accountants and students. We train, develop and support each one of them so that they have the knowledge and values to help build local and global economies that are sustainable, accountable and fair. We've been at the heart of the accountancy profession since we were founded in 1880 to ensure trust in business. We share our knowledge and insight with governments, regulators and business leaders worldwide as we believe accountancy is a force for positive economic change across the world.

Contents

1. Introduction

ASSURANCE ON CONTROLS OPERATED BY A THIRD PARTY

1. Many entities ('User Entities') outsource aspects of their business activities to third party organisations that provide services ('Service Organisations'). These activities range from performing a specific task under the direction of the User Entity to replacing entire business units or functions. The activities outsourced are often integral to the User Entity's business operations and, where they affect the User Entity's financial statements, the User Entity's external auditor may be required to understand and test controls over those outsourced business activities, particularly where they involve the processing of financial transactions.

2. AAF 01/20 has been developed to enable the Service Organisation to engage an independent practitioner (the 'Service Auditor') to provide an assurance opinion over the relevant controls which seek to manage risks on behalf of User Entities. The assurance opinion can then be made available to User Entities and their external auditors ('User Organisations'), avoiding the need for several different User Organisations to test the same controls.

3. It is for those charged with governance of the Service Organisation (the 'Senior Management') to decide whether to prepare a report on their organisation's internal controls and whether to have this reported on by a Service Auditor. In certain circumstances, Senior Management may, for example, consider it more appropriate to allow access to User Organisations or to provide a report on a specific aspect of their operations as this impacts an individual User Entity. This guidance does not require Service Organisations to report on internal controls in the manner described. However, if Senior Management decide to provide a report other than in accordance with this guidance, they may not make any reference to this guidance in that report.

SCOPE

4. AAF 01/20 provides generic guidance to a Service Auditor reporting on specific services performed by the Service Organisation (the 'Subject Matter'). It is also intended to provide high-level guidance to Senior Management who prepare the report on the Subject Matter, as it clarifies their responsibilities.

5. AAF 01/20 is also expected to help User Organisations to understand the scope and type of assurance provided in the Service Auditor's Report.

6. The demand for Service Organisations to report on their internal controls to User Entities originated in the asset management sector, where this type of reporting continues to be prevalent. This guidance includes a minimum set of benchmarks against which the Subject Matter can be assessed (the 'Criteria') for the following activities:

   a) Custody;
   b) Fiduciary management;
   c) Fund accounting;
   d) Investment management;
   e) Investment administration;
   f) Pension administration;
   g) Private equity;
   h) Property investment management;
   i) Property investment administration;
   j) Transfer agency; and
   k) Information Technology (IT).

7. Where the need for reports on internal controls has extended beyond these activities, this guidance can be applied. However, it is the responsibility of the Service Organisation to determine appropriate Criteria, based on their understanding of the relevant industry.

8. Where Senior Management decide to prepare a report on the relevant internal controls, it is of greater benefit to User Organisations if it covers internal controls in operation throughout a given period of time (a 'Type 2 report')[1], and the guidance that follows generally assumes that the report covers a period. However, a report on internal controls at a single point in time (a 'Type 1 report')[2] may be an alternative where a Service Organisation is preparing its report on internal controls for the first time. A repeat Type 1 report is expected to be unusual and would generally only be provided to User Entities if there have been significant changes to the control environment or if the Service Organisation has considered the needs of User Entities and concluded that they only require a Type 1 report.

INTERNATIONAL FRAMEWORK

9. This guidance follows the framework for assurance engagements set out in the IAASB Assurance Framework and International Standard on Assurance Engagements (ISAE) 3000 (Revised) *Assurance Engagements other than Audits or Reviews of Historical Financial Information*, published by the IAASB. The IAASB Assurance Framework defines the elements of assurance engagements and describes the objectives for such engagements. ISAE 3000 (Revised) provides generic guidance on the principal aspects of assurance engagements.

10. Compliance with ISAE 3000 (Revised) requires, among other things, the Service Auditor to comply with the International Federation of Accountants' International Code of Ethics for Professional Accountants (the 'IFAC Code'), and implement quality control procedures that are applicable to the individual assurance engagement.

11. AAF 01/20 is intended to be compatible with ISAE 3402 *Assurance Reports on Controls at a Service Organization*.

TRANSITION FROM AAF 01/06

12. AAF 01/20 replaces AAF 01/06 and is effective for periods beginning on or after 1 July 2020. Early adoption of this guidance is encouraged.

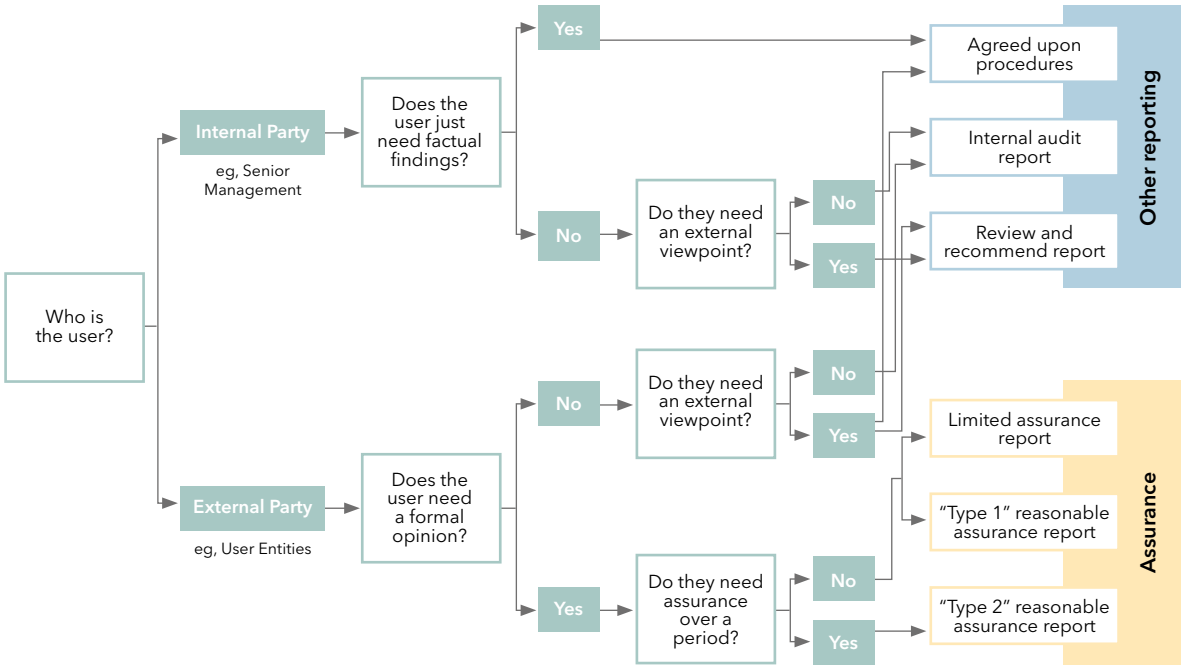
[1] See Part 2 of this document for more information on Type 2 reports.

[2] See Part 2 of this document for more information on Type 1 reports.

2. Assurance engagements

13. In an assurance engagement, a Service Auditor expresses an opinion designed to enhance the degree of confidence of the intended User Entities over the Subject Matter performed by the Responsible Party, eg, the Service Organisation, by reference to certain Criteria.

14. There are a number of options for assurance or other reporting engagements. The choice is mainly driven by the needs of the users – ie, the degree to which the user of the report will draw their own conclusion or rely on a report. The decision drivers for different types of assurance or other reporting engagements are set out in the diagram below:



15. Other reporting engagements include:
    - Agreed upon procedures;
    - Internal audit report; and
    - Review and recommend report.

16. For such other reporting engagements, no formal assurance opinion is being issued by a Service Auditor.

17. Assurance engagements comprise:
    - Limited assurance report;
    - 'Type 1' reasonable assurance report; and
    - 'Type 2' reasonable assurance report.

18. In a limited assurance engagement, the Service Auditor expresses an opinion stating whether they have identified anything that contradicts or disproves the existence and/or operation of the Subject Matter outlined in the report.

19. In a reasonable assurance engagement, the Service Auditor seeks to obtain sufficient appropriate evidence that enables them to express a positive opinion on the existence and/or operation of the Subject Matter outlined in the report.

20. The principal difference between a reasonable assurance engagement and a limited assurance engagement is the weight of evidence required to support the opinion of the Service Auditor (and hence the level of assurance that is provided). For a limited assurance engagement the Service Auditor collects less evidence than for a reasonable assurance engagement. The Service Auditor achieves this ordinarily by performing different or fewer tests than those required for reasonable assurance or using smaller sample sizes for the tests performed. For example, the opinion in a limited assurance engagement may be: 'Based on the procedures performed, nothing came to our attention to indicate that the management assertion on XYZ is materially misstated.', whereas the opinion in a reasonable assurance engagement may be 'Based on the procedures performed, in our opinion, the management assertion on XYZ is reasonably stated.'

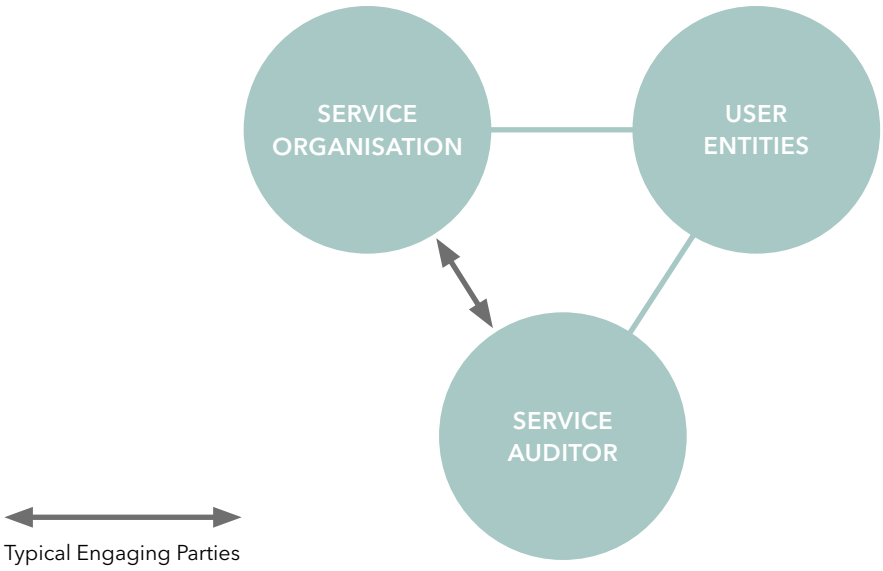
21. Absolute assurance exists as a concept whereby a Service Auditor forms a conclusion and issues an assurance report based on complete certainty. This requires testing 100% of a population and all instances of controls being operated, assuming that such controls are suitably designed to address all the requirements of the Criteria. While this is considered possible in concept, from a practical standpoint, it cannot realistically be achieved owing to the weight of evidence required. Therefore, it is not envisaged that absolute assurance could be applied to reports issued under this guidance.

22. This guidance is prepared for a Service Auditor performing a reasonable assurance engagement.

NATURE OF ENGAGEMENT AND ENGAGEMENT LIFE CYCLE

23. For reasonable assurance engagements, the following three conditions will exist:

- A three-party relationship. For the purposes of this guidance, the three parties are the:
  - Service Organisation;
  - Service Auditor; and
  - User Entities.
- A defined Subject Matter: i.e., something to report on which for the purposes of this guidance are principally the Control Activities;
- Established Criteria: i.e., something to report against which for the purposes of this guidance are principally the Control Objectives.



24. The Service Organisation is responsible for providing information on specific Control Activities to meet the Control Objectives. The Service Auditor performs the assurance engagement in accordance with this guidance.

25. The resulting reporting package ('the Report') comprises the following four components:

- A Management Statement concerning the Control Activities of the Service Organisation and Senior Management's assertion on them.
- A Service Auditor's Report explaining the scope of their assurance work carried out and giving their opinion.
- A Description of the Service Organisation, including the Control Activities of the Service Organisation. This comprises two parts:
  - An overview of the services provided, together with details of the governance arrangements, key functions and processes, key systems and supporting infrastructure[3]; and
  - A detailed description of the Control Activities which are designed to meet the Control Objectives, along with the results of testing performed by the Service Auditor.
- Other Information, which may include additional information that is likely to be helpful to User Organisations but is not included within the scope of the Service Auditor's Report.

26. The diagram below sets out the key activities for each stage in the reasonable assurance engagement life cycle:

[3] The COSO Framework may be used here.

IDENTIFYING REPORTING CRITERIA – CONTROL OBJECTIVES

27. In an assurance report provided under this guidance, the Criteria are typically the Control Objectives around which the Service Organisation has identified its Control Activities. These Control Objectives reflect the risks relevant to User Entities that are being managed by the Service Organisation.

28. An assurance engagement under this guidance requires the Service Auditor to express an overall opinion on the information assessed relative to certain Control Objectives. Control Objectives also help Senior Management and User Organisations to understand how the Service Auditor has evaluated Control Activities to reach their conclusion. The Control Objectives need to be relevant, complete, reliable, neutral and understandable so as to communicate the basis of the evaluation.

29. Appendix 1 sets out detailed Control Objectives for the financial service activities referred to in paragraph 6. These Control Objectives are those which are considered to be common to these types of financial services organisations, and should therefore be included as a minimum set of Criteria for reports issued under this guidance. This facilitates consistency of reporting and enables User Organisations to compare the control environments across similar types of Service Organisation. These minimum Control Objectives are not exhaustive and it remains the responsibility of Senior Management to ensure that the described Control Objectives are sufficient to meet the expectations of User Entities. A Service Organisation may therefore consider the need to add further Control Objectives and supporting Control Activities where appropriate. Illustrative supplementary Control Objectives are provided in Appendix 1 that correspond to additional activities that may be performed by Service Organisations. Where a Service Organisation performs such additional activities, the inclusion of these supplementary Control Objectives should be included in the scope of the Report, as appropriate.

30. The Control Objectives in Appendix 1 should form a minimum scope for the Report. If certain Control Objectives do not apply because the services are not provided or are materially modified, Senior Management must explain the omission/modification in their Management Statement.

31. In many sectors complex supply chains have developed where Service Organisations depend upon other, specialist organisations to undertake activities for them. Sometimes the specialist organisations are simply suppliers (for example, a benchmark data provider or an external law firm). However, other commercial outsourcing relationships are more fundamental to the responsibilities of the Service Organisation in the context of User Organisations. Where the Service Organisation would have carried out the operation of related Control Activities in-house, had it not outsourced to a third party, the organisation undertaking the outsourced activity is known as a Subservice Organisation. Examples are investment administration outsourced to another party and Information Technology (IT) outsourced to another group entity outside the scope of the Report.

32. Service Organisations retain responsibility for the Control Activities that have been outsourced to a Subservice Organisation. They are required to monitor the effective operation of controls over activities carried out on their behalf. Additional considerations are required where a Service Organisation uses a Subservice Organisation to perform some aspects of the services provided to User Entities. Details are provided in paragraphs 104 to 109 and Appendix 8.

33. Service Organisations that employ the services of Subservice Organisations include monitoring and oversight Control Activities at two levels: at a governance level and at an operational level.

    a. Governance: The Governance level concerns the strategic and contractual relationship between the Service Organisation and the Subservice Organisation. The relevant oversight Control Activities at the Governance level are included under a specific Control Objective that may include, for example, review of contractual terms, review of established service standards (or service level agreements) or periodic service level meetings.

b. Operational: The Service Organisation retains responsibility for the outsourced activities. It also retains responsibility for managing the risks associated with those activities on behalf of User Organisations. Therefore, the Service Organisation should not exclude Control Objectives that relate to the outsourced activities on the basis that they do not perform the primary Control Activities over those activities. The Service Organisation retains the relevant Control Objectives that relate to the activities being performed, setting out the monitoring Control Activities in place to oversee the activities of the Subservice Organisation in relation to each relevant Control Objective. For example, review of daily reconciliation exception reports, review of monthly NAV reports or review of daily back-up completion reports.

34. In conducting their work, the Service Auditor assesses the fairness of presentation, design suitability and, where appropriate, operating effectiveness of Control Activities against the Control Objectives.

3. Responsibilities of senior management of the service organisation

35. To meet User Entities' expectations in terms of the level of control over services provided on their behalf, Senior Management identify Control Objectives together with the Control Activities which they consider appropriate to enable these Control Objectives to be met. The key responsibilities of Senior Management are:

    - Acceptance of responsibility for internal controls;
    - Providing a description of the Service Organisation's Control Activities and the governance arrangements within which they operated for the relevant period (the 'Description');
    - Assessment of the effectiveness of the Service Organisation's Control Activities against the Control Objectives;
    - Supporting their evaluation with sufficient evidence, including documentation; and
    - Providing a Management Statement.

ACCEPTANCE OF RESPONSIBILITY FOR INTERNAL CONTROLS

36. Senior Management are responsible for the design, implementation and operation of the Control Activities of the Service Organisation. This is acknowledged in the Management Statement, an assertion provided by Senior Management within the Report and signed by an Authorised Signatory of the Service Organisation. The contents of the Management Statement are set out in paragraph 58.

37. Suitably designed Control Activities, when complied with individually or in combination with other Control Activities, are expected to operate so as to prevent or detect errors that could result in the failure to achieve the specified Control Objectives. Senior Management evaluate the design and operation of Control Activities during the relevant reporting period.

38. The Service Auditor's tests are separate from the Service Organisation's own procedures for evaluating the effectiveness of the Control Activities. The work of the Service Auditor cannot be used as part of the basis for the Service Organisation's assessment of whether Control Activities are suitably designed or the operation of the Control Activities is effective.

39. It is also the responsibility of Senior Management to take reasonable steps to prevent and detect fraud.

PROVIDING A DESCRIPTION OF THE SERVICE ORGANISATION'S CONTROL ACTIVITIES AND THE GOVERNANCE ARRANGEMENTS WITHIN WHICH THEY OPERATED FOR THE RELEVANT PERIOD (THE 'DESCRIPTION')

40. Senior Management are responsible for the completeness, accuracy, validity and method of presentation of the Description. The Description sets out an overview of the services provided, together with details of the governance arrangements, key functions and processes, key systems and supporting infrastructure and a detailed description of the Service Organisation's Control Activities designed to meet the Control Objectives. The Service Auditor may assist the Service Organisation in preparing the Description (refer to paragraph 71); however, the representations in the Description are the responsibility of Senior Management.

41. The description of Control Objectives and Control Activities does not necessarily address every service provided by the Service Organisation but presents a level of detail that provides sufficient information for User Entities to assess control risk, and for their auditors to plan an audit of User Entities' financial statements as if a Service Organisation were not used.

42. Senior Management, where appropriate, seek to describe Control Activities in a manner which permits verification and is understandable to User Organisations. To achieve this and to promote consistency in approach, Senior Management may find it helpful to differentiate between the different components of the overall system of internal controls which are being described in the Report. The principal components are in general likely to include Control Objectives, process descriptions and Control Activities. Process descriptions provide context for the operation of Control Activities. Process descriptions and Control Activities are precise in order to avoid the possibility of different interpretations being placed on these by different User Organisations.

43. Control Activity descriptions need to be factual, objective, specific and verifiable:

    - Factual: a true representation of the Control Activity undertaken.
    - Objective: avoids the use of subjective words such as adequate, appropriate, should, regular, timely, etc.
    - Specific: contains sufficient detail to allow User Organisations to understand the nature, timing and extent of the Control Activity, who is responsible for its performance and what IT, if any, supports it.
    - Verifiable: avoids the use of non-verifiable words such as only, always, never, etc. Evidence is retained to demonstrate the performance of the Control Activity and to support testing of the Control Activity by Senior Management and the Service Auditor.

44. Where the Service Organisation has introduced significant changes to its system or Control Activities within the reporting period, the system or Control Activities before and after the change and the implications are documented in the Description by Senior Management. The judgement as to the significance of the change is based on its impact on the Control Objective relevant to User Entities.

ASSESSMENT OF THE EFFECTIVENESS OF THE SERVICE ORGANISATION'S CONTROL ACTIVITIES AGAINST THE CONTROL OBJECTIVES

45. Senior Management must determine those Control Activities in place to address the Control Objectives they have identified. In doing so, it is important for Senior Management to differentiate between processes executed by the Service Organisation and the Control Activities in place to check the operation of those processes. Typically, the main types of Control Activities are:

    - Reconciliation and resolution;
    - Exception reporting, review and escalation;
    - Independent/management review;
    - Monitoring and action;
    - Authorisation;
    - Verification/validation; and
    - System configuration and access.

It is expected that the majority of other procedures are not Control Activities.

46. Senior Management should identify an appropriate combination of preventative, detective, automated and manual Control Activities to satisfy a Control Objective.

47. Most Service Organisations use IT in the delivery of their operational processes. The Description sets out which applications and related infrastructure are used, their role in the delivery of services in scope for the Report, and Senior Management's governance over this IT environment. IT Control Objectives and Control Activities are included within the Description. The minimum suitable IT Control Objectives are provided in Appendix 1. Automated Control Activities are considered for inclusion under the relevant Control Objectives, for example automated reconciliation processes.

SUPPORTING THEIR EVALUATION WITH SUFFICIENT EVIDENCE, INCLUDING DOCUMENTATION

48. Senior Management support the assertions made in the Management Statement in respect of the design, implementation and operating effectiveness of the Service Organisation's Control Activities with sufficient evidence. The nature of Senior Management's evaluation activities depends largely on the circumstances of the Service Organisation and the significance of particular Control Activities. Evaluation procedures may include review and testing by internal audit or a third party, under the direction of Senior Management, (for example an internal audit resource augmentation arrangement or another third party assurance report on a specific subject), business risk and/or compliance personnel.

49. Monitoring of Control Activities involves assessing the effectiveness of those Control Activities throughout the period, identifying and reporting exceptions to appropriate individuals within the Service Organisation and taking necessary corrective actions as soon as is practical. Senior Management may monitor Control Activities through ongoing activities, separate evaluations or a combination of the two.

50. Ongoing monitoring activities are built into normal recurring procedures, including regular supervisory reviews. Ongoing monitoring activities may include using information communicated by third parties, such as User Entity complaints or settlement and confirmation breaches, which may indicate exceptions or highlight areas requiring improvement.

51. Senior Management may use a risk and control self-assessment process where this is supplemented by review of further evidence to support its efficacy, for example sample testing of control owner attestations by internal audit or a third party (under the direction of management) and review of key risk indicators, breach rates, or loss incidents.

52. Senior Management consider the sufficiency of this evidence and whether any additional evaluation of specific areas may be appropriate to enable them to provide a written Management Statement as to the effectiveness of the internal controls. The process that Senior Management undertake may include considering:

    - Evidence available from on-going monitoring of Control Activities;
    - Any exceptions that have come to their attention, for example, through management testing, internal audit reports and reports by regulators; and
    - Evaluation as to the likelihood that the failure of certain Control Activities could result in a Control Objective not being met, the extent to which that Control Objective is not met and the degree to which other Control Activities, if effective, achieve the same Control Objective.

53. The Service Auditor's Report is not a substitute for Senior Management's own processes to undertake and provide a reasonable evaluation in support of its Management Statement.

54. Documentation of Control Activities in place is evidence of Control Activities being identifiable, capable of being monitored and communicable to those responsible for their performance. Inadequate documentation may indicate an exception in the Service Organisation's Control Activities and is subject to evaluation by the Service Auditor as to its significance.

55. Documentation of Control Activities may take various forms depending on the nature and type of relevant information. Policy manuals, process models and flowcharts could be used for recording the process in place and design of the Control Activity. The operation of a Control Activity will be demonstrated by evidence including, for example, checklists, automated matching, meeting agendas and minutes and documentation of the performance of a review.

56. Senior Management evaluate whether the documentation includes:

- The Control Activities necessary to address each Control Objective;
- Information about how Control Activities are initiated, authorised, recorded, processed and reported; and
- The results of Senior Management's testing and evaluation.

PROVIDING A MANAGEMENT STATEMENT

57. Through evaluation and documentation, Senior Management accumulate sufficient information to come to an overall conclusion in respect of the design and operating effectiveness of the Service Organisation's Control Activities during a specified period. Their opinion is based on the Control Objectives and includes an assessment of the impact of any exceptions on specific Control Objectives or the efficacy of the control environment taken as a whole. Senior Management communicate their opinion and the details of any relevant exceptions to User Organisations in the Management Statement.

58. The Management Statement contains:

a. A statement of Senior Management's responsibilities with regard to the identification of Control Objectives relevant to the Service Organisation and the description of the related Control Activities.

b. Reference to the Description which sets out details of each of the specific Control Activities designed to achieve the Control Objectives together with details of any significant changes to the Control Objectives and Control Activities during the period and the impact of any Subservice Organisations.

c. Reference to the use of this guidance with details of any omitted, materially modified or additional Control Objectives considered appropriate by Senior Management.

d. Details of any relevant exceptions considered significant by Senior Management, ie, where these exceptions are likely to impact on the achievement of one or more Control Objectives during the period.

e. A statement by Senior Management that they have assessed the effectiveness of the Control Activities and their opinion that:

i. The Description describes fairly the Control Activities that relate to the Control Objectives referred to in (b) above which were in place;

ii. The Control Activities described are suitably designed such that there is reasonable assurance that the specified Control Objectives would be achieved if the described Control Activities were complied with satisfactorily and User Entities applied the Complementary User Entity Controls identified; and

iii. The Control Activities described were operating with sufficient effectiveness to provide reasonable assurance that the related Control Objectives were achieved during the specified period.

f. The name, job title and signature of the Authorised Signatory signing on behalf of Senior Management.

g. The date of that signature.

A template Management Statement is provided in Appendix 2.

59. Where Control Activities carried out by a Subservice Organisation are included in the Report, Senior Management are responsible for ensuring that the Subservice Organisation also provides a Management Statement for inclusion in the Report, alongside Senior Management's own (refer to paragraphs 31 and 32).

60. An exception in a Control Activity (or a combination of Control Activity exceptions) may be identified by Senior Management or by the Service Auditor.

COMPLEMENTARY CONTROL ACTIVITIES OF USER ENTITIES

61. The Control Objectives stated in the Description may be worded so that they are capable of being achieved through the effective operation of Control Activities implemented by the Service Organisation alone. It is expected that in most cases the activities of the Service Organisation will be described with the assumption that User Entities have Control Activities in place: for example, the authorisation of transactions, review of the completeness and accuracy of information submitted to the Service Organisation, written notification of changes, review of reports provided by the Service Organisation, and appropriate restrictions on access to relevant IT. If this is the case, the Description of the Control Activities at the Service Organisation also refers to Complementary User Entity Controls.

62. Where Complementary User Entity Controls are required to fully achieve Control Objectives, the Description separately identifies those Control Activities and the specific Control Objectives that cannot be achieved by the Service Organisation alone. This is typically set out in a separate section headed 'Complementary User Entity Controls'.

OTHER RESPONSIBILITIES OF THE SERVICE ORGANISATION

63. Other responsibilities of the Service Organisation include:

- Providing the Service Auditor with access to appropriate Service Organisation resources, such as personnel, systems, documentation, contracts, reports of internal reviews and minutes of key meetings;
- Disclosing to the Service Auditor any relevant outsourcing relationships with Subservice Organisations and arranging for the Service Auditor to have access to the relevant Subservice Organisations' resources, as described above, should the Control Activities be included in the Report. Where outsourced Control Activities are not included in the Report, the Service Organisation includes monitoring Control Activities over the processes carried out by the Subservice Organisations and discloses to the Service Auditor any Complementary Subservice Organisation Controls that have been assumed to be in place when designing monitoring Control Activities (refer to paragraphs 31 and 32);
- Disclosing to the Service Auditor any significant changes in Control Activities that have occurred since the Service Organisation's last examination or within the period subject to examination if the Service Organisation has not previously engaged a Service Auditor to issue a Service Auditor's Report;

- Disclosing to the Service Auditor and the affected User Entities any illegal acts, fraud, or uncorrected errors attributable to Senior Management or employees that may affect its User Entities and their whistle-blowing arrangements;
- Disclosing to the Service Auditor any relevant design exceptions in Control Activities of which it is aware, including those for which Senior Management believe the cost of remediation may exceed the benefits;
- Disclosing to the Service Auditor all significant instances of which it is aware when Control Activities have not operated with sufficient effectiveness to achieve the specified Control Objectives; and
- Providing the Service Auditor with Senior Management's Representation Letter in the form requested by the Service Auditor and, where a Subservice Organisation's Control Activities are included in the Report, arranging for the Subservice Organisation to provide the Subservice Organisation's Senior Management's Representation Letter to the Service Auditor (refer to paragraphs 162 to 164).

OTHER INFORMATION PROVIDED BY THE SERVICE ORGANISATION

64. A Service Organisation may wish to present Other Information that is not part of the Description in its Report, for example:
    - Senior Management's responses to exceptions identified by the Service Auditor's testing, including additional information about planned improvements to the relevant processes and Control Activities.
    - Background information on the entities within the Service Organisation's group, the services they provide and their regulatory permissions.
    - An outline of the Service Organisation's business continuity and disaster recovery plans.
    - Additional detail on the IT system architecture and data flows not included in the Description.
    - Additional information on compliance with regulatory standards over specific aspects of the business which is not directly relevant to the Control Activities covered by the Report, but which is of interest to the User Entities, for example regulations covering anti-money laundering, client money and data protection.
    - Additional information on measures undertaken to protect the organisation against viruses or other malicious attacks that go beyond the scope of the Description.
    - HR policies and processes.
    - An outline of any planned changes to processes or IT.
    - An outline of the insurance arrangements of the Service Organisation.
65. Where information of this nature is presented, it is presented in a separate appendix to the Report and made clear that it does not constitute a part of the Description.
66. For the avoidance of doubt, Senior Management are responsible for ensuring any appendices to the Report are factually accurate and not misleading. These appendices are not within the scope of the Service Auditor's opinion.

4. Guidance for the service auditor

ACCEPTING AN ENGAGEMENT

68. It is important that there is a clear understanding and agreement concerning the scope and purpose of the engagement between the Service Auditor, the Service Organisation and, if applicable, the User Entities that are party to the engagement.

69. The Service Auditor considers whether the engagement team collectively possesses the necessary professional competencies having regard to the nature of the assignment.

70. Before accepting any professional engagement, the Service Auditor considers whether there are any ethical factors which should lead them to decline the appointment. ICAEW members are subject to the ethical and other guidance laid down by the Institute, including the fundamental principles of the prevailing Code of Ethics adopted by the ICAEW, in performing any professional services, to maintain the standard of their conduct.

71. When performing additional non-audit assurance engagements, appropriate consideration should be given to independence of mind and in appearance with respect to the Service Organisation and any other parties to the engagement. Examples include:

    - The provision of assistance to the Service Organisation in preparing its Description which may result in a self-review threat should be assessed; and
    - The performance of services for User Entities whose interests are in conflict or who are in dispute with each other in relation to the Subject Matter in question.

    If the Service Auditor identifies threats to their independence, safeguards need to be considered. These might include:

    - The use of independent teams, where appropriate; and
    - An independent review of the key judgements on the engagement.

72. The Service Auditor's Report may be received by a range of persons who are not party to the engagement. The Service Auditor does not intend to assume responsibility to persons who are not party to the engagement, but legal actions from such persons may nonetheless occur. The Service Auditor therefore needs to apply appropriate engagement acceptance procedures in order to assess the risks associated with taking on a particular engagement and accordingly whether to do so and, if so, on what terms. Where the Service Auditor accepts such an engagement, suitably rigorous internal risk management policies are applied to manage any increased level of risk. Relevant steps for managing professional liability are covered in the following section[4].

MANAGING PROFESSIONAL LIABILITY

73. Depending on the engagement circumstances the Service Auditor enters into one or a combination of the following arrangements:

    a. A tri-partite or multi-partite engagement contract with the Service Organisation and User Entities, accepting that they owe a duty of care not only to the Service Organisation but also to those User Entities, including provisions limiting liability if appropriate (recognising that such a contract may not be achievable where User Entities are numerous).

    b. An engagement with the Service Organisation with the facility for User Entities to enjoy a duty of care from the Service Auditor if they accept the relevant terms of the engagement letter previously agreed with the Service Organisation as if they had signed that letter when originally issued, including the same provisions limiting liability[5].

[4] Further guidance can be found in BL 09/15 *Managing the professional liability of professional accountants*.

[5] This will require the consent of the Service Organisation/original addressees, ideally in the engagement letter.

c. An engagement with the Service Organisation alone but before allowing User Entities access to the Service Auditor's Report, require User Entities:

   i. To acknowledge in writing that the Service Auditor owes User Entities no duty of care; and

   ii. To agree in writing that no claims may be brought against the Service Auditor by User Entities in relation to the Service Auditor's Report[6].

d. An engagement with the Service Organisation alone disclaiming any liability or duty to others (including User Entities) by notice in the Service Auditor's Report. The Service Auditor also considers supporting this disclaimer with an indemnity from the Service Organisation to apply where a third party claim is made (recognising that such an indemnity may not be attractive commercially, may not be effective if the Service Organisation is not financially stable, and may not operate to prevent a claim: see further paragraph 81)[7]. It is also open to Service Auditors to consider with their legal advisers the use of the Contract (Rights of Third Parties) Act 1999 to manage the risk of liability to third parties. The above arrangements do not prevent User Entities taking legal action against the Service Organisation.

74. The Service Auditor will describe carefully in the Service Auditor's Report the work that they do, including the description of the test procedures they have performed. In the latter context, close definition of what is meant by enquiry, observation, inspection and re-performance is desirable. Some illustrative definitions are set out at Appendix 7.

75. The Service Auditor disclaims responsibility and liability to User Entities' auditors, having regard to the responsibility of User Entities' auditors for their own audit reports and for determining to what extent (if any) the Service Auditor's Report amounts to sufficient appropriate audit evidence for the purposes of their audit of a relevant User Entity's financial statements.

76. The Service Auditor may become aware of other third parties that are not User Entities of the Service Organisation, such as banks and other lenders or prospective purchasers of the Service Organisation, who may also request the Service Auditor's Report. The Service Organisation or the third party may approach the Service Auditor for consent to make the Service Auditor's Report available to such third parties, as the engagement contract agreed with the Service Organisation contains disclosure and use restrictions. The Service Auditor's Report is not prepared for third parties or with their interests or needs in mind, and the Service Auditor may decline this request. The Service Auditor will have set out the purpose of their report in the Service Auditor's Report, and will have included a disclaimer of liability to third parties in line with paragraph 73(d) above in that Service Auditor's Report. If the request is not declined, the Service Auditor can advise the third party that the Service Auditor's Report was not prepared for the third party or the third party's benefit, that consent to the Service Auditor's Report being made available to a third party will only be given if the third party agrees that the third party should not rely on the Service Auditor's Report and acknowledges in writing that the Service Auditor owes the third party no duty of care and agrees that no claims may be brought against the Service Auditor by the third party in relation to the Service Auditor's Report.

77. The Service Auditor may also receive requests from the Service Organisation for consent to the release of the Service Auditor's Report to potential User Entities with whom the Service Organisation may be exploring the possibility of a relationship, or the Service Auditor may become aware that contrary to disclosure and use restrictions agreed with the Service Organisation in the engagement contract, such potential User Entities are gaining access to the Service Auditor's Report. The Service Auditor may decline any such request. If the request is not declined, the written

[6] The Service Auditor may wish to have regard to the principles outlined in Audit 04/03 *Access to working papers by investigating accountants*, bearing in mind that Audit 04/03 addresses different circumstances relating to third party issues, when developing a written form of such acknowledgment and agreement.

[7] The Service Auditor considers the legal effectiveness of disclaiming liability and of the proposed disclaimer in light of the particular circumstances of their engagement (see for example, the guidance in Technical Release 09/15BL *Managing the professional liability of accountants*). Service Auditors are advised to seek their own independent legal advice.

acknowledgement and agreement described above in relation to other third parties may be a practical solution to the management of risk in relation to potential User Entities. Where that is not practical, the Service Auditor requires the Service Organisation (as a condition for giving consent, where requested) to send all such potential User Entities a written statement, to accompany the Service Auditor's Report, pointing out that the Service Auditor did not undertake the work for potential User Entities and does not accept any responsibility to potential User Entities and denies liability to them. The Service Auditor may wish to provide the Service Organisation with a pro-forma statement and may wish to include reference to this in their engagement letter.

78. If correspondence between Service Auditors and User Entities, potential User Entities or third parties results from a disclaimer notice or otherwise, the Service Auditor decides (with independent legal advice if appropriate) how to bring such correspondence to a satisfactory close before it becomes protracted or undermines the original objective.

79. The Service Organisation may choose to distribute reports to User Organisations through electronic means. This may result in additional risks associated with reports being received and relied upon by parties other than the original intended User Organisations. As such, the Service Auditor considers appropriate arrangements to manage and mitigate against such additional risks.

AGREEING THE TERMS OF ENGAGEMENT

80. The Service Auditor agrees on the terms of engagement with the parties to the engagement in accordance with the contractual relationship as discussed in paragraph 73. To avoid misunderstandings, the agreed terms are recorded in writing in an engagement letter.

81. The written terms of the Service Auditor's engagement include:

    a. The agreed use of the Report and the extent to which, the context in which, and the basis on which, the Report may be made available by the Service Organisation to User Organisations and in certain circumstances to other parties;

    b. Confirmation that the Service Auditor's Report is not to be recited or referred to in whole or in part in any other published document without the Service Auditor's consent or as otherwise required by law or regulation;

    c. The respective responsibilities of the Service Organisation and the Service Auditor for the different elements of the Report;

    d. Acknowledgment by Senior Management on behalf of the Service Organisation for the design and operating effectiveness of Control Activities to achieve the related Control Objectives;

    e. The scope of the work to be performed by the Service Auditor;

    f. A reference to the need for Senior Management's Representation Letter;

    g. An explanation of the inherent limitations of the work, and for whom the work is being undertaken;

    h. Limitations to the liability of the Service Auditor, including an appropriate liability cap; and

    i. Provisions for an indemnity, if considered appropriate.

82. Example extracts from an engagement letter for a Service Auditor's Report on internal controls of a Service Organisation are given in Appendix 5 for illustrative purposes. The Service Auditor applies their own judgement to develop suitable wording for their engagement letter to reflect this guidance and their own particular circumstances. Where the engaging parties include User Entities or any other parties, the nature and the content of the engagement letter may differ from the example extracts.

83. The Service Auditor considers excluding liability in respect of any loss or damage caused by, or arising from fraudulent acts, misrepresentation, concealment of information or deliberate default on the part of the Service Organisation, Senior Management, the Service Organisations' employees or agents due to the impact of such omissions and representations on the Report.

84. If, before the completion of the engagement, the Service Auditor receives a request from the Service Organisation to change an assurance engagement to a non-assurance engagement or to change, for instance, the scope of the engagement, the Service Auditor considers whether this has reasonable justification. An example of a justified request to change the scope is if there is a specific product or service that can be clearly ring fenced where each of the User Entities of that product or service no longer require the report. A common example where this is likely not to be justified is where one or more key Control Activities have been found to have reportable exceptions that will probably give rise to a qualification of the Service Auditor's opinion. The majority of imposed limitations of scope are unlikely to be justified.

QUALITY CONTROL

85. The Service Auditor performs the assurance engagement in the same professional manner as any other engagement and in accordance with the scope agreed and recorded in the engagement letter.

86. When performing an assurance engagement under this guidance, the Service Auditor is subject to International Standard on Quality Control (ISQC) (UK) 1 'Quality control for firms that perform audits and reviews of historical financial information, other assurance and related services engagements' or the successor standards. ISQC (UK) 1 requires that a firm of chartered accountants has an obligation to establish a system of quality control designed to provide it with reasonable assurance that the firm and its personnel comply with relevant professional standards and regulatory and legal requirements and that assurance reports issued by the firm or engagement partners are appropriate in the circumstances.

87. The elements of such a system of quality control which are relevant to an individual engagement include leadership responsibilities for quality on the engagement, ethical requirements, acceptance and continuance of client relationships and specific engagements, assignment of engagement teams, engagement performance (in particular supervision, consultation, review and documentation) and monitoring.

PLANNING

88. Where the Report is referred to as being prepared in accordance with the framework for reporting set out in this guidance, the Service Auditor plans and performs their work so as to provide a reasonable basis for their opinion. Professional judgement is needed to determine the required nature, timing and extent of the tests to be carried out and the reliance, if applicable, on any Service Organisation's internal auditors.

89. The Service Auditor's work is planned so as to have a reasonable expectation of detecting, at the time the work is undertaken, relevant exceptions in respect of the Control Activities described by Senior Management and tested in accordance with the terms of the engagement. However, the work cannot be expected to detect problems which may be considered significant from the point of view of a particular User Entity and the scope of the work may mean that all Control Activities relevant to an individual User Entity may not have been tested.

90. The Service Auditor is not expected to assess the adequacy of the evaluation of Control Activities performed by Senior Management as part of an engagement to report on the Service Organisation's Control Activities, but is expected to make enquiries about Senior Management's assessment to inform their own planning and risk assessment.

THE SERVICE AUDITOR'S PROCEDURES

Materiality

91. When planning and performing the engagement, the Service Auditor considers materiality with respect to the fair presentation of the Description, the suitability of design of Control Activities and, as appropriate, the operating effectiveness of Control Activities to achieve the related Control Objectives stated in the Description. It is not for the Service Auditor to attempt to define a financial materiality level in relation to errors, because the Service Auditor will not know the financial materiality levels appropriate to the individual User Entities as defined by them and/or their Auditors.

92. It is the Service Auditor's judgement as to what constitutes a material matter. Examples of instances where a matter is expected to be considered material include:

- Following commencement of the engagement, Senior Management inappropriately amending the scope of the Report to exclude some User Entities, products, locations or excluding Control Activities as a result of the findings of the Service Auditor (refer to paragraph 84);
- The omission of Control Objectives that are otherwise relevant to the risks associated with the services performed on behalf of User Entities; or
- Control Activities identified to address a Control Objective not addressing all attributes of that Control Objective.

Fairness of the Description

93. The Service Auditor reads the Description of Control Activities to gain an understanding of the representations made by Senior Management in the Description. After reading the Description, the Service Auditor performs test procedures to determine whether the Description presents fairly, in all material respects, the Service Organisation's Control Activities that relate to the Control Objectives referred to by Senior Management which were in place.

94. To determine whether the Description is fairly presented, the Service Auditor gains an understanding of the services provided by the Service Organisation. Procedures to gain this understanding may include:

- Discussing aspects of the control framework and relevant Control Activities with Senior Management and other personnel of the Service Organisation;
- Determining who the User Entities are and how the services provided by the Service Organisation are likely to affect the User Entities, for example, the predominant type of User Entities;
- Reviewing standard terms of contracts with User Entities to gain an understanding of the Service Organisation's contractual obligations;
- Observing the procedures performed by the Service Organisation's personnel; reviewing the Service Organisation's policy and procedure manuals and other systems documentation, for example, flowcharts, narratives and organisation charts; and

- Performing observation and enquiry with the Service Organisation to attest to the fair presentation of the Description and related Control Activities, which may include performing walk-throughs of selected transactions.

95. The Service Auditor compares their understanding of the services provided to the User Entities by the Service Organisation with Senior Management's assertions made in the Management Statement to determine the fairness of the Description. Fairly described Control Activities do not omit or distort significant information that may affect the User Entities' assessments of control risk.

96. Fairly described Control Activities include a complete set of associated Control Objectives that are developed based on Control Objectives in Appendix 1. If there are inappropriate or unexplained omissions or material modifications with regard to the Control Objectives, the Service Auditor asks Senior Management to amend the Description. If it is not amended the Service Auditor considers implications for the Service Auditor's Report.

97. Where significant changes to Control Activities are introduced during the period covered in the Report, Senior Management report this fact. If the Service Auditor becomes aware that Senior Management have not done this, they ask Senior Management to amend the Description.

Design of Control Activities

98. As a part of their work, the Service Auditor determines whether the Control Activities are suitably designed. A Control Activity is suitably designed if individually, or in combination with other Control Activities, it is likely to prevent or detect errors that could result in the non-achievement of specified Control Objectives when the described Control Activities are complied with satisfactorily. A Control Activity may be applicable to more than one Control Objective.

99. The Service Auditor's assessment of the suitability of Control Activity design should include:

    - Considering the linkage between the Control Activities and the associated Control Objectives;
    - Considering the ability of the Control Activities to prevent or detect errors related to the Control Objectives;
    - Performing walk-throughs of selected transactions and the impact of Control Activities; and
    - Performing further procedures, using a combination of the following:
        - Enquiry of appropriate Service Organisation personnel;
        - Inspection of documents and reports;
        - Observation of the application of specific Control Activities, to determine whether they are suitably designed to achieve the specified Control Objectives and if they are operated as prescribed, by appropriately qualified or experienced persons; and
        - Re-performance of a reconciliation or calculation.

100. Where certain Control Objectives of the Service Organisation are reliant on Control Activities executed by the User Entities in order to achieve Control Objectives, the Service Auditor considers whether such Complementary User Entity Controls are included in the Description. If they are not and Senior Management fail or refuse to amend the Description, the Service Auditor considers adding an explanatory paragraph to describe the required Complementary User Entity Controls and considers the implications for the Service Auditor's opinion on the fairness of the Description (refer to paragraph 130).

Operating effectiveness

101. The Service Auditor performs tests of the relevant Control Activities to obtain evidence about the operating effectiveness of the Control Activities during a specified reporting period. Operating effectiveness is concerned with how a Control Activity is applied, the consistency with which it is applied, and by whom it is applied. The Service Auditor determines the nature, timing and extent of the tests to be performed to form their opinion on the operating effectiveness of the Control Activities. The Service Auditor may wish to provide the User Entities with a further explanation of the tests that they have performed in an appendix to the Service Auditor's Report.

102. Where the Service Auditor is unable to test a described Control Activity because, for example, it was not required to operate during the year, they state the fact that no tests have been carried out and the reason in their description of tests. The Service Auditor also seeks Senior Management confirmation of these Control Activities where there was no operation and related rationales in Senior Management's Representation Letter.

103. The Service Auditor must use evidence relating to the reporting period only. Each Control Activity is assessed for operating effectiveness for every reporting period.

SERVICE ORGANISATIONS THAT USE OTHER SERVICE ORGANISATIONS

104. The Service Organisation determines whether its description of Control Activities should include the relevant Control Activities carried out by the Subservice Organisation on its behalf. The two methods of dealing with Subservice Organisations in reports on internal controls are the carve-out method and the inclusive method.

105. The carve-out method is a method of addressing the services provided by a Subservice Organisation, whereby Senior Management's Description of the processes and Control Activities includes the nature of the services performed by the Subservice Organisation and Senior Management's monitoring and oversight of these services to achieve the stated Control Objectives. The Description excludes details of the Subservice Organisation's relevant Control Objectives and related Control Activities and these are therefore excluded from the scope of the Service Auditor's engagement.

106. The inclusive method is a method of addressing the services provided by a Subservice Organisation, whereby Senior Management's Description of its processes and Control Activities includes a description of the nature of the services provided by the Subservice Organisation, as well as the Subservice Organisation's relevant Control Objectives and related Control Activities.

107. Although the inclusive method provides more information for User Entities than the carve-out method, the inclusive method may not be appropriate or feasible in all circumstances. Factors that are relevant in determining which approach to use include the following:

- The nature and extent of the information about the Subservice Organisation that User Organisations may need;
- The challenges entailed in implementing the inclusive method;
- Whether the Service Auditor is independent of the Subservice Organisation (in an inclusive method engagement, the Service Auditor's Report covers the Service Organisation and the Subservice Organisation, and the Service Auditor would need to be independent of both entities); and
- The availability of a Type 1 or Type 2 Service Auditor's Report on the Subservice Organisation that meets the needs of User Organisations.

108. A Service Organisation may use multiple Subservice Organisations and may prepare its Description using the carve-out method of presentation for some Subservice Organisations and the inclusive method of presentation for other Subservice Organisations. The Service Auditor determines whether the guidance concerning the inclusive method of presentation has been applied to all the Subservice Organisations for which the inclusive method is used and that the guidance concerning the carve-out method has been applied to all the Subservice Organisations for which the carve-out method has been used.

109. Further details on how the inclusive and carve-out methods for Subservice Organisations are applied can be found in Appendix 8.

NATURE, TIMING AND EXTENT OF TESTS

110. Tests of Control Activities over operating effectiveness might include a combination of enquiry of the appropriate personnel, observation of the application of the Control Activities, inspection of relevant documentation and re-performance of the Control Activity. Enquiry alone does not provide sufficient evidence to support an opinion about the operating effectiveness of a specific Control Activity.

111. Tests of operating effectiveness provide evidence that enables the Service Auditor to report on the entire period covered by the Report. Certain Control Activities may not have evidence of their operation that can be tested at a later date and accordingly, the Service Auditor tests the operating effectiveness of such Control Activities at various times throughout the reporting period.

112. Where Control Activities to be tested depend upon the completeness and accuracy of information produced by the Service Organisation, it is determined whether it is necessary to obtain evidence supporting the operational effectiveness of the Control Activities over the production of that information. Typically this will arise where a manual Control Activity relies upon the completeness and accuracy of information included in a system-generated report. For example, 'management reviews a system report to identify any client agreement breaches'; in this example the operating effectiveness of the Control Activity is dependent on the operating effectiveness of the system Control Activities relating to completeness of the information within that report. Management may consider identifying the key system-generated reports in the relevant Control Activities.

    When using information produced by the Service Organisation, the Service Auditor evaluates whether the information is sufficiently reliable for the Service Auditor's purposes, including, as necessary:

    - Obtaining evidence about the completeness and accuracy of the information;
    - Testing the Control Activities in place that support the completeness and accuracy of the information; and/or
    - Evaluating whether the information is sufficiently precise and detailed for the Service Auditor's purposes.

113. Where the Service Organisation has implemented changes to its Control Activities, the Service Auditor evaluates how the change of Control Activities impacts the coverage of the relevant Control Objectives. Where a change of Control Activities occurs during the period, the Service Auditor also evaluates the effectiveness of both the superseded and new Control Activities in the period covered. The Service Auditor agrees with Senior Management how it is possible for the Control Activities to be tested before and after the change.

114. Where the change of Control Activities occurs within the period, both the superseded and the new Control Activities should be listed in the Service Auditor's Report, with a clear indication of the periods to which each Control Activity is applicable.

115. The number of instances of the Control Activity operating selected as a sample for testing depends on a combination of attributes, including:
    - Frequency of operation (eg, daily, weekly);
    - Nature of operation (eg, manual, automated);
    - Complexity of Control Activity (eg, number of people involved, number of steps to be performed);
    - Level of judgement within operation (eg, approval of estimates without tolerance settings);
    - Likelihood of error (eg, previous records of errors, other factors listed above); and
    - Degree of centralisation of operation (eg, harmonised procedure manuals, centralised training, centralised governance).
116. When selecting samples, the Service Auditor:
    - Considers the purpose of the test procedure when defining the population from which the samples will be selected; and
    - Selects items for the sample in such a way that the sample covers the full reporting period, but otherwise selects those items using a random method.
117. Where a test procedure cannot be fully completed for a sampled item, the Service Auditor should consider whether the Control Activity applies to the whole population. If it doesn't, the population has been defined incorrectly:
    - If the population has been defined incorrectly, the Control Activity should be split out with separate populations and test procedures being applied; or
    - If the population and test procedure have been defined correctly, the item is treated as an exception.
118. Examples of sample sizes are given in Appendix 6.

DESCRIBING TESTS OF OPERATING EFFECTIVENESS AND EXCEPTION REPORTING

119. The Report sets out:
    a. The Service Organisation's Control Objectives;
    b. The Service Organisation's Control Activities to meet each Control Objective;
    c. The tests of the Control Activities performed by the Service Auditor;
    d. The results of each of those tests on a Control Activity by Control Activity basis; and
    e. The conclusions reached by the Service Auditor.

The diagram below illustrates an example tabular layout to present this information alongside the Description prepared by Senior Management and also indicates the ownership for each of these inputs. This illustration does not include details of the process description that provides context for the operation of the Control Activities.

Control Objective #3.5	Cash and investment positions are completely and accurately recorded	
Control Activity	**Description of test procedures performed**	**Result of testing**
3.5.1 On a daily basis, cash records per the administration system are reconciled to custodian bank records using an automated reconciliation system. Teams resolve the exceptions and annotate the exceptions report with explanations and/or actions taken to resolve each item. Reconciling items are reported on an exceptions report.	For a selection of days, obtained electronic copies of the exceptions report from the reconciliation system and inspected the annotations made by the operations team of explanations for, and/or actions taken to resolve, each item. For a selection of exceptions, inspected evidence of supporting documentation being retained for actions taken.	No exceptions noted.
3.5.2 On a daily basis, the client administration manager reviews the reconciliation exceptions report for evidence that all exceptions have been explained and/or resolved. This review is evidenced by electronic sign off on the exceptions report, copies of which are archived in the reconciliation system.	For a selection of days, obtained electronic copies of the exceptions report from the reconciliation system and inspected the electronic signature of the client administration manager as evidence of review.	Exception noted: For one out of a selection of 30 days, there was no evidence of sign off by the client administration manager on the electronic copy of the reconciliation exceptions report. No other exceptions noted.

Service Organisation responsibility for completion

Service Auditor responsibility for completion

120. The Service Auditor describes the nature, timing and extent of tests applied. In describing the nature of tests, the Service Auditor defines the types of tests performed. Illustrative definitions of tests such as enquiry, inspection, observation and re-performance are provided in Appendix 7. In describing the extent of tests, the Service Auditor indicates whether the items tested represent a sample or all the items in the population. Where an exception is reported, it is helpful to User Organisations for information on the sample or population size to be provided. If an exception is identified for a Control Activity that supports more than one Control Objective, the exception is reported against each Control Objective.

REPORTING BY THE SERVICE AUDITOR

Reporting on Description misstatements, design deficiencies or when Control Activities are not operating effectively

121. Having completed their testing work, the Service Auditor applies professional judgement in order to form an opinion and formally expresses this, in writing, in the Service Auditor's Report.

122. The Service Auditor's Report can take one of three forms:

- Unqualified;
- Qualified; or
- Adverse.

123. The reporting options are summarised as follows:

Unqualified			Qualified		Adverse
No exceptions	Minor exceptions	Non-applicable Control objective	Major exceptions	Limitation of testing	Pervasive exceptions

Unqualified Service Auditor's Report:

No exceptions

124. An unqualified Service Auditor's Report may be issued by the Service Auditor where it has sufficient evidence to reasonably conclude, in all material respects, on the matters within the scope of the engagement; ie, fairness of presentation, suitability of design and operating effectiveness of the Control Activities.

Minor exceptions

125. Where minor exceptions relating to the tests of operating effectiveness of Control Activities are identified, an unqualified Service Auditor's Report may still be issued by the Service Auditor where such exceptions fall within acceptable parameters determined by the Service Auditor, based on professional judgement. In order for exceptions to be concluded as minor they should, individually and in aggregate, be neither material to the achievement of the Control Objective nor pervasive to the Service Organisation or the Control Activities being performed. In such circumstances, no additional wording is required to be placed before the Service Auditor's opinion in the Service Auditor's Report, but the nature and extent of the minor exceptions are disclosed in the results of the testing performed by the Service Auditor.

Non-applicable control objective

126. Where the Service Auditor is unable to opine on a, or part of a, Control Objective because one or more related Control Activities were not required to operate during the reporting period (i.e. an event-driven Control Activity), it adds an explanatory paragraph preceding the opinion to the Service Auditor's Report setting out the non-applicable control objective. Examples of event-driven control activities include data migrations and new client take-on. This may not necessarily be accompanied by a qualification of the Service Auditor's opinion if there is sufficient evidence

to reasonably conclude, in all material respects, on all other matters within the scope of the engagement. An example of a Non-applicable control objective paragraph is provided in appendix 4 (d). Where a control objective is non-applicable, Senior Management also add a corresponding explanatory paragraph in the Management Statement. In such circumstances, the Service Auditor makes appropriate enquiries to satisfy itself that the Control Activities did not operate during the reporting period.

Qualified Service Auditor's Report:

Major exceptions

127. The Service Auditor issues a qualified Service Auditor's Report when either:

- The Service Auditor is unable to obtain sufficient evidence to conclude, in all material respects, on the matters within the scope of the engagement ie, fairness of presentation, suitability of design and operating effectiveness of the Control Activities; or
- The Service Auditor, based on the evidence obtained, concludes that, in all material respects, the matters within the scope of the engagement ie, fairness of presentation, suitability of design and operating effectiveness of the Control Activities are not in accordance with the relevant Control Objectives (or Criteria).

128. The following circumstances may therefore give rise to a qualified Service Auditor's Report:

- Where there are omissions or errors in respect of the Control Objectives;
- Where there are major exceptions in relation to the fair presentation of Control Activities;
- Where there are major exceptions in relation to the design suitability of Control Activities; and
- Where major exceptions (which are not pervasive) are identified in relation to the operating effectiveness of Control Activities:

- Exceptions may be considered to be major where they result in one or more Control Objectives not being met that do not impact upon the conclusion that the overall system of Control Activities is designed and operating effectively. For example, where a Control Objective is not met but does not impact on the achievement of other Control Objectives in the Report; or
- Exceptions may be considered pervasive where the ineffective design or operation of the impacted Control Activities and Control Objectives causes the overall system of control to not operate effectively. For example, where the exceptions result in a Control Objective that underpins the achievement of one or more other Control Objectives not being met. This may include Control Objectives over system access or programme change where other Control Objectives rely on information produced from the affected systems.

a) Qualifications with respect to Control Objectives

129. The Service Auditor discusses with Senior Management when they become aware that the Control Objectives are incomplete or inappropriate in light of the Criteria so that Senior Management may amend the Description to include the minimum Control Objectives. If Senior Management refuse or fail to do so the Service Auditor adds an explanation in the Service Auditor's Report identifying the omitted or inappropriate Control Objectives. In addition, the wording of the opinion paragraph may also be qualified.

b) Qualifications with respect to fair presentation of the Description

130. It is the responsibility of Senior Management and not the Service Auditor to ensure the completeness and fair presentation of the Description. Where the Control Activities are incomplete or inappropriate (which may result in some or all elements of a Control Objective not being achieved), the Service Auditor discusses this with Senior Management so that they may amend the Description to include or update the associated Control Activities. If Senior Management refuse or fail to amend the Description, the Service Auditor adds an explanatory paragraph preceding the opinion to the Service Auditor's Report identifying the omitted or inappropriate Control Activities to draw these to the attention of User Entities. In addition, the wording of the opinion paragraph in the Service Auditor's Report may be qualified. An example illustrating an exception to the fair presentation of the Description is provided in Appendix 4 (a).

131. Although the Service Auditor may qualify their opinion on the fairness of the Description of Control Activities, this does not necessarily affect the suitability of design or operating effectiveness of the Control Activities because the Service Auditor's opinion relates only to the Control Objectives that are included in the Description.

c) Qualifications with respect to design suitability

132. Where the Service Auditor concludes that a set of Control Activities are not suitably designed in relation to a specified Control Objective, it considers the design deficiencies in its overall assessment of the Control Activities. In performing this assessment, the Service Auditor discusses with Senior Management whether any other compensating Control Activities exist which may address the design deficiencies identified. Senior Management may amend the Description to include such compensating Control Activities which would then be subject to design suitability testing by the Service Auditor. If Senior Management refuse to include compensating Control Activities or they do not exist, then the Service Auditor may determine that the Control Activities are not suitably designed to achieve a specified Control Objective. The Service Auditor adds an explanatory paragraph preceding the opinion to the Service Auditor's Report identifying the design deficiencies and qualifies the opinion of the Service Auditor's Report. An example illustrating an exception to the suitability of design is provided in Appendix 4 (b).

d) Qualifications with respect to Operating Effectiveness

133. Where the Service Auditor's tests identify exceptions to the operating effectiveness of one or more Control Activities, it considers whether these exceptions, individually or in aggregate, mean that a Control Objective has not been achieved. In performing this assessment, the Service Auditor discusses with Senior Management whether any other compensating Control Activities exist which may address the exceptions identified. Senior Management may amend the Description to include such compensating Control Activities which would then be subject to design suitability and operating effectiveness testing by the Service Auditor. If Senior Management refuse to include compensating Control Activities or they do not exist, then the Service Auditor may determine that one or more Control Objectives have not been achieved and may therefore qualify its opinion on the achievement of these Control Objectives. The Service Auditor adds an explanatory paragraph preceding the opinion to the Service Auditor's Report and qualifies the opinion of the Service Auditor's Report. An example illustrating an exception which results in a qualification to the operating effectiveness is provided in Appendix 4 (c).

134. In some cases exceptions individually or in aggregate may be so pervasive that the Service Auditor issues an adverse opinion (see below).

e) Qualifications with respect to sub periods

135. Where significant changes to Control Activities are introduced during the period covered in the Service Auditor's Report, Senior Management report this fact.

136. In order to form a conclusion for the entire reporting period covered by the Service Auditor's Report, the Service Auditor tests the fair presentation, design suitability and operating effectiveness of the Control Activities both before and after the change. Senior Management are responsible for ensuring that sufficient evidence is available to support the testing of old and new Control Activities in each sub-period before and after the change. Where material deficiencies, exceptions or lack of evidence in relation to Control Activities in a sub-period are identified, the Service Auditor may qualify its conclusion on the achievement of one or more Control Objectives for a particular sub-period without qualifying its opinion for the entire reporting period. As with other qualifications, the Service Auditor adds an explanatory paragraph preceding the opinion to the Service Auditor's Report and qualifies the opinion of the Service Auditor's Report.

Limitation of testing

137. It is the responsibility of Senior Management to maintain appropriate evidence to support both the assertions made in the Management Statement as well as testing of the Control Activities by the Service Auditor. In some exceptional circumstances, such evidence is unavailable due to circumstances beyond the control of the Service Organisation. In these exceptional circumstances, the Service Auditor adds an explanatory paragraph preceding the opinion to the Service Auditor's Report setting out a limitation of testing. This may not necessarily be accompanied by a qualification of the Service Auditor's opinion, if there is sufficient evidence to reasonably conclude, in all material respects, on all other matters within the scope of the engagement.

138. Where a Limitation of Testing is to be applied, Senior Management should also add a corresponding explanatory paragraph in the Management Statement. In the case where the lack of evidence is beyond the control of the Service Organisation (for example, the evidence has been destroyed by accident by a third party), the Service Auditor should make appropriate enquiries before concluding on whether a qualification of the opinion is required.

Adverse Service Auditor's Report

139. Where the Service Auditor, having obtained sufficient and appropriate evidence, concludes that misstatements, omissions or exceptions (whether individually or in aggregate) are both material and pervasive to the Control Objectives as a whole, then an adverse Service Auditor's Report should be issued.

140. When expressing an adverse opinion, the Service Auditor states that the matters within the scope of the engagement ie, fairness of presentation, suitability of design and operating effectiveness of Control Activities relating to the Subject Matter are not in accordance with the Control Objectives (or Criteria) in all material respects due to the significance of the matters giving rise to the adverse Service Auditor's Report.

ELEMENTS OF THE REPORT THAT ARE NOT COVERED BY THE SERVICE AUDITOR'S REPORT

141. As discussed in paragraphs 64 to 66 where the Service Organisation has included information other than that which constitutes part of the Description of Control Activities in its Report, this is outside the scope of the Service Auditor's Report. Such information is placed in a separately distinguishable section within the Report. This section is titled 'Other Information provided by the Service Organisation'. The Service Auditor reads such information for consistency with their understanding of the Service Organisation. They also make reference in the Service Auditor's Report and at the top of the section with this additional information that these matters do not fall under the scope of the conclusion within the Service Auditor's Report.

142. Senior Management's responses to any reported exceptions that Senior Management wish to be included in the Report are also positioned either in the section titled 'Other Information provided by the Service Organisation' or in a separately distinguishable section within the Report.

143. If Senior Management wish to position a factual response next to the Service Auditor's reported exception, the response is assessed and, where possible, tested for validity by the Service Auditor and the test is also described here.

SUBSEQUENT EVENTS

144. Management are responsible for identifying and disclosing subsequent events. The Service Auditor enquires whether the Service Organisation is aware of any events subsequent to the reporting period, or point in time, up to the date of the Service Auditor's Report that could have a material effect on the Description of the Service Organisation's system or Service Auditor's opinion.

145. The Service Auditor performs procedures to obtain evidence of such events. If the Service Auditor becomes aware such an event has occurred, deemed significant to the User Entities, and the information about that event has not been disclosed by the Service Organisation within its Description or Management Statement, the Service Auditor discloses it in the Service Auditor's Report.

146. The Service Auditor has no obligation to perform any procedures regarding the Description of the Service Organisation's system, or the suitability of design and implementation or operating effectiveness of Control Activities, after the date or period to which the Service Auditor's Report refers.

THE SERVICE AUDITOR'S REPORT

147. The Service Auditor's opinion is expressed in a written report addressed to Senior Management. The Service Auditor's Report draws the attention of the readers to the basis of the Service Auditor's work, i.e., this guidance and ISAE 3000 (Revised) and ISAE 3402, as applicable.

148. The Service Auditor's Report reflects the agreement set out in the engagement letter. The Service Auditor's Report makes clear for whom it is prepared and who is entitled to rely upon it and for what purpose as established in paragraphs 80 to 84.

149. The Service Auditor concludes on the fair presentation of the Description and the design and operating effectiveness of Control Activities in relation to a specified reporting period.

150. Control Activities have inherent limitations and accordingly errors and irregularities may occur and not be detected. Also Control Activities cannot guarantee protection against fraudulent collusion especially on the part of those holding positions of authority or trust. The Service Auditor refers to such inherent limitations in the Service Auditor's Report.

151. Key contents of the Service Auditor's Report are shown below. A pro-forma Service Auditor's Report is available in Appendix 3.

152. The Service Auditor's Report contains:

    a. A title identifying the Service Auditor's Report.

    b. An addressee identifying the engaging parties to whom the Service Auditor's Report is directed.

    c. The date / period covered by the Service Auditor's Report.

    d. Identification of the applicable engagement letter.

    e. Reference to ISAE 3000 (Revised), and ISAE 3402, as applicable, and this guidance.

    f. Use of the Service Auditor's Report by Senior Management.

    g. Restrictions on the use of the Service Auditor's Report to Senior Management [and User Entities party to the engagement] and the replication of the Service Auditor's Report in whole or in part.

    h. Limitation of the liability of the Service Auditor to Senior Management [and User Entities party to the engagement].

    i. An identification and description of the Subject Matter information.

    j. A statement about whether Subservice Organisations have been handled using the inclusive or carve-out method (or where relevant, both). The Service Auditor also reinforces that the Opinion does not cover Control Activities of a carved-out Subservice Organisation.

    k. The identification of Senior Management as the Responsible Party and the respective responsibilities of Senior Management and the Service Auditor.

    l. Criteria against which the Subject Matter is evaluated.

    m. A reference to where in the Report details of the tests performed are described.

    n. Inherent limitations associated with the evaluation/measurement of the Subject Matter against the Criteria.

    o. The Service Auditor's opinion with the description of the Service Auditor's findings including sufficient details of errors and exceptions found.

    p. The name and signature of the firm/Service Auditor and the location of the office performing the engagement.

    q. The Service Auditor's Report date.

USING INTERNAL AUDITORS

153. The Service Auditor has regard to the requirements in the International Standards on Auditing (ISAs) (UK) and the needs of User Organisations when deciding whether to use internal auditors in relation to the performance of the engagement. The Service Auditor considers independence requirements in relation to the provision of internal audit services to the Service Organisation.

Using the work of internal audit

154. If the Service Auditor chooses to use the work of the internal audit department[8] in obtaining some of the evidence, the Service Auditor determines whether the work can be included within their own testing approach by evaluating whether:

[8] The internal audit department equally applies to internal, external or co-source arrangements.

- The internal audit department's organisational structure, policies and procedures support the objectivity of the department within the Service Organisation;
- The work was performed by internal audit having adequate technical training and proficiency;
- The work was properly supervised, reviewed and documented;
- Adequate evidence has been obtained to enable internal audit to draw reasonable conclusions; and
- The conclusions reached are appropriate based on the type and extent of tests performed and the results of those tests.

155. The Service Auditor performs sufficient procedures on the relevant work of the internal audit department to determine its adequacy for inclusion in the Service Auditor's principal evidence, including re-performing some of this work.

156. The Service Auditor also describes the work of the internal audit department and the Service Auditor's procedures in respect of this work in the section of the Report that describes the Service Auditor's tests of Control Activities. In addition, the use of internal audit work is cited within the Service Auditor's Report.

Direct assistance from internal audit

157. Direct assistance from internal audit is only appropriate if staff members being provided by the internal audit department have no influence on forming the Service Auditor's opinion.

158. If the Service Auditor plans on using internal audit staff to provide direct assistance, the Service Auditor:

- Assesses the existence of threats to the objectivity of those internal audit staff and the related safeguards applied to reduce or eliminate those threats;
- Prior to the use of internal audit staff, obtains a written confirmation from the Service Organisation that internal audit staff providing direct assistance to the Service Auditor will be allowed to follow the Service Auditor's instructions, and that the Service Organisation will not intervene or influence the work the internal audit staff perform for the Service Auditor; and
- Puts in place supervision and review structures so that all outputs from the internal audit staff are owned by the Service Auditor.

159. The Service Auditor references the tests performed by the internal audit staff within the Report as if they were the Service Auditor's own tests.

CONSIDERATIONS FOR UNCORRECTED ERRORS, FRAUD, NON-COMPLIANCE WITH LAWS OR REGULATIONS, OR ILLEGAL ACTS

160. In the course of performing procedures at a Service Organisation, the Service Auditor may become aware of uncorrected errors, non-compliance with laws or regulations, fraud or illegal acts attributable to the Service Organisation's systems, management or employees that may affect one or more User Entities.

161. Unless clearly inconsequential and considered not to affect any User Entities, the Service Auditor determines from Senior Management whether this information has been communicated to the affected User Entities. If Senior Management have not communicated this information and is unwilling to do so, the Service Auditor's appropriate actions may include:

- Communicating with third parties, for example with a regulatory body, where required to do so; and
- Obtaining legal advice about the consequences of different courses of action.

Where Senior Management do not respond appropriately, the Service Auditor considers whether to resign from the engagement or the implications on the Service Auditor's Report.

SENIOR MANAGEMENT'S REPRESENTATION LETTER

162. In all engagements, the Service Auditor obtains written representations signed by Senior Management who the Service Auditor believes is responsible for and knowledgeable, directly or through others in the Service Organisation, about the matters covered in the representations. The refusal by Senior Management to provide the representations considered necessary by the Service Auditor may be considered in forming the Service Auditor's opinion (refer to paragraph 127).

163. Senior Management's Representation Letter should be signed and is normally dated on the same day as the Management Statement and Service Auditor's Report.

164. If Senior Management's Representation Letter is signed and dated before the Management Statement and Service Auditor's Report, the Service Auditor requires written confirmation from Senior Management that the representations made still hold true as at the Management Statement and Service Auditor's Report date.

BRIDGING LETTER

165. Some User Organisations may desire a different Report period to that provided by the Service Organisation, eg, the User Entity's financial year end and the Report period end are not coterminous.

In these cases, it is usual for the User Entity to request a formal representation letter (a 'Bridging Letter') from Senior Management of the Service Organisation to cover the non-coterminous period relevant to the User Entity. An example Bridging Letter is available in Appendix 9.

Appendix 1: illustrative control objectives

As set out in paragraph 29, this appendix sets out detailed Control Objectives for the financial service activities referred to in paragraph 6. These Control Objectives are those which are considered to be common to these types of financial services organisations, and should therefore be included as a minimum set of Criteria for reports issued under this guidance. This facilitates consistency of reporting and enables User Organisations to compare the control environments across similar types of Service Organisation. These minimum Control Objectives are not exhaustive and it remains the responsibility of Senior Management to ensure that the described Control Objectives are sufficient to meet the expectations of User Entities. A Service Organisation may therefore consider the need to add further Control Objectives and supporting Control Activities where appropriate. Illustrative supplementary Control Objectives are provided in this appendix that correspond to additional activities that may be performed by Service Organisations. Where a Service Organisation performs such additional activities, the inclusion of these supplementary Control Objectives should be included in the scope of the report, as appropriate.

(A) CUSTODY

Accepting clients

- New client agreements and amendments are authorised prior to initiating custody activity
- Client details and accounts are completely and accurately set up onto relevant systems prior to initiating custody activity
- Asset transitions are completely and accurately recorded and communicated to clients in line with client instructions

Authorising and processing transactions

- Investment and related cash and foreign exchange transactions are authorised and recorded completely, accurately and within agreed timescales
- Investment and related cash and foreign exchange transactions are settled and failed trades are reported within agreed timescales
- Corporate actions are identified, processed, reported and recorded completely, accurately and within agreed timescales
- Cash receipts and payments are authorised, processed and recorded completely, accurately and within agreed timescales
- Lender and borrower participation in lending programs is authorised and loan initiation, maintenance and termination are accurate and within agreed timescales
- Loans are fully collateralised and the collateral together with its related income is recorded completely, accurately and within agreed timescales

Maintaining financial and other records

- New security master data and changes to existing security master data are authorised and recorded completely and accurately
- Investment income and related tax reclaims are collected and accurately recorded and within agreed timescales
- Investments with observable prices are accurately valued using prices obtained from independent external pricing sources and portfolio valuations are complete and distributed within agreed timescales

- Investments without independently available observable prices or prices where only a single pricing source is available are valued according to approved pricing policies and, where necessary, using approved pricing models, assumptions and inputs
- Cash and investment positions for securities held by third parties (including sub custodians and depositories) are completely and accurately recorded and reconciled to third party data within agreed timescales

Safeguarding assets

- Physically held securities are safeguarded from loss, misappropriation and unauthorised use

Managing and monitoring compliance and outsourcing

- Sub-custodians are approved prior to initiating any custody activity
- Outsourced activities provided by Subservice Organisations are governed by contracts and service level agreements that are authorised and subject to regular review
- The services provided by Subservice Organisations are regularly monitored and assessed against the standards set out in the service level agreements
- Errors are identified, reported to clients and resolved in accordance with established policies

Reporting to clients

- Client reporting in respect of client cash and investment holdings is complete and accurate and provided within agreed timescales
- Cash and investment positions and details of securities lent are reported to interested parties accurately and within agreed timescales

Information technology

See Appendix 1 (k)

(B) FIDUCIARY MANAGEMENT

Accepting clients

- New fiduciary management agreements and amendments are authorised prior to initiating fiduciary management activities
- Client details, accounts, investment guidelines and restrictions are completely and accurately set up onto relevant systems prior to initiating fiduciary management activity

Authorising and processing transactions

- Investment strategy is set in accordance with the fiduciary management agreement and implemented within agreed timescales
- Third party asset managers are identified, selected and approved before prospective asset managers and their related investments are proposed to the client
- Complete and authorised third party asset manager agreements are operative prior to initiating investment activity
- Investment and related cash and foreign exchange transactions are properly authorised, monitored for execution and recorded in a timely and accurate manner
- Manager transition costs are monitored
- Liquidity levels are maintained and monitored in accordance with the fiduciary management agreements

Maintaining financial and other records

- Investments by third party asset managers are monitored for compliance with the clients' required valuation methodologies
- Cash and investment positions are completely and accurately recorded and reconciled to third party data
- Management fees and other account expenses are accurately calculated and recorded where required by the fiduciary management agreements

Managing and monitoring compliance and outsourcing

- Client portfolios are managed in accordance with investment objectives and monitored for compliance with investment guidelines and restrictions
- Outsourced activities provided by Subservice Organisations are governed by contracts and service level agreements that are authorised and subject to regular review and conflicts of interest are identified to clients
- The services provided by Subservice Organisations are regularly monitored and assessed against the standards set out in the service level agreements
- Transaction errors (including guideline breaches, trading errors and client reporting errors) are identified, reported to clients and resolved in accordance with established policies
- Ongoing due diligence monitoring is performed on third party asset managers in accordance with agreed timescales

Reporting to clients

- Client reporting in respect of strategic asset allocations, performance and management fees is complete and accurate and provided within agreed timescales

Information technology

See Appendix 1 (k)

(C) FUND ACCOUNTING

Accepting clients

- New client agreements and amendments are authorised prior to initiating fund accounting activity
- Fund details, including accounting and unitholder records, are completely and accurately set up onto relevant systems prior to initiating fund accounting activity
- Opening balances for client take-ons, including in specie transfers, are completely and accurately recorded and communicated to clients in line with client instructions

Authorising and processing transactions

- Investment, related cash and foreign exchange transactions are completely and accurately recorded within agreed timescales
- Corporate actions are processed, and recorded completely, accurately and within required timescales

Maintaining financial and other records

- New security master data and changes to existing security master data are authorised and recorded completely and accurately
- Investment income and related tax reclaims are completely and accurately recorded in the proper period
- Investments with observable prices are accurately valued using prices obtained from independent external pricing sources
- Investments without independently available observable prices or prices where only a single pricing source is available are valued according to approved pricing policies and, where necessary, using approved pricing models, assumptions and inputs
- Cash and investment positions are completely and accurately recorded and reconciled to third party data
- Expenses are identified and accurately recorded in accordance with the agreed client requirements and timescales
- Fund net asset values are completely and accurately calculated and reported in accordance with agreed timescales
- Issues and cancellations of shares/units are completely and accurately recorded and shares/units are regularly reconciled
- Distributions are accurately calculated and recorded within agreed timescales

Reporting to clients

- Periodic reports to fund governing bodies are accurate, complete and distributed in accordance with agreed timescales

Information technology

See Appendix 1 (k)

Illustrative supplementary control objectives:

Managing and monitoring compliance and outsourcing

- Outsourced activities provided by Subservice Organisations are governed by contracts and service level agreements that are authorised and subject to regular review
- The services provided by Subservice Organisations are regularly monitored and assessed against the standards set out in the service level agreements

Reporting to clients

- Interim and annual reports and accounts are prepared completely, accurately and within required timescales

(D) INVESTMENT MANAGEMENT

Accepting clients

- New client agreements and amendments, including investment guidelines and restrictions, are authorised prior to initiating investment activity
- Client details, accounts, investment guidelines and restrictions are completely and accurately set up onto relevant systems prior to initiating investment activity
- Opening balances for client take-ons, including in-specie transfers, are completely and accurately recorded and communicated to clients in line with client instructions

Authorising and processing transactions

- Investment transactions are authorised, executed and allocated accurately within agreed timescales
- Transactions are only undertaken with approved counterparties
- Transaction costs are authorised, calculated accurately and reviewed
- Investment and related foreign exchange and cash transactions are completely and accurately recorded and communicated for settlement within agreed timescales
- Corporate actions are processed and recorded completely, accurately and within agreed timescales
- Voluntary corporate actions are authorised
- Client new monies and withdrawals are identified, processed, reported and recorded completely and accurately; withdrawals are appropriately authorised

Maintaining financial and other records

- New security master data and changes to existing security master data are authorised and recorded completely and accurately
- Investment income and related tax reclaims are completely and accurately recorded in the proper period
- Investments with observable prices are accurately valued using prices obtained from independent external pricing sources
- Investments without independently available observable prices or prices where only a single pricing source is available are valued according to approved pricing policies and, where necessary, using approved pricing models, assumptions and inputs
- Cash and investment positions are completely and accurately recorded and reconciled to third party data
- Investments are accurately registered, and cash is segregated from that of the investment manager
- Investment management and performance fees and other account expenses are accurately calculated and recorded

Safeguarding of assets

- Cash is managed with regard to diversification of risk and security of funds

Managing and monitoring compliance and outsourcing

- Client investments and cash are managed in accordance with investment objectives and monitored for compliance with investment guidelines and restrictions
- Transaction errors (including guideline breaches, trading errors and client reporting errors) are identified, reported to clients and resolved in accordance with established policies
- Counterparty exposures are monitored for compliance with the firm's limits and guidelines
- Outsourced activities provided by Subservice Organisations are governed by contracts and service level agreements that are authorised and subject to regular review
- The services provided by Subservice Organisations are regularly monitored and assessed against the standards set out in the service level agreements

Reporting to clients

- Client reporting in respect of portfolio valuation, transactions, holdings and income is complete and accurate and provided within agreed timescales

Information technology

See Appendix 1 (k)

Illustrative supplementary control objectives:

Authorising and processing transactions

- Changes to model configuration and parameters used to generate trades for quantitative strategies are tested and approved prior to implementation

Maintaining financial and other records

- Pooled fund unitholder activity is recorded completely, accurately and within agreed timescales
- Net asset values for pooled funds are calculated and recorded completely, accurately and within agreed timescales

Safeguarding of assets

- Fund liquidity is managed with due regard to fund liabilities and investor redemptions

(E) INVESTMENT ADMINISTRATION

Accepting clients

- New client agreements and amendments are authorised prior to initiating investment administration activity
- Client details and accounts are completely and accurately set up onto relevant systems prior to initiating investment administration activity
- Opening balances for client take-ons, including in specie transfers, are completely and accurately recorded and communicated to clients in line with client instructions

Authorising and processing transactions

- Investment transactions are authorised, executed and allocated accurately within agreed timescales
- Corporate actions are processed and recorded completely, accurately and within required timescales
- Voluntary corporate actions are authorised
- Client new monies and withdrawals are processed and recorded completely and accurately; withdrawals are appropriately authorised

Maintaining financial and other records

- Investment income and related tax reclaims are completely and accurately recorded in the proper period
- Investments with observable prices are accurately valued using prices obtained from independent external pricing sources
- Investments without independently available observable prices or prices where only a single pricing source is available are valued according to approved pricing policies and, where necessary, using approved pricing models, assumptions and inputs
- Cash and investment positions are completely and accurately recorded and reconciled to third party data
- Expenses are identified and accurately recorded in accordance with the agreed client requirements and timescales

Managing and monitoring compliance and outsourcing

- Outsourced activities provided by Subservice Organisations are governed by contracts and service level agreements that are authorised and subject to regular review
- The services provided by Subservice Organisations are regularly monitored and assessed against the standards set out in the service level agreements

Reporting to clients

- Periodic reports to clients and their customers are accurate, complete and distributed within agreed timescales

Information technology

See Appendix 1 (k)

Illustrative supplementary control objectives:

Maintaining financial and other records

- Pooled funds are priced and administered accurately and within agreed timescales

(F) PENSION ADMINISTRATION

Accepting clients

- New client agreements and amendments are authorised prior to initiating pension administration activity
- Pension scheme member details and accounts are completely and accurately set up onto relevant systems in accordance with the scheme rules and individual elections
- Opening balances for client take-ons are completely and accurately recorded and communicated to clients in line with client instructions

Authorising and processing transactions

- Contributions and transfers-in received, and where applicable allocation of members' funds to investment options are processed completely, accurately and within agreed timescales
- Switches of members' funds between investment options and other rebalancing transactions are processed completely, accurately and within agreed timescales
- Benefits payable and transfer values are calculated in accordance with scheme rules and relevant legislation and are paid within agreed timescales

Maintaining financial and other records

- Member records consist of up-to-date and accurate information
- Requests to change member records are validated for authenticity
- Contributions and benefit payments are completely and accurately recorded in the proper period
- Investment transactions, balances and related income are completely and accurately recorded in the proper period

Safeguarding assets

- Member records are securely held and access is restricted to authorised individuals
- Cash in scheme bank accounts is safeguarded and payments are suitably authorised

Managing and monitoring compliance and outsourcing

- Receipts of contributions are monitored against required timescales
- Pensions administration activities are governed by service level agreements that are authorised and subject to regular review. Service performance is regularly monitored and assessed against the standards set out in service level agreements.
- Transaction errors are identified, reported to clients and resolved in accordance with established policies

Reporting to clients

- Periodic reports to participants and scheme trustees are complete, accurate, and provided within required timescales

Information technology

See Appendix 1 (k)

Illustrative supplementary control objectives:

Managing and monitoring compliance and outsourcing

- Receipt of contributions, in accordance with schemes rules and legislative requirements, are monitored
- Periodic reports to The Pensions Regulator and HMRC are complete and accurate

Reporting to clients

- Annual reports and accounts prepared for pension schemes are complete, accurate and provided within required timescales

(G) PRIVATE EQUITY

Accepting clients

- New funds are properly developed and authorised, and take account of legal and tax requirements
- Relevant take on procedures have been performed for each of the investors prior to acceptance, including AML and KYC considerations
- Policies on investments (for example investment selection, investment governance, valuations, monitoring and oversight) are properly established and communicated to investors prior to any investment activity

Authorising and processing investment transactions

- Pre investment: investment decisions are researched and documented in accordance with the firm's stated investment strategy and the approvals follow the firm's investment governance procedures
- Diligence and abort costs are controlled following the firm's documented procedures and communicated to investors
- Post investment: rights and obligations of the investment are recorded and maintained. Where contingent consideration arrangements exists for a transaction, these are monitored and tracked appropriately
- Investment and related cash transactions are completely and accurately recorded and communicated for settlement within agreed timescales
- Rights and obligations are recorded and monitored until exit

Maintaining financial and other records

- Investment income and related tax reclaims are completely and accurately recorded in line with relevant accounting standards within the proper period
- Investments without independently available observable prices or prices where only a single pricing source is available are valued according to approved pricing policies and, where necessary, using approved pricing models, assumption and inputs
- Investor drawdowns and distributions are authorised, processed and recorded completely and accurately
- Changes to data in relation to investors (subscription amounts, bank information, correspondence address, key contacts) are approved
- Investment management fees and expenses of the funds are authorised, accurately calculated, recorded and allocated in accordance with the fund's legal documentation
- Cash and investment positions are completely and accurately recorded and reconciled to third party data or documents of title held

Managing and monitoring compliance and outsourcing

- Investment performance and conflicts of interest arising from new or ongoing investments are appropriately monitored, assessed and reported in line with policy
- Client investments and cash are managed in accordance with investment objectives and monitored for compliance with policies on investment and any identified errors are resolved in accordance with established policies

- Outsourced activities provided by Subservice Organisations are governed by contracts and service level agreements that are authorised and subject to regular review
- The services provided by Subservice Organisations are regularly monitored and assessed against the standards set out in the service level agreements

Reporting to clients

- Investor reporting is complete and accurate and provided within agreed timescales

Information technology

See Appendix 1 (k)

Illustrative supplementary control objectives:

Accepting clients

- Changes to investors after fund investment closures are communicated to relevant investors and fund equalisations are performed in line with the relevant agreements

Authorising and processing investment transactions

- Investment allocations are made in accordance with the terms of the partnership or supporting agreements
- Investment transactions and commitments are properly authorised and executed completely and accurately in a timely manner (this is intended to include acquisitions and exits)

Maintaining financial and other records

- Carried interest payment and other one-off expenses of the funds are authorised, accurately calculated, recorded and allocated in accordance with the fund's legal documentation and are independently verified

(H) PROPERTY INVESTMENT MANAGEMENT[9]

Accepting clients

- New client agreements and amendments, including investment guidelines and restrictions, are authorised prior to initiating investment activity
- Client details, accounts, investment guidelines and restrictions are completely and accurately set up onto relevant systems prior to initiating investment activity
- Opening balances for client take-ons are completely and accurately recorded and communicated to clients in line with client instructions

Authorising and processing transactions

- Property purchases, sales and developments are authorised and implemented in accordance with investment guidelines and restrictions
- Costs associated with buying, selling and/or developing properties are authorised and recorded completely and accurately and are monitored
- Client new monies and withdrawals are processed and recorded completely and accurately; withdrawals are appropriately authorised
- Properties are insured against loss or damage

Maintaining financial and other records

- New property master data and changes to existing property master data including records related to ownership, tenant and lease information is recorded completely and accurately
- Property and related cash transactions are completely and accurately recorded
- Valuations are undertaken, reviewed and recorded completely and accurately in accordance with client requirements
- Property investment management fees and performance fees are accurately calculated and recorded
- Cash is completely and accurately recorded and reconciled to third party data
- Property investments are accurately registered and cash is segregated

Safeguarding of assets

- Fund liquidity is managed with due regard to fund liabilities and investor redemptions

Managing and monitoring compliance and outsourcing

- Investments and cash are managed in accordance with investment objectives and monitored for compliance with guidelines and restrictions
- Transaction and client reporting errors are identified, reported to clients and resolved in accordance with established policies

[9] This does not cover REITs and PUTs.

- Outsourced activities provided by Subservice Organisations are governed by contracts and service level agreements that are authorised and subject to regular review
- The services provided by Subservice Organisations are regularly monitored and assessed against the standards set out in the service level agreements

Reporting to clients

- Client reporting in respect of property transactions, holdings, valuations and income is complete and accurate and provided within agreed timescales

Information technology

See Appendix 1 (k)

Illustrative supplementary control objectives:

Maintaining financial and other records

- Rental income, service charges and other property expenses are accurately calculated and recorded within the proper period

(I) PROPERTY INVESTMENT ADMINISTRATION[10]

Accepting clients

- New client agreements and amendments are authorised prior to initiating property administration activity
- Client details, accounts and property related information are completely and accurately set up onto relevant systems prior to initiating property administration activity
- Opening balances for client take-ons are accurately recorded and communicated to clients in line with client instructions

Authorising and processing transactions

- New tenancy agreements and leases are authorised and in place prior to occupation
- Changes to tenancy agreements and leases are reviewed within agreed timescales and are authorised
- Rents are reviewed in accordance with tenancy agreements and the outcome of the reviews are approved, recorded, and processed completely, accurately and in the proper period
- Service charges are completely and accurately calculated and are approved
- Suppliers of property services are approved in accordance with administration agreements where applicable

Maintaining financial and other records

- New property master data and changes to existing property master data including records related to ownership, tenant and lease information is recorded completely and accurately
- Property income and related tax are completely and accurately recorded in the proper period and collected within agreed timescales
- Service charges are recorded within the proper period and collected in accordance with tenancy agreements
- Payments are authorised, processed and recorded completely and accurately within agreed timescales
- Property management fees and other property expenses are completely and accurately calculated and recorded
- Disbursements to clients are authorised, processed and recorded completely and accurately within agreed timescales
- Cash relating to property management is completely and accurately recorded and reconciled to third party data

Managing and monitoring compliance and outsourcing

- Transaction errors are identified, reported to clients and resolved in accordance with established policies
- Outsourced activities provided by Subservice Organisations are governed by contracts and service level agreements that are authorised and subject to regular review

[10] This includes work undertaken by managing agents.

- The services provided by Subservice Organisations are regularly monitored and assessed against the standards set out in the service level agreements

Reporting to clients

- Client reporting in respect of property transactions, holdings and income is complete and accurate and provided within agreed timescales

Information technology

See Appendix 1 (k)

(J) TRANSFER AGENCY

Accepting clients

- New client agreements and amendments are authorised prior to accepting end investor subscriptions
- Client details and accounts are set up and administered in accordance with client agreements and applicable regulations prior to accepting end investor subscriptions
- End investor details, accounts, subscription limits and restrictions are completely and accurately set up onto relevant systems and in accordance with the requirements of fund policies and applicable regulation prior to accepting end investor subscriptions
- Adherence to applicable subscription limits is checked in advance of the completion of subscription transactions
- Opening end investor balances for client take-ons, are completely and accurately recorded and communicated to clients in line with client instructions

Authorising and processing transactions

- Subscription and redemption documentation and end investor identity are validated
- Subscriptions, redemptions and related adjustments are authorised and processed completely and accurately within agreed timescales
- Cash receipts and payments are processed accurately, completely and within agreed timescales
- Subscription and redemption confirmations are produced and distributed accurately, completely and within agreed timescales

Maintaining financial and other records

- Transfer agent records completely and accurately reflect securities and cash held by custodians
- Subscriptions and redemptions are recorded completely and accurately and units are regularly reconciled
- Distributions are accurately calculated, authorised , completely and accurately recorded and paid within agreed timescales

Managing and monitoring compliance and outsourcing

- Transaction and client reporting errors are identified, reported to clients and rectified in accordance with established policies
- Outsourced activities provided by Subservice Organisations are governed by contracts and service level agreements that are authorised and subject to regular review
- The services provided by Subservice Organisations are regularly monitored and assessed against the standards set out in the service level agreements

Reporting to clients

- End investor and fund reporting in respect of transactions and holdings is complete and accurate and provided within required timescales

Information technology

See Appendix 1 (k)

Illustrative supplementary control objective:

Managing and monitoring compliance and outsourcing

- Compensation payments are authorised, accurately calculated and approved in accordance with fund policies

(K) INFORMATION TECHNOLOGY

Restricting access to systems and data

- Physical access[11] to In-scope systems is restricted to authorised individuals
- Logical access to In-scope systems and data is restricted to authorised individuals in accordance with job roles and/or business requirements
- Client and third party access[12] to In-scope systems and data[13] is restricted and/or monitored
- Segregation of incompatible duties within and across business and technology functions is formally defined[14], implemented[15], updated and enforced by logical security controls

Maintaining integrity of the systems

- Scheduling and internal processing of data is complete, accurate and within agreed timescales[16]
- Transmission of data to/from external parties is complete, accurate, executed within agreed timescales and secure[17] in line with external party agreements
- Network perimeter security devices[18] are installed and changes are tested and approved
- Anti-virus definitions are periodically updated across all terminals and servers, deployment and settings are periodically reviewed and updated when required; and patterns of attempted external breaches are monitored
- Data received from external parties[19] is scanned for known vulnerabilities, any compromised data is quarantined and definitions of threats are periodically updated

Maintaining and developing systems hardware and software

- Development and implementation of both in house and third party In-scope systems are authorised, tested and approved
- Data migration or modification is authorised, tested and, once performed, reconciled back to the source data
- Changes to existing In-scope systems, including hardware upgrades, software patches and direct configuration changes, are authorised, tested and approved in line with policy[20]

[11] Physical access may include access to server rooms and office floor space with desktops, that hold application hardware and facilities that house cloud hardware holding relevant data.

[12] Third party access relates to access that is not directly by employees, such as clients' customers, contractors, vendors etc.

[13] This includes both where systems and data are maintained / held in-house and also where systems and data are maintained / held externally.

[14] Management have formalised and documented which roles and privileges are incompatible.

[15] Management have documented which functions and privileges each role is approved to perform and which, per the defined segregation of incompatible duties, are not permitted to perform.

[16] This is to distinguish from the data transmissions control activities. This control activity aims to cover the completeness and accuracy of job schedules.

[17] E.g., encryption, dedicated lease lines and not just password protected files.

[18] This may include firewalls, anti-malware and intrusion detection technology.

[19] This may include mechanisms such as email, dedicated interfaces, file transfer protocol and via any removable media.

[20] This is to consider all types of change management methodologies in addition to normal change processes (e.g. standard and emergency changes).

Recovering from processing interruptions

- IT related Disaster Recovery Plans are documented, updated, approved and tested
- In-scope systems and data are backed up and tested such that they can be restored completely and within agreed timescales
- Problems and incidents relating to In-scope systems are identified and resolved within agreed timescales

Managing and monitoring compliance and outsourcing

- Outsourced activities provided by Subservice Organisations are governed by contracts and service level agreements that are authorised and subject to regular review
- The services provided by Subservice Organisations are regularly monitored and assessed against the standards set out in the service level agreements

Illustrative supplementary control objectives:

Recovering from processing interruptions

- Performance and capacity of In-scope systems are monitored and issues are resolved
- The physical IT equipment is maintained in a controlled environment

Appendix 2: example management statement

A. TYPE 1

Statement by the Senior Management of [name of Service Organisation]

As Senior Management of [name of Service Organisation] ('the Service Organisation') we are responsible for the identification of Control Objectives relating to the provision of [identify activity, eg, 'custody services and related information technology'] by the Service Organisation and the design, implementation and operation of the Service Organisation's Control Activities to provide reasonable assurance that the Control Objectives are achieved.

In carrying out those responsibilities we have regard not only to the interests of User Entities but also to those of the owners of the business and the general effectiveness and efficiency of the relevant operations.

The accompanying description has been prepared for User Entities who have used the [identify activity, eg, 'custody services and related information technology'] and their auditors who have a sufficient understanding to consider the description, along with other information including information about Control Activities operated by User Entities themselves.

We have evaluated the fairness of the description and the design suitability of the Service Organisation's Control Activities in accordance with the Technical Release AAF 01/20 ('AAF 01/20'), issued by the Institute of Chartered Accountants in England and Wales, and the Control Objectives for [identify activities, eg, 'custody and information technology'] set out in AAF 01/20 [and the International Standard on Assurance Engagements 3402 ('ISAE 3402')[21], issued by the International Auditing and Assurance Standards Board].

We confirm that:

a. The accompanying description in sections [a to b] fairly presents the Service Organisation's [identify activity, eg, 'custody'] services as at [date]. In addition to the Control Objectives specified in AAF 01/20, the criteria used in making this statement were that the accompanying description:

    i. Presents how the services were designed and implemented, including: the types of services provided, and as appropriate, the nature of transactions processed; the procedures, both automated and manual, by which User Entities' transactions were initiated, recorded and processed; the accounting records and related data that were maintained, reported and corrected as necessary; the system which captured and addressed significant events and conditions, other than User Entities' transactions; and other aspects of our control environment, risk assessment process, monitoring and information and communication systems, that were relevant to our Control Activities; and

    ii. Does not omit or distort information relevant to the scope of the services being described, while acknowledging that the description is prepared to meet the common needs of a broad range of User Entities and their auditors and may not, therefore, include every aspect of the services that each individual User Entity may consider important in its own particular environment.

b. The Control Activities related to the Control Objectives stated in the accompanying Description were suitably designed. The criteria used in making this statement were that:

    i. The risks that threatened achievement of the Control Objectives stated in the Description were identified; and

    ii. The identified Control Activities would, if operated as described, provide reasonable assurance that those risks did not prevent the stated Control Objectives from being achieved.

Authorised Signatory

[name of Service Organisation]

[date]

[21] Dual reporting under the International Standard on Assurance Engagements 3402 is optional.

Further guidance

In the following instances Senior Management highlight in the Management Statement omissions of and material modifications to control objectives, or where there is a qualified opinion:

- Where Control Objectives specified in this guidance have been omitted from the Report, the Management Statement sets out the Control Objectives that have been omitted and provides the reasons why they are not considered relevant to User Organisations.
- Where Control Objectives specified in this guidance have been materially modified, the Management Statement sets out the Control Objectives that have been materially modified and provides the reasons why.
- Where the use of Subservice Organisations has been omitted from the Report, the Management Statement sets out the services provided by each of the Subservice Organisations that have been omitted from the Description (where the Carve-out Method has been applied) or the Control Activities undertaken by Subservice Organisations that have been omitted from the Report (where the Inclusive Method has been applied) and provide the reasons why they are not considered relevant to User Organisations.
- Where the Service Auditor has qualified their opinion (i.e. qualification or adverse), the Management Statement sets out the facts and circumstances, cross referring to the Service Auditor's Report and the relevant sections of the Report.

B. TYPE 2

Statement by the Senior Management of [name of Service Organisation]

As Senior Management of [name of Service Organisation] ('the Service Organisation') we are responsible for the identification of Control Objectives relating to the provision of [identify activity, eg, 'custody services and related information technology'] by the Service Organisation and the design, implementation and operation of the Service Organisation's Control Activities to provide reasonable assurance that the Control Objectives are achieved.

In carrying out those responsibilities we have regard not only to the interests of User Entities but also to those of the owners of the business and the general effectiveness and efficiency of the relevant operations.

The accompanying description has been prepared for User Entities who have used the [identify activity, eg, 'custody services and related information technology'] and their auditors who have a sufficient understanding to consider the description, along with other information including information about Control Activities operated by User Entities themselves.

We have evaluated the fairness of the description and the design suitability of the Service Organisation's Control Activities in accordance with the Technical Release AAF 01/20 ('AAF 01/20'), issued by the Institute of Chartered Accountants in England and Wales, and the Control Objectives for [identify activities, eg, 'custody and information technology'] set out in AAF 01/20 [and the International Standard on Assurance Engagements 3402 ('ISAE 3402')[22], issued by the International Auditing and Assurance Standards Board].

We confirm that:

a. The accompanying description in sections [a to b] fairly presents the Service Organisation's [identify activity, eg, 'custody'] services throughout the period [date] to [date]. In addition to the Control Objectives specified in AAF 01/20, the criteria used in making this statement were that the accompanying description:

[22] Dual reporting under the International Standard on Assurance Engagements 3402 is optional.

i. Presents how the services were designed and implemented, including: the types of services provided, and as appropriate, the nature of transactions processed; the procedures, both automated and manual, by which User Entities' transactions were initiated, recorded and processed; the accounting records and related data that were maintained, reported and corrected as necessary; the system which captured and addressed significant events and conditions, other than User Entities' transactions; and other aspects of our control environment, risk assessment process, monitoring and information and communication systems, that were relevant to our Control Activities; and

ii. Includes relevant details of changes to the Service Organisation's system during the period; and

iii. Does not omit or distort information relevant to the scope of the services being described, while acknowledging that the description is prepared to meet the common needs of a broad range of User Entities and their auditors and may not, therefore, include every aspect of the services that each individual User Entity may consider important in its own particular environment.

b. The Control Activities related to the Control Objectives stated in the accompanying Description were suitably designed and operated effectively throughout the period [date] to [date]. The criteria used in making this statement were that:

i. The risks that threatened achievement of the Control Objectives stated in the Description were identified; and

ii. The identified Control Activities would, if operated as described, provide reasonable assurance that those risks did not prevent the stated Control Objectives from being achieved; and

iii. The Control Activities were consistently applied as designed.

Authorised Signatory

[name of Service Organisation]

[date]

Further guidance

In the following instances Senior Management highlight in the Management Statement omissions of and material modifications to control objectives, or where there is a qualified opinion:

- Where Control Objectives specified in this guidance have been omitted from the Report, the Management Statement sets out the Control Objectives that have been omitted and provides the reasons why they are not considered relevant to User Organisations.
- Where Control Objectives specified in this guidance have been materially modified, the Management Statement sets out the Control Objectives that have been materially modified and provides the reasons why.
- Where the use of Subservice Organisations has been omitted from the Report, the Management Statement sets out the services provided by each of the Subservice Organisations that have been omitted from the Description (where the Carve-out Method has been applied) or the Control Activities undertaken by Subservice Organisations that have been omitted from the Report (where the Inclusive Method has been applied) and provide the reasons why they are not considered relevant to User Organisations.
- Where the Service Auditor has qualified their opinion (i.e. qualification or adverse), the Management Statement sets out the facts and circumstances, cross referring to the Service Auditor's Report and the relevant sections of the Report.

Appendix 3: example service auditor's report

A. TYPE 1

Independent Service Auditor's assurance report on Control Activities at [Insert name of Service Organisation] (the 'Service Organisation')

To the Senior Management of [Insert name of Service Organisation]

Scope

We have been engaged to report on [Insert name of Service Organisation]'s [and [insert name of Subservice Organisation]'s] Description of its [describe Service Organisation's activity, eg, custody services and related information technology] at [date] [on pages /in sections] (the 'Description'), and on the suitability of the design of Control Activities to achieve the related Control Objectives.

[Name of Subservice Organisation] (the 'included Subservice Organisation') is an independent Service Organisation that provides [type of subservice eg, information technology] to the Service Organisation. The Service Organisation's Description includes a description of the included Subservice Organisation's [type of subservice eg, information technology] system used by the Service Organisation to provide [nature of service activity eg, custody services] to its User Entities, as well as relevant Control Objectives and Control Activities of the included Subservice Organisation.]

[The Service Organisation uses a [type of subservice] Service Organisation (the 'Subservice Organisation[s]') for its [type of subservice activity eg, information technology]. The Description includes only the Control Activities and related Control Objectives of the Service Organisation and excludes the Control Objectives and related Control Activities of the [type of subservice eg, information technology] Subservice Organisation[s]. Our examination did not extend to Control Activities of the [type of subservice eg, information technology] Subservice Organisation[s].]

[The Description indicates that certain Control Objectives specified in the Description can be achieved only if Complementary User Entity Controls contemplated in the design of the Service Organisation's Control Activities are suitably designed and operating effectively, along with related Control Activities at the Service Organisation. We have not evaluated the suitability of the design or operating effectiveness of such Complementary User Entity Controls.]

While the Control Activities and related Control Objectives may be informed by the Service Organisation's need to satisfy legal or regulatory requirements, our scope of work and our conclusions do not constitute assurance over compliance with those laws and regulations.

The Service Organisation's [and the included Subservice Organisation's] responsibilities

The Service Organisation [and the included Subservice Organisation] [is/are] responsible for: preparing the Description [on pages /in sections] and the accompanying Management Statement[s] set out [on/in] [page/section], including the completeness, accuracy and method of presentation of the Description and the Management Statement[s]; providing the [Service Organisation's activities, eg, custody services and related information technology] covered by the Description; specifying the Criteria and stating them in the Description; identifying the risks that threaten the achievement of the Control Objectives; and designing and implementing Control Activities to achieve the stated Control Objectives.

The Control Objectives stated in the Description [on pages/in sections] include the internal Control Objectives developed for [Service Organisation's activities eg, custody and related information technology] as set out in ICAEW Technical Release AAF 01/20 [except where stated otherwise].

Our Independence and Quality Control

In carrying out our work, we complied with the Institute of Chartered Accountants in England and Wales (ICAEW) Code of Ethics, which includes independence and other requirements founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour. We also apply International Standard on Quality Control (UK) 1 and accordingly maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Service Auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design of the Control Activities to achieve the related Control Objectives stated in that Description based on our procedures. We conducted our engagement in accordance with International Standards on Assurance Engagements 3000 (Revised) [International Standards on Assurance Engagements 3402] and ICAEW Technical Release AAF 01/20. Those standards and guidance require that we comply with ethical requirements and plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the Description is fairly presented and the Control Activities were suitably designed to achieve the related Control Objectives stated in the Description.

An assurance engagement to report on the Description and design of Control Activities at a Service Organisation involves performing procedures to obtain evidence about the presentation of the Description and the suitability of design of the Control Activities. Our procedures included assessing the risks that the Description is not fairly presented and that the Control Activities were not suitably designed to achieve the related Control Objectives stated in the Description. We did not perform any procedures regarding the operating effectiveness of Control Activities, and therefore no opinion is expressed thereon. An assurance engagement of this type also includes evaluating the overall presentation of the Description and the suitability of the Control Objectives stated therein.

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

Inherent limitations

The Service Organisation's [and the included Subservice Organisation's] Description is prepared to meet the common needs of a broad range of User Entities and their auditors ('User Organisations') and may not, therefore, include every aspect of the Service Organisation's [and the included Subservice Organisation's] activities that each individual User Entity may consider important in its own particular environment. Also, because of their nature, Control Activities at a Service Organisation [or Subservice Organisation] may not prevent or detect and correct all errors or omissions in processing or reporting transactions. Our opinion is based on historical information and the projection to future periods of any evaluation of the fairness of the presentation of the Description, or the suitability of the design or operating effectiveness of the Control Activities would be inappropriate.

Opinion

In our opinion, in all material respects, based on the Criteria described in the Service Organisation's [and the included Subservice Organisation's] Management Statement[s] [on page/ in section]:

(a) the Description [on pages/in sections] fairly presents the Service Organisation's [and the included Subservice Organisation's] [activities, eg, custody services and related information technology] as designed and implemented at [date]; and

(b) the Control Activities related to the Control Objectives stated in the Description were suitably designed to provide reasonable assurance that the specified Control Objectives would be achieved if the described Control Activities operated effectively at [date] [and User Entities applied the Complementary User Entity Controls referred to in the scope paragraph of this assurance report].

[Other information

The information included in [pages/section] describing the Service Organisation's [identify elements of the description of controls not covered by the assurance report eg, business continuity planning] is presented by the Service Organisation to provide additional information and is not part of the Service Organisation's description of Control Activities that may be relevant to User Entities' internal control. Such information has not been subjected to the procedures applied in the examination of the Description of the Service Organisation, related to the [activity, eg, custody services], and accordingly, we express no opinion on it.]

Use of our report

This report is made solely for the use of the Service Organisation and solely for the purpose of reporting on the Control Activities of the Service Organisation [and the included Subservice Organisation], in accordance with the terms of our engagement letter dated [date] (the 'agreement').

Our report must not be recited or referred to in whole or in part in any other document nor made available, copied or recited to any other party, in any circumstances, without our express prior written permission. We permit the disclosure of this report, in full only, including the description of tests of Control Activities and results thereof by the Service Organisation at its discretion to User Entities using its [activity, eg, custody services] and to the auditors of such User Entities, to enable User Organisations to verify that a Service Auditor's Report has been commissioned by the Service Organisation and issued in connection with the Control Activities of the Service Organisation [and the included Subservice Organisation], and without assuming or accepting any responsibility or liability to User Organisations on our part.

To the fullest extent permitted by law, we do not accept or assume responsibility to anyone other than the Service Organisation for our work, for this report, or for the opinions we have formed.

Chartered Accountants

[Office Location]

[Date]

B. TYPE 2

Independent Service Auditor's assurance report on Control Activities at [Insert name of Service Organisation] (the 'Service Organisation')

To the Senior Management of [Insert name of Service Organisation]

Scope

We have been engaged to report on [Insert name of Service Organisation]'s [and [insert name of Subservice Organisation]'s] Description of its [describe Service Organisation's activity, eg, custody services and related information technology] throughout the period [date] to [date] [on pages /in sections] (the 'Description'), and on the suitability of the design and operating effectiveness of Control Activities to achieve the related Control Objectives.

[[Name of Subservice Organisation] (the 'included Subservice Organisation') is an independent Service Organisation that provides [type of subservice eg, information technology] to the Service Organisation. The Service Organisation's Description includes a description of the included Subservice Organisation's [type of subservice eg, information technology] system used by the Service Organisation to provide [nature of service activity eg, custody services] to its User Entities, as well as relevant Control Objectives and Control Activities of the included Subservice Organisation.]

[The Service Organisation uses a [type of subservice] Service Organisation (the 'Subservice Organisation[s]') for its [type of subservice activity eg, information technology]. The Description includes only the Control Activities and related Control Objectives of the Service Organisation and excludes the Control Objectives and related Control Activities of the [type of subservice eg, information technology] Subservice Organisation[s]. Our examination did not extend to Control Activities of the [type of subservice eg, information technology] Subservice Organisation[s].]

[The Description indicates that certain Control Objectives specified in the Description can be achieved only if Complementary User Entity Controls contemplated in the design of the Service Organisation's Control Activities are suitably designed and operating effectively, along with related Control Activities at the Service Organisation. We have not evaluated the suitability of the design or operating effectiveness of such Complementary User Entity Controls.]

While the Control Activities and related Control Objectives may be informed by the Service Organisation's need to satisfy legal or regulatory requirements, our scope of work and our conclusions do not constitute assurance over compliance with those laws and regulations.

The Service Organisation's [and the included Subservice Organisation's] responsibilities

The Service Organisation [and the included Subservice Organisation] [is/are] responsible for: preparing the Description [on pages /in sections] and the accompanying Management Statement[s] set out [on/in] [page/section] [a], including the completeness, accuracy and method of presentation of the Description and the Management Statement[s]; providing the [Service Organisation's activities, eg, custody services and related information technology] covered by the Description; specifying the Criteria and stating them in the Description; identifying the risks that threaten the achievement of the Control Objectives; and designing, implementing and effectively operating Control Activities to achieve the stated Control Objectives.

The Control Objectives stated in the Description [on pages /in sections] include the internal Control Objectives developed for [Service Organisation's activities eg, custody and related information technology] as set out in ICAEW Technical Release AAF 01/20 [except where stated otherwise].

Our Independence and Quality Control

In carrying out our work, we complied with the Institute of Chartered Accountants in England and Wales (ICAEW) Code of Ethics, which includes independence and other requirements founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour. We also apply International Standard on Quality Control (UK) 1 and accordingly maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Service Auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the Control Activities to achieve the related Control Objectives stated in that Description based on our procedures. We conducted our engagement in accordance with International Standards on Assurance Engagements 3000 (Revised) [International Standards on Assurance Engagements 3402] and ICAEW Technical Release AAF 01/20. Those standards and guidance require that we comply with ethical requirements and plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the Description is fairly presented and the Control Activities were suitably designed and operating effectively to achieve the related Control Objectives stated in the Description.

An assurance engagement to report on the Description and design of Control Activities at a Service Organisation involves performing procedures to obtain evidence about the presentation of the Description and the suitability of design of the Control Activities. Our procedures included assessing the risks that the Description is not fairly presented and that the Control Activities were not suitably designed or operating effectively to achieve the related Control Objectives stated in the Description. Our procedures also included testing the operating effectiveness of those Control Activities that we consider necessary to provide reasonable assurance that the related Control Objectives stated in the Description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the Description, the suitability of the Control Objectives stated therein, and the suitability of the Criteria specified by the Service Organisation and described on [page/section].

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

Inherent limitations

The Service Organisation's [and the included Subservice Organisation's] Description is prepared to meet the common needs of a broad range of User Entities and their auditors ('User Organisations') and may not, therefore, include every aspect of the Service Organisation's [and the included Subservice Organisation's] [activities, eg, custody services and information technology] that each individual User Entity may consider important in its own particular environment. Also, because of their nature, Control Activities at a Service Organisation [or Subservice Organisation] may not prevent or detect and correct all errors or omissions in processing or reporting transactions. Our opinion is based on historical information and the projection to future periods of any evaluation of the fairness of the presentation of the Description, or the suitability of the design or operating effectiveness of the Control Activities would be inappropriate.

Opinion

In our opinion, in all material respects, based on the Criteria described in the Service Organisation's [and the included Subservice Organisation's] Management Statement[s] [on page/in section]:

(a) the Description [on pages/in sections] fairly presents the Service Organisation's [and the included Subservice Organisation's] [activities, eg, custody services and related information technology] as designed and implemented throughout the period from [date] to [date];

(b) the Control Activities related to the Control Objectives stated in the Description were suitably designed to provide reasonable assurance that the specified Control Objectives would be achieved if the described Control Activities operated effectively throughout the period [from [date] to [date] [and User Entities applied the Complementary User Entity Controls referred to in the scope paragraph of this assurance report]; and

(c) the Control Activities tested, which [together with the Complementary User Entity Controls referred to in the scope paragraph of this assurance report, if operating effectively,] were operating with sufficient effectiveness to provide reasonable assurance that the Control Objectives stated in the Description were achieved throughout the period from [date] to [date].

Description of tests of Control Activities

The specific Control Activities tested and the nature, timing and results of those tests are detailed on [pages /section].

[Other information

The information included in [pages/section] describing the Service Organisation's [identify elements of the description of controls not covered by the assurance report eg, business continuity planning] is presented by the Service Organisation to provide additional information and is not part of the Service Organisation's description of Control Activities that may be relevant to User Entities' internal control. Such information has not been subjected to the procedures applied in the examination of the Description of the Service Organisation, related to the [activity, eg, custody services], and accordingly, we express no opinion on it.]

Use of our report

This report and the description of tests of Control Activities and results thereof on [pages /section] are made solely for the use of the Service Organisation and solely for the purpose of reporting on the Control Activities of the Service Organisation [and the included Subservice Organisation], in accordance with the terms of our engagement letter dated [date] (the 'agreement').

Our report must not be recited or referred to in whole or in part in any other document nor made available, copied or recited to any other party, in any circumstances, without our express prior written permission. We permit the disclosure of this report, in full only, including the description of tests of Control Activities and results thereof by the Service Organisation at its discretion to User Entities using its [activity, eg, custody services] and to the auditors of such User Entities, to enable User Organisations to verify that a Service Auditor's Report has been commissioned by the Service Organisation and issued in connection with the Control Activities of the Service Organisation [and the included Subservice Organisation], and without assuming or accepting any responsibility or liability to User Organisations on our part.

To the fullest extent permitted by law, we do not accept or assume responsibility to anyone other than the Service Organisation for our work, for this report, or for the opinions we have formed.

Chartered Accountants

[Office Location]

[Date]

Appendix 4: examples of explanatory paragraphs and qualification wording

(A) DESCRIPTION MISSTATEMENTS

Appendix 1 specifies a minimum set of Control Objectives for inclusion in the Report. Exceptionally, in the event that Senior Management do not include a particular Control Objective in their Report then their Management Statement explains the fact and the reasons for the omission. Where Senior Management fail or refuse to disclose the omission, or the Service Auditor considers the justification being unsatisfactory, the Service Auditor discloses the fact and qualifies their opinion. For example:

We draw attention to page [x] of the Report which sets out the control objectives. One of the control objectives, [specify], in Technical Release AAF 01/20, is not included in the management statement and no explanation for the omission is provided.

Except for the matter referred to above concerning the fairness of the description of control activities, in our opinion, ...

The refusal or failure of the directors to amend incomplete or inappropriate descriptions of control activities or control objectives may lead to the description of internal controls being considered not fair. Where the Service Auditor considers that this merits qualification, this might be phrased as follows:

The Report states, on page [x], that cash records are reconciled to bank statements on a daily basis. Our work indicates that whilst this is the procedure for UK bank accounts, reconciliations of overseas accounts are only carried out as and when bank statements are received, which is typically once per month.

Except for the matter referred to above concerning the fairness of the description of control activities, in our opinion, …

(B) DESIGN DEFICIENCIES

Design deficiencies may, for example, result either from a key control being absent or from Control Activities that do not prevent or detect errors as described. The following is an example of wording that may be appropriate where the Service Auditor qualifies their opinion on the design effectiveness due to the absence of a key control.

As explained in the Management Statement, six monthly reconciliations of physical securities held to the books and records are undertaken. The reconciliation procedures did not however include a control for follow up of reconciling items and for independent review and approval of the reconciliations.

Except for the matter referred to above concerning the control design, in our opinion, …

(C) EXCEPTIONS TO OPERATING EFFECTIVENESS

Tests of operating effectiveness carried out by the Service Auditor in relation to specific Control Activities are detailed either (a) adjacent to the relevant Control Activities in the Report or (b) in an appendix to the Service Auditor's Report. Where the results of the tests identify an exception to the Control Activities, this is reported after the test, and the Service Auditor considers whether the exceptions affect the achievement of the Control Objective. Where a Control Objective is not achieved the Service Auditor inserts an explanatory paragraph with appropriate reference and qualifies their opinion. For example:

In the Management Statement it is stated that six monthly reconciliations of physical securities held to the books and records are undertaken and that there is a process for following up reconciling items. Our tests of operating effectiveness indicated that there were a significant number of reconciling items that were not being resolved on a timely basis in accordance with the organisation's policy.

Except for the matter referred to above concerning the operating effectiveness of the control activities, in our opinion, ...

Where the results of the Service Auditor's tests of operational effectiveness and the deficiency have been integrated and fully explained in the Report, the Service Auditor may alternatively consider cross-referring their qualification to where these details may be found. For example:

Except for the matter explained on page [z] concerning the follow up of reconciling items on physical security reconciliations, the control activities tested, as set out [on pages [x] to [y] of the report by the senior management / in the attachment to this report], in our opinion, …

(D) NON-APPLICABLE CONTROL OBJECTIVE

Where the Service Auditor is unable to test Control Activities as a result of those Control Activities not having operated during the reporting period (i.e. an event driven Control Activity), it adds an explanatory paragraph preceding the opinion in the Service Auditor's Report. For example:

The scope of our engagement includes all control objectives and control activities included in the Description with the exception of those set out in section [X] Accepting Clients, [include any other sections where non-applicable control objective applies]. Specifically:

We did not perform any procedures over the control activities in relation to the control objectives:

- *New client agreements and amendments, including investment guidelines and restrictions, are authorised prior to initiating investment activity;*
- *Client details, accounts, investment guidelines and restrictions are completely and accurately set up onto relevant systems prior to initiating investment activity;*
- *Opening balances for client take-ons, including in-specie transfers, are completely and accurately recorded and communicated to clients in line with client instructions;*

since there were no new clients during the period [insert dates].

[Include additional explanatory paragraphs for other event driven controls which did not operate during the period]

Accordingly, we do not express an opinion thereon.

Appendix 5: example extracts from an engagement letter

These extracts are provided for illustrative purposes only. The Service Auditor applies their own judgement to develop suitable wording for their engagement letters to reflect this guidance and their own particular circumstances[23].

RESPONSIBILITIES OF SENIOR MANAGEMENT

Those charged with governance ('Senior Management') of [name of Service Organisation] ('the Service Organisation') in relation to which the Service Auditor's Report is to be provided, are and shall be responsible for the design, implementation and operation of Control Activities that provide adequate level of control over [describe Service Organisation's activity, eg, custody services]. Senior Management's responsibilities are and shall include:

- acceptance of responsibility for internal controls;
- evaluation of the effectiveness of the Service Organisation's Control Activities using suitable Control Objectives;
- supporting their evaluation with sufficient evidence, including documentation; and
- providing a written report ('Management Statement') of the effectiveness of the Service Organisation's internal controls for the relevant financial period.

In drafting this report Senior Management have regard to, as a minimum, the Control Objectives specified within Technical Release AAF 01/20 issued by ICAEW but they may add to these to the extent that this is considered appropriate in order to meet User Entities' expectations.

RESPONSIBILITIES OF THE SERVICE AUDITOR

It is our responsibility to form an independent conclusion, based on the work carried out in relation to the Control Activities of the Service Organisation's [describe Service Organisation's activity, eg, custody services] carried out at the specified business units of the Service Organisation [located at [ ]] as described in the Management Statement and report this to Senior Management.

SCOPE OF THE SERVICE AUDITOR'S WORK

We conduct our work in accordance with the procedures set out in AAF 01/20, issued by ICAEW. Our work will include enquiries of management, together with tests of certain specific Control Activities.

In reaching our conclusion, the criteria against which the Control Activities are to be evaluated are the internal Control Objectives developed for Service Organisations as set out in the AAF 01/20 issued by ICAEW.

Any work already performed in connection with this engagement before the date of this letter will also be governed by the terms and conditions of this letter.

We may seek written representations from Senior Management in relation to matters on which independent corroboration is not available. We shall seek confirmation from Senor Management that any significant matters of which we should be aware have been brought to our attention.

[23] The above extracts may be appropriate illustrations only for an engagement formed between the Service Auditor and the Service Organisation. Where a multi-party engagement is formed in line with paragraph 73(a), wording should be revised and additional clauses should be inserted as appropriate. Where a User Entity agrees to sign up to the engagement terms at a later date, additional wording maybe inserted in line with paragraph 73(b) to clarify the basis on which the User Entity signs up and to secure the consent of the Service Organisation/original addressees. The wording will include adjustment of the section on 'Use of Report' and the addition of wording in the section on Liability Provisions to refer to the provisions applying to 'Senior Management as a body, the Service Organisation (and User Entities who are to become, by signature, a party to the engagement letter)' and to losses suffered by, and aggregate liability to, 'Senior Management as a body, the Service Organisation (and any User Entities who are to become, by signature, a party to the engagement letter)'.

INHERENT LIMITATIONS

Senior Management acknowledge that Control Activities designed to address specified Control Objectives are subject to inherent limitations and, accordingly, errors or irregularities may occur and not be detected. Control Activities cannot guarantee protection against fraudulent collusion especially on the part of those holding positions of authority or trust. Furthermore, the opinion set out in the Service Auditor's Report will be based on historical information and the projection of any information or conclusions in the Service Auditor's Report to any future periods will be inappropriate.

USE OF THE SERVICE AUDITOR'S REPORT

The Service Auditor's Report will, subject to the permitted disclosures set out in this letter, be made solely for the use of Senior Management of the Service Organisation, and solely for the purpose of reporting on the internal controls of the Service Organisation, in accordance with these terms of our engagement.

Our work will be undertaken so that we might report to Senior Management those matters that we have agreed to state to them in the Service Auditor's Report and for no other purpose.

The Service Auditor's Report will be issued on the basis that it must not be recited or referred to or disclosed, in whole or in part, in any other document or to any other party, without the express prior written permission of the Service Auditor. We permit the disclosure of the Service Auditor's Report, in full only, to User Entities [of the Service Organisation using the Service Organisation's [identify activity, eg, 'custody services'] ('User Entities')] [(as defined in appendix [ ] to this letter),] and to the auditors of such User Entities, to enable User Entities and their auditors to verify that the Service Auditor's Report has been commissioned by Senior Management of the Service Organisation and issued in connection with the internal controls of the Service Organisation without assuming or accepting any responsibility or liability to them on our part.

To the fullest extent permitted by law, we do not and will not accept or assume responsibility to anyone other than Senior Management as a body and the Service Organisation for our work, for the Service Auditor's Report or for the opinions we will have formed.

LIABILITY PROVISIONS[24]

We will perform the engagement with reasonable skill and care and acknowledge that we will be liable to Senior Management as a body and the Service Organisation for losses, damages, costs or expenses ('losses') suffered by Senior Management as a body and the Service Organisation as a result of our breach of contract, negligence, fraud or other deliberate breach of duty. Our liability shall be subject to the following provisions:

- We will not be so liable if such losses are due to the provision of false, misleading or incomplete information or documentation or due to the acts or omissions of any person other than us, except where, on the basis of the enquiries normally undertaken by us within the scope set out in these terms of engagement, it would have been reasonable for us to discover such defects;
- We accept liability without limit for the consequences of our own fraud or other deliberate breach of duty and for any other liability which it is not permitted by law to limit or exclude;

[24] The Service Auditor may wish to seek independent legal advice on language that addresses both the matters covered in the illustrative wording set out in this Liability section together with any related matters such as provisions indicating that liability does not extend to consequential losses. The Service Auditor may also consider any applicable independence requirements.

- Subject to the previous provisions of this Liability paragraph, our total aggregate liability whether in contract, tort (including negligence) or otherwise, to Senior Management as a body and the Service Organisation, arising from or in connection with the work which is the subject of these terms (including any addition or variation to the work), shall not exceed the amount of [To be discussed and negotiated].

To the fullest extent permitted by law, the Service Organisation agrees to indemnify and hold harmless [name of the Service Auditor] and its partners and staff against all actions, proceedings and claims brought or threatened against [name of the Service Auditor] or against any of its partners and staff by any persons other than Senior Management as a body and the Service Organisation, and all loss, damage and expense (including legal expenses) relating thereto, where any such action, proceeding or claim in any way relates to or concerns or is connected with any of [name of the Service Auditor]'s work under this engagement letter.

Senior Management as a body and the Service Organisation agree that they will not bring any claims or proceedings against any of our individual partners, members, directors or employees. This clause is intended to benefit such partners, members, directors and employees who may enforce this clause pursuant to the Contracts (Rights of Third Parties) Act 1999 ('the Act'). Notwithstanding any benefits or rights conferred by this agreement on such partners, members, directors or employees by virtue of the Act, we and Senior Management as a body may together agree in writing to vary or rescind the agreement set out in this letter without the consent of any such partners, members, directors or employees. Other than as expressly provided in this paragraph, the provisions of the Act are excluded.

Any claims, whether in contract, negligence or otherwise, must be formally commenced within [years] after the party bringing the claim becomes aware (or ought reasonably to have become aware) of the facts which give rise to the action and in any event no later than [years] after any alleged breach of contract, negligence or other cause of action. This expressly overrides any statutory provision which would otherwise apply.

This engagement is separate from, and unrelated to, our audit work on the financial statements of the Service Organisation for the purposes of the Companies Act 2006 or other legislation and nothing herein creates obligations or liabilities regarding our statutory audit work, which would not otherwise exist. [Equivalent paragraphs where the Service Organisation is other than a Companies Act entity].

[Appendix: The list of User Entities to whom the Service Auditor's Report may be made available[25].]

[25] A list of User Entities may not be practical where there is an extensive list.

Appendix 6: example sample size table

The Service Auditor applies its own sampling methodology established in accordance with prevailing audit and assurance standards. In determining the number of items to be tested for each control activity, the Service Auditor considers the factors referred to in paragraph 115.

The table below is an illustration to assist Service and User Organisations understand how many items the Service Auditor may test.

Frequency of control	Assumed population of control occurrences*	Number of items to test (low, medium, high risk)
Annual	1	1
Quarterly	4	2
Monthly	12	2 to 5
Weekly	52	5, 10, 15
Daily	250	20, 30, 40
Multiple times per day	Over 250	25, 45, 60

The illustration above is based on a 12 month reporting period. The Service Auditor may choose to vary sample sizes for longer or shorter reporting periods.

Appendix 7: illustrative definition of enquiry, observation, inspection and re-performance

In describing the nature of tests carried out, it is desirable for the Service Auditor to define in the Service Auditor's Report what is meant by such procedures as enquiry, observation, inspection and re-performance (see paragraph 74). Illustrative definitions which may assist the Service Auditor in this regard are set out below.

ENQUIRY

Enquired of [name of Service Organisation] personnel. Enquiries seeking relevant information or representation from personnel were performed to obtain, among other things:

- Knowledge, additional information and affirmation regarding the Control Activities; and
- Corroborating evidence of the Control Activities.

OBSERVATION

Observed the application or existence of specific Control Activities as represented.

INSPECTION

Inspected documents and records indicating performance of the Control Activities. This included, among other things:

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

RE-PERFORMANCE

Re-performed the Control Activity or processing application of the Control Activities to check the accuracy of their operation. This included, among other things:

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

Appendix 8: service organisations that use other service organisations

The Service Organisation determines whether its description of Control Activities should include the relevant Control Activities carried out by a Subservice Organisation on its behalf. This Appendix provides further guidance on applying the two methods available: the carve-out method and the inclusive method.

APPLYING THE CARVE-OUT METHOD

The purpose of the Description of the services provided by the Subservice Organisation is to:

- Alert User Organisations to the fact that another entity (the Subservice Organisation) is involved in the performance of the outsourced services and that such services may affect the User Entities' internal control;
- Identify the services the Subservice Organisation provides; and
- Identify the instances when achievement of a Control Objective included in the Description is dependent upon Control Activities performed by the Subservice Organisation (Complementary Subservice Organisation Controls (CSOCs)).

The Description of the Service Organisation's system and the scope of the Service Auditor's engagement should include the Service Organisation's Control Activities that monitor the effectiveness of Control Activities at the Subservice Organisation, which may include a combination of ongoing monitoring to determine that potential issues are identified within agreed timescales and separate evaluations to determine the effectiveness of internal control is maintained over time. Examples of monitoring Control Activities include:

- Reviewing and reconciling output reports;
- Holding periodic discussions with the Subservice Organisation;
- Making regular site visits to the Subservice Organisation;
- Testing Control Activities at the Subservice Organisation by the Service Organisation's internal audit function;
- Reviewing reports on the Subservice Organisation's system, where available, prepared in accordance with recognised standards (such as those produced by the ICAEW, IAASB or AICPA); and
- Monitoring external communications, such as User Entity complaints relevant to the services provided by the Subservice Organisation.

The Description should include the nature of the relevant services performed by the Subservice Organisation which support the achievement of the Service Organisation's Control Objectives, but it need not describe the detailed transaction processes, Control Objectives or Control Activities at the Subservice Organisation. The Description of the Service Organisation's system carves out those Control Objectives for which related controls operate only or primarily at the Subservice Organisation. However, the Description should contain sufficient information concerning the carved-out services to enable User Organisations to:

- Understand the significance and relevance of the Subservice Organisation's services to User Entities' internal controls; and
- Determine what additional information they may need to obtain from the Subservice Organisation to assess the relevant risks.

The CSOCs disclosed in the Service Organisation's Description should be specific to the services provided, but may be presented as broad control categories or objectives, rather than as a detailed list of Control Activities.

Where the carved out Subservice Organisation has issued a Type 1 or Type 2 controls report to its User Entities, the Service Auditor should determine whether the Service Organisation has included and addressed relevant Complementary User Entity Controls (CUECs) described in the Subservice Organisation's Report, or specified in the contract or service level agreement between the Service Organisation and the Subservice Organisation.

APPLYING THE INCLUSIVE METHOD

As described in paragraph 107, applying the inclusive method can be difficult. The most common circumstance where the inclusive method is applied in practice is where the Subservice Organisation is another entity in the same Group as the Service Organisation. For example, IT services are often centralised into one entity which supports all other Group entities.

The Service Organisation is the party which engages with the Service Auditor. However, Senior Management of the Subservice Organisation:

- Acknowledge and accept responsibility for preparing the Description as it relates to the Subservice Organisations services;
- Select the Criteria to be used;
- Specify the Control Objectives;
- Identify the risks that threaten the achievement of the Control Objectives; and
- Acknowledge and accept responsibility for the relevant design and operation of control activities.

Matters to be agreed upon or coordinated by the Service Organisation and the Subservice Organisation include:

- The scope of the examination and the period to be covered by the Service Auditor's Report;
- Acknowledgment from Senior Management of the Subservice Organisation that they will provide the Service Auditor with a Management Statement and Senior Management's Representation Letter;
- The planned content and format of the inclusive Description;
- The representatives of the Subservice Organisation and the Service Organisation who will be responsible for:
    - Providing each entity's description;
    - Integrating the descriptions; and
- Access to the Subservice Organisation's people and transactions, and for a Type 2 report, the timing of the tests of Control Activities.

The refusal by Senior Management of a Subservice Organisation that is being presented using the inclusive method to provide Senior Management's Representation Letter may result in a qualified opinion and may be sufficient to cause the Service Auditor to withdraw from the engagement when withdrawal is possible under applicable law or regulation.

There may be instances in which a Subservice Organisation uses the services of another Service Organisation to perform services that are likely to be relevant to User Entities' internal controls. In those circumstances, the other Service Organisation that provides services to the Subservice Organisation is also a Subservice Organisation. The Service Organisation considers whether to include the controls of each Subservice Organisation in scope.

Appendix 9: bridging letters

The Bridging Letter does not constitute part of the engagement described within this guidance, and as such the Service Auditor is not involved, nor has any responsibility, in any part of the Bridging Letter process.

The Bridging Letter is signed on behalf of Senior Management, in line with the guidance in paragraph 36 for Management Statements.

The contents of a Bridging Letter may include:

- Reference to the latest issued Report, including the date of issue;
- A summary of the request from the User Entity;
- Summary of any significant changes to the Description within the latest Report;
- Details of any significant changes to the risks, Control Objectives or Control Activities within the Bridging period;
- Details of any major and relevant other exceptions, and their impact on the Control Objectives, in the Bridging period;
- A statement by Senior Management that they have assessed the effectiveness of the Control Activities for the Bridging period, akin to paragraph 58 within the Management Statement; and
- An explanation of remediation that has been implemented by management where the latest issued Report contains a qualified opinion.

An example Bridging Letter is as follows:

To the management of [User Entity name requesting the letter]

We have received your request for information regarding relevant changes in [service organisation]'s control environment in the period in-between the last provided AAF 01/20 report and the date of this letter.

We confirm the latest AAF 01/20 report was the report titled [insert report title], dated [insert report date], which covered the period [or point in time] up to [date of the end of the reporting period covered], and covered [services In-scope within the last report].

Through the governance processes that we have in place within [service organisation], as we have summarised in our Management Statement within the above mentioned AAF report, we can confirm that for the period [day after the date of the end of the reporting period covered] to [date of this letter] and for the control environment relevant to the above mentioned report:

- There have been no significant changes to the Description within the latest report[1]
- There have been no changes to the risks within the In-scope control environment that would give rise to changes to any of the control objectives listed in the last report[1]
- There has been no reduction in the coverage of risk provided by the control objectives for the services covered per the last report[1]
- There have been no changes to the control activities within our control environment, significant enough to cause one or more of the existing control objectives not to be met[1]
- Control activities listed within the report have been operationally effective [subject to the following exceptions[2]].

[We take this opportunity to draw your attention to the Complementary User Entity Controls within our report and highlight your role, as our customers, to assess the operational effectiveness of this set of controls within your own control environment.]

Please note this letter has not been subject to review by our Service Auditor, [Service Auditor of the last report], and is not a substitute for the AAF 01/20 reports that we produce and provide to you.

Director

Date

Signed on behalf of the Board of Directors

[1] If there have been any changes, these should be highlighted to the customer as part of this letter.

[2] Where control exceptions relevant to the scope of the last AAF report have been identified by management, these should be listed out within the letter in sufficient detail so the reader can identify the controls that are impacted, the nature of the issue and the level of risk posed to the customer.

Glossary

The following table is a glossary of this terms used in this guidance.

Term	Definition
AAF 01/06	The original version of this guidance.
Agreed Timescales	Agreed between parties, distinct from Required Timescales. This may cover both internal (e.g. documents such as policies, procedures, SLAs) and external (e.g. client agreements).
Automated Control Activities	Automated Control Activities are where the operator of the Control Activity is IT rather than human. For example, a Control Activity where there is a daily programmed pull of prices from an external market source into a trading platform, or a programmed reconciliation that runs automatically after the upload of prices with an automatic email alert to pre-determined management inboxes with prices over a pre-programmed daily percentage variance threshold. Note, where the daily threshold check is triggered by a person, then there is a manual element to the Control Activity, being that it is run each day, and an automated element to the Control Activity, which is the analysis of prices against a pre-programme threshold percentage limit and the automatic email alerts for breaches.
Authorised Signatory	A person who has been delegated authority to sign on behalf of their Service Organisation.
Bridging Letter	A formal representation letter from Senior Management to a User Entity to cover a non-coterminous period relevant to that User Entity.
Complementary User Entity Controls (CUECs)	User Entity Control Activities which complement Service Organisation Control Activities.
Complementary Subservice Organisation Controls (CSOCs)	Subservice Organisation Control Activities which complement Service Organisation Control Activities.
Control Activities	See definition of Subject Matter. The Control Activities were referred to as a 'Control Procedures' in the original version of this guidance.
Control Objectives	See definition of Criteria.
Control Procedures	See definition of Control Activities.

Criteria	A set of benchmarks against which the Subject Matter can be assessed. For a report on internal controls, the Criteria are typically articulated as 'Control Objectives' which reflect the risks being managed by a Service Organisation on behalf of User Entities.
Data	Any data that is relevant to the provision of in-scope Services.
Description	A Description by Senior Management of the Service Organisation concerning the Control Activities of the Service Organisation. This comprises two parts: a. An overview of the services provided, together with details of the governance arrangements, key functions and processes, key systems and supporting infrastructure; and b. A detailed description of the Control Activities which are designed to meet the Control Objectives.
ICAEW Code of Ethics	This is the prevailing Code of Ethics adopted by the ICAEW.
In-scope Systems	Systems directly relevant to any operational control within the report (e.g. automated functionality or a system generated report used in the operation of a control). This includes relevant IT components (i.e. database, operating system, applications, and network).
Management Statement	A statement by Senior Management concerning the Control Activities of the Service Organisation and a conclusion on them.
Material	Information is material if omitting, misstating or obscuring it could reasonably be expected to influence the assessments of the User Entities.
Other Information	Additional information that is likely to be helpful to a User Organisation but is not included within the scope of the Service Auditor's report.
Report	A written report setting out details of the Service Organisation's Control Activities for the relevant period in accordance with this guidance.
Required Timescales	Required by law or regulation, distinct from Agreed Timescales.
Responsible Party	See definition of Service Organisation.

Review and recommend report	This is a narrative report on a defined subject matter (for example: governance, process and controls), often in response to an event, as part of risk mitigation or for diagnostic or monitoring purposes, comprising the collection and analysis of information together with observations or recommendations by an independent practitioner. For example, an Operational Due Diligence report or a Skilled Persons (or equivalent) Report for the Financial Conduct Authority or other regulatory authority.
Senior Management	Those charged with governance of the Service Organisation. In a company these may be the Board of Directors.
Senior Management's Representation Letter	Written representations signed by Senior Management.
Service Auditor	An independent reporting accountant responsible for issuing an opinion on the Subject Matter using the Criteria of the Report. The Service Auditor was referred to as a 'Practitioner' or 'Reporting Accountant' in the original version of this guidance.
Service Auditor's Report	The Service Auditor's reasonable assurance report explaining the scope of work carried out and giving their opinion.
Service Auditor's Opinion	The Service Auditor's reasonable assurance opinion on the subject matter.
Service Organisation	The organisation that is responsible for the Subject Matter of the Report – and for the purpose of this guidance, may also be referred to as a 'Responsible Party' which provides services to User Entities and is issuing the Report.
Subservice Organisation	A Service Organisation used by the Service Organisation.
Subject Matter	The specific services performed by the Service Organisation that are being reported on. For the purpose of this guidance, the Subject Matter is defined as the system of internal controls put into place by a Service Organisation to manage certain risks on behalf of User Entities.
Type 1	A Report on Control Activities at a single point in time for which the Service Auditor assesses the fairness of presentation and design suitability of Control Activities against the Control Objectives.

Type 2	A Report which covers Control Activities in operation throughout a given period of time for which the Service Auditor assesses the fairness of presentation, design suitability and operating effectiveness of Control Activities against the Control Objectives.
User Entities	Third party customers of the Service Organisation who are the intended recipients of the Report on the services being provided (which forms the Subject Matter).
User Organisations	The User Entities and their auditors.

There are over 1.8m chartered accountants and students around the world – talented, ethical and committed professionals who use their expertise to ensure we have a successful and sustainable future.

Over 181,500 of these are ICAEW Chartered Accountants and students. We train, develop and support each one of them so that they have the knowledge and values to help build local and global economies that are sustainable, accountable and fair.

We've been at the heart of the accountancy profession since we were founded in 1880 to ensure trust in business. We share our knowledge and insight with governments, regulators and business leaders worldwide as we believe accountancy is a force for positive economic change across the world.

www.charteredaccountantsworldwide.com
www.globalaccountingalliance.com

ICAEW
Chartered Accountants' Hall
Moorgate Place
London
EC2R 6EA
UK

T +44 (0)20 7920 8100
E generalenquiries@icaew.com
icaew.com

Chartered Accountants Worldwide
Member

GAA
Global Accounting Alliance