AUDIT • ADVISORY • TAX

Elevating **people**.
Elevating **business**.
Elevating **society**.

Independent Assurance or SOC Reports

ISAE 3402 and ISAE 3000

Introduction

Today it is almost normal practice for an organisation to outsource some of their core tasks, data processing or even IT infrastructure to third parties. These third parties (also called "service organisations") make many claims about the quality of their services to their customers (also called "user organisations/entities") – including the quality of their internal control systems to mitigate risks. When a user entity outsources these tasks and functions, many of the risks of the service organisation become risks of the user entity.

In light of several prominent internal control breakdowns (e.g. security / privacy breaches and fraud) and increasing regulatory focus on internal control, user-entities are increasing their due diligence for prospective service organisations and governance oversight of current service organisations. Consequently, the need for an annual independent assurance report, issued by an independent audit firm like BDO (also called the "service auditor"), that enables the management of a service organisation to demonstrate to a user entity that their internal controls were adequately designed and operated effectively.

Thus, on an annual basis, a user entity can demand from their service provider an independent assurance reports, expressing an opinion on the service organisation's internal controls relating to either:

- financial reporting; or
- the security, availability and privacy of data as well as the processing integrity of systems.

ISAE 3402

When an organisation (user entity) requires independent assurance on a third party or supplier's (service organisation's) internal controls, that are most likely relevant to the organisation's internal control over financial reporting, the service organisation can obtain an ISAE 3402* report from BDO. The report will express an opinion on the design and operational effectiveness of these internal controls.

** The International Auditing and Assurance Standards Board's (IAASB) International Standard on Assurance Engagements 3402, Assurance Reports on Controls at a Service Organisation (ISAE 3402).*

ISAE 3000

When an organisation (user entity) is concerned about the design and operational effectiveness of their third parties or suppliers' security / privacy controls, controls over data availability as well as the processing integrity of their systems, the third party (service organisation) can obtain an ISAE 3000* report from BDO. The report will express an opinion on the design and operational effectiveness of these internal controls.

** International Standard on Assurance Engagements (ISAE) – ISAE 3000: Assurance Engagements Other Than Audits or Reviews of Historical Financial Information – established by the International Auditing and Assurance Standards Board ("IAASB").*

Why BDO for your ISAE needs?

Assurance:

BDO has extensive experience in issuing SOC 1 and SOC 2 reports – regardless the industry you are operating in. We have assisted numerous clients in the past to progress from a Type 1 report to a Type 2 report. All our clients (service organisations) use these reports to provide their clients and their auditors (also called the "user auditor") with the necessary assurance that they have adequate and effective controls in place to protect their financial and other interests.

Mark of Excellence:

On a yearly basis BDO's clients receive value for money by using this independent assurance report to establish transparency and trust with their clients (user entities). This report not only assists a BDO client to retain their current client base but also to secure new clients – as the ISAE report is the international mark of excellence and quality.

Assistance in Statutory Audits:

BDO also works in close cooperation with our clients' external auditors to ensure that we cover the required scope and tests so that they can rely, from a statutory audit perspective, on our reports and assurance work. This makes it possible for our clients to avoid multiple audits (initiated by their clients' auditors).

Transparency on Systems and Controls:

BDO's ISAE reports are detailed reports that also describe a service organisation's systems and controls being used to deliver their services to a client. It allows a client (user entity) to better understand the service organisation's systems and control processes and how their own internal control system should be designed and implemented to ensure a seamless control environment (user entities perceive this as a value add to improve on their own control systems).

Strong Governance Culture:

An ISAE assurance engagement strengthens the general governance culture of an organisation. Because ISAE engagements occur once a year, BDO clients had experienced an improvement, year-on-year, in their governance processes and culture. It also allows a service organisation to develop a better understanding of their own system processes and controls.

Readiness Assessments:

BDO can assist you to prepare for the assurance engagement by doing a readiness assessment upfront. The readiness assessment identifies gaps in the internal control system and it allows our clients to correct those discrepancies before a Type 1 or Type 2 assurance engagement starts. By making use of a readiness assessment, a service organisation can avoid a "red report" – i.e. a qualified opinion – and wasted expenditure.

Step-by-Step Assistance:

BDO assists every client with advice during the entire process – from the writing of their assertion to the development of their system description to the identification of their control objectives and controls (controls are also benchmarked by us against international practice).

Knowledge:

BDO has a knowledgeable team who understands the nature of service organisations and how important it is to a service organisation to establish a trust relationship with their clients.

Professionalism:

BDO's professional team consists of chartered accountants and IT professionals and, in close cooperation with each other, assesses clients' financial process, application and general IT controls.

Elevating **people**. Elevating **business**. Elevating **society**.

ISAE reports

ISAE 3402 report

An ISAE 3402 report provides a vehicle for reporting on a service organisation's system of internal controls that are relevant to a user organisation's internal controls over financial reporting. ISAE 3402 reports are normally intended to be auditor-to-auditor (i.e. from service auditor to user auditor) communications. The ISAE 3402 replaced the old SAS 70 standard and report.

By obtaining an ISAE 3402 report, the service organisation can avoid multiple audits on their internal control – as user entities' auditors may rely upon the report's opinion and detailed findings – as issued by the service auditor. The ISAE 3402 report contains a description of the controls, control objectives, tests performed by the service auditor as well as test results – specifically included for the information of the user auditor, who, under normal circumstances, would have had to deal with the service organisation directly to identify controls, control objectives and perform tests.

Why a BDO ISAE 3402 report?

- A service organisation might want to obtain an ISAE 3402 report for marketing purposes - as it is easier to take on and retain clients if they can demonstrate that they as service provider have proper internal controls in place to mitigate risk relevant to a user entity's financial reporting.
- For certain user organisations, again, it is a minimum requirement; i.e. their service providers must have an ISAE 3402 report before they would do business with them.
- An ISAE 3402 report, issued by BDO (as a service auditor), differentiates the service organisation from its competitors by demonstrating due diligence on the establishment of a proper internal control system over financial reporting.
- An ISAE 3402 report creates trust between the service organisation and user organisation.
- Without an ISAE 3402 report a service organisation may have to deal with multiple audit requests from its clients and their respective (user) auditors. Multiple visits from their clients' auditors can place a strain on the service organisation's resources. An annual ISAE 3402 report ensures that all user organisations and their auditors have access to a report describing the systems of the service organisation as well as the systems of internal control.
- A user organisation who receives an ISAE 3402 report from its service provider, receives valuable information regarding the service organisation's controls and the effectiveness of those controls. The user organisation receives a detailed description of the service organisation's controls and an independent assessment of whether or not the controls that were placed in operation, are suitably designed, and operating effectively (in the case of a Type II report).
- A user organisation should provide a service auditor's report to their own auditor (user auditor). This will greatly assist the user auditor in executing the audit of the user organisation's financial statements. Without a service auditor's report, the user organisation would likely have to incur additional costs in sending their auditors to the service organisation to perform their procedures. It therefore means reduced audit fees for the user organisation.

ISAE 3402 – SOC 1 report

The ISAE 3402 report is the international equivalent of the American / Canadian SOC 1 report. The SOC 1 report replaced the old SAS 70 report and primarily covers business critical processes and system controls around financial reporting - although general IT controls should be covered as well.

ISAE reports

ISAE 3000 REPORT

The difference between ISAE 3402 and ISAE 3000 is that, whilst an ISAE 3402 report covers a service organisation's internal controls that are most likely relevant to a user organisation's internal control over financial reporting, the ISAE 3000 standard covers independent assurance engagements other than audits or reviews of historical financial information. The ISAE 3000 can therefore be used to express an opinion on a service organisation's security, availability and privacy of data as well as the processing integrity its systems.

Under the ISAE 3000 standard it is possible to express an opinion on all above principles (i.e. security, availability, privacy and processing integrity) or on only a selected one or more principles. For example, an opinion can be expressed on only privacy (e.g. compliance with POPIA and GDPR). An opinion can also be expressed on only security (e.g. compliance with ISO 27001).

The same benefits derived from obtaining an ISAE 3402 report, can also be gained by obtaining an ISAE 3000 report.

ISAE 3000 – SOC 2 Report

The ISAE 3000 report is the international equivalent of the American / Canadian SOC 2 report. The ISAE 3000 standard should be used to express an opinion on internal controls not related to financial reporting – e.g. IT security, general IT controls, data privacy etc.

Type 1 and type 2 reports

Both the ISAE 3402 (SOC 1) and ISAE 3000 (SOC 2) standards allow for the issuing of two types of reports:

Type 1 Report:

This report expresses an opinion on only the design and implementation of internal controls – e.g. a design inefficiency refers to the lack of a control or a poorly designed control and / or poor implementation. The Type 1 report is normally issued the first time around – i.e. when a service organisation hasn't obtained a SOC 1 or SOC 2 report before. The rationale behind a Type 1 report is that it allows a service organisation to first correct any poorly designed or implemented controls – before a Type 2 report is issued.

Type 2 Report:

This report expresses an opinion on not only the design and implementation of internal controls, but also the effectiveness of controls – e.g. control ineffectiveness refers to an existing (well designed and implemented) control that doesn't achieve its control objectives; i.e. it is not functioning and achieving its objectives as Management has intended it to do. The Type 2 report is the most sought after report – and can be issued after the service organisation has ensured that their controls are designed and implemented effectively (and controls had an opportunity to mature over several months).

BDO

AUDIT • ADVISORY • TAX

Elevating **people**.
Elevating **business**.
Elevating **society**.

For more info, please contact:

Head of ITCE

✉ jjansenvanrensburg@bdo.co.za

☎ +27 11 481 3129