ISAE 3402: Demonstrable IT assurance

The ISAE 3402 is an assurance report for organisations that want to demonstrate they are in control over their IT and that their processes are arranged and executed properly. Kiwa has years of experience in information security and certification in different industries

As a services organisation you can nowadays hardly operate without recognition obtained by external certification. Customers demand demonstrable quality. Besides ISO and SAS70, ISAE 3402 is also more and more required. It is one of the few certifications where quality measures are actually assessed in terms of effectiveness. On top of that, the management of the organisation also needs to declare in writing that the system is functioning well. These are internationally acknowledged certifications that can be used all over the world.

The ISAE 3402 is ideal for organisations that are active in the business services industry or organisations that are outsourcing parts of their business-critical process and want to make absolutely sure that this is handled properly. Think of questions such as: 'How does my supplier comply with the rules and legislation in the fields of privacy, such as GDPR?' Or: 'Is there a proper change process in place?'

ISAE 3402 Type 1 and Type 2

With an ISAE 3402 an independent (RE-) auditor assesses the quality of outsourced activities offered by a services organisation to a user organisation and the degree of control over these activities by the user organisation. The ISAE 3402 declaration can be issued in a Type 1 and Type 2 reporting.

ISAE 3402 Type 1

Because an ISAE 3402 type 1 report concerns a specific date, a Type 1 report is of limited use for a user organisation and its accountant because it doesn't reveal whether measures have worked effectively during a certain period. Another difference between a Type 1 and a Type 2 report is that the auditor not required to include his or her findings in the report.

ISAE 3402 Type 2

Kiwa N.V.
info@kiwa.nl
+31 (0)88 998 44 00

An ISAE 3402 Type 2 is content-wise the same report as a Type 1 rapport. The difference is that the declaration of the RE auditor also states that the described control measures have worked effectively over a period of at least six months. As a result, the audit is much more extensive than a Type 1 audit. For instance, control measures that are performed on a daily basis are assessed 15 to 25 times per year on their effectiveness.
A user organisation obviously has more certainty with a Type 2 report that the services are being managed as agreed. The period during which an ISAE Type 2 takes place is at least six months, provided there are no special circumstances such as the acquisition of a new organisational entity or a new IT system.

ISAE 3402 audit

An ISAE 3402 audit works as follows. First the scope is determined by looking at the organisation, its policies and processes, including the measures that are implemented and the purpose that the organisation aims for. Based on that, a GAP analysis is conducted. This offers you a baseline that enables you to counter any deficiencies.
After this phase, the actual assessment takes place during which the measures are being tested and validated. Among other matters, the effectiveness, the relation to the identified risks and the way the process is controlled will be evaluated. The findings will be reported and discussed with you in detail. Because the ISAE 3402 focusses on the previous period, this audit takes place on a yearly basis.

Mandatory aspects of the ISAE-report

- A description of the internal control framework;
- A confirmation of the service organisation;
- A service auditor assurance report.

Compulsory elements are therefore prescribed, but not all elements are included in the way in which these elements must be presented in the report.

Why an ISAE 3402 audit by Kiwa?

Kiwa has a track record of many years in information security and certification in major industries.
AN ISAE 3402 assurance report contributes to more profound demonstrability of the control of IT processes to customers and other stakeholders.
Kiwa can help by performing:

- Workshops – joint determination of the scope of the investigation
- Intermediate GAP-analyses – knowing where you stand;
- Type 1 assurance report – Set up and existence of your measures;
- Type 2 assurance report – Set up, existence and working of your measures;
- The ISAE 3402 certification can be executed in combination with ISO 27001. This creates one audit moment with the same auditors for both audits.

Do want to know more about the ISAE 3402 or how you can integrate this standard with your existing ISO 27001 certification? Feel

Kiwa N.V.
info@kiwa.nl
+31 (0)88 998 44 00

free to contact us for more information.

Kiwa N.V.
info@kiwa.nl
+31 (0)88 998 44 00