Review of assurance over outsourced controls

KPMG Technology Assurance

Are you sure that your company's outsourced processes operate in accordance with the relevant regulations? Have you considered that risk reduction is becoming an increasingly important aspect when inviting contractors for tenders?

Nowadays it is a common operating practice to outsource business support, system operations and data processing activities. At the same time market and regulatory requirements mandate maintaining the reliability of the control environment in question. To address these concerns KPMG's services are based on the ISAE 3402 and the SSAE 16 audit standards, which evaluate in a formal report – which can be submitted to a third party – the design, implementation and operating effectiveness of IT controls at service organisations. Certification of these standards is advantageous for both companies that outsource their processes and the service organisations which take them over.

Do the following issues sound familiar to you?

As a company with outsourced processes

- Considerable resources are necessary to verify for contractors and supervisory authorities that the control environment at the service organisation is appropriate.

- The confidentiality, integrity and availability of data handled by service organisations might be insufficient.

- Your company has no internal resources for regular and documented control testing.

As service provider

- Your client expects you to comply with the ISAE 3402 or the SSAE 16 standard.

- Your control environment is not documented and thus you cannot prove that it is sufficient.

How can we help?

The following services from KPMG's IT Risk Advisory Services practice can help your company with planning the control environment, testing the controls and performing retrospective reviews.

For companies with outsourced processes

- **ISAE 3402 (SOC1) and SSAE 16 (SOC2/SOC3) advisory and preparation for the audit:** In an SOC1 review we audit the internal controls over financial reporting (ICOFR) and inspect whether controls in a given moment are appropriate. For an SOC2/SOC3 audit we examine legal compliance and operating effectiveness for a given period. In an SOC2 review we issue a detailed report, and for an SOC3 review we issue a short management summary.

- **Review of assurance over outsourced controls, including auditor certificate:** If required, at the end of our review we issue an auditor certificate of the results and make a declaration on the level of assurance that has been gained. Thus, we can represent our clients in supervisory audits.

For service providers

- **ISAE 3402 (SOC1) and SSAE 16 (SOC2/SOC3) advisory and preparation for the audit:** For both review types we examine whether your implemented and operational controls conform to the activities of the client organisation to which you provide services. For an SOC1 review we inspect internal controls over financial reporting (ICOFR), including a review of both transaction processing and supporting general IT controls. During an SOC2/3 review we audit the legal compliance and operating effectiveness of controls for a given period and related to the services you provide to your current clients. This review covers the areas of IT security, availability, configuration changes, integrity of data processing and protection of personal data. An SOC2 review encompasses the issuing of a detailed report, while in an SOC3 review we issue a short management summary.

- **Review of assurance over outsourced controls, including auditor certificate:** We issue you a certificate of our review whose results can be used to verify your level of assurance to clients.

What advantages do we bring?

For companies with outsourced processes

- Relying on the ISAE 3000 methodology we can efficiently reduce losses resulting from a lack of legal and regulatory compliance.

- The implementation and monitoring of controls in relation to outsourced processes is a focus area from both regulatory and legal points of view. Thus, compliance is not only a business interest, but it is also crucial for risk management. Our service facilitates your company's eligibility to gain an auditor certificate.

For service providers

- Standard-compliant operation and related certification increase the levels of trust of the interested parties.

- With the help of the standards we harmonise business and IT aspects, helping to ensure effective co-operation in order to achieve common goals.

If you feel these issues are relevant to your business, please contact us for further details:
———

KPMG.hu