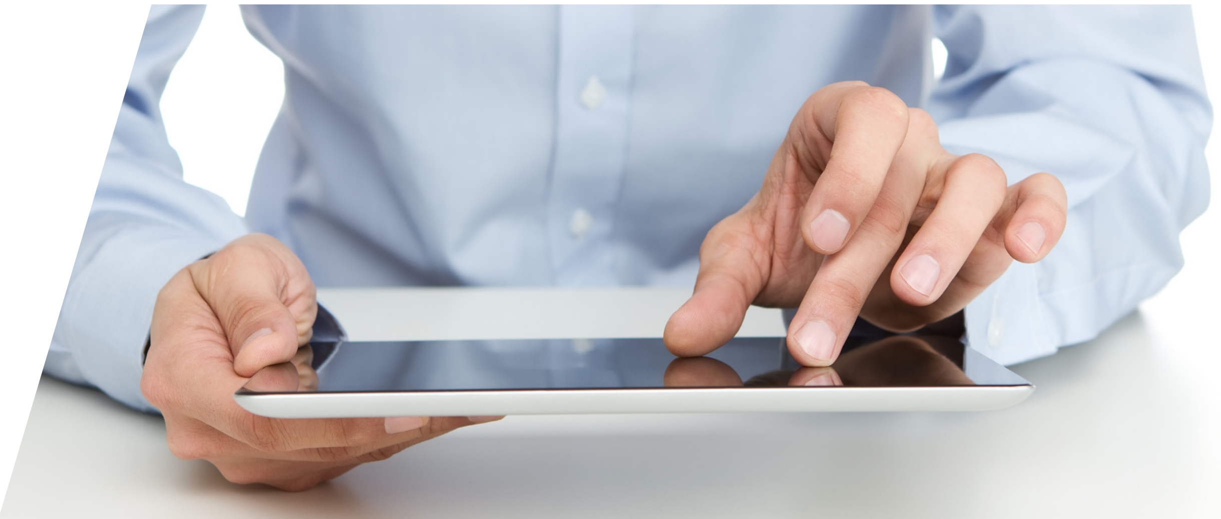
How to effectively use Service Organization Control (SOC 2 and SOC 3) Reports for increased Assurance over Outsourced Controls regarding Security, Availability, Processing Integrity, Confidentiality and Privacy

You are a service organization managing critical systems, storing and processing private and/or confidential client information, and/or processing transactions for multiple clients.

THE CHALLENGE | YOUR BENEFITS | KPMG APPROACH | CREDENTIALS | CONTACT

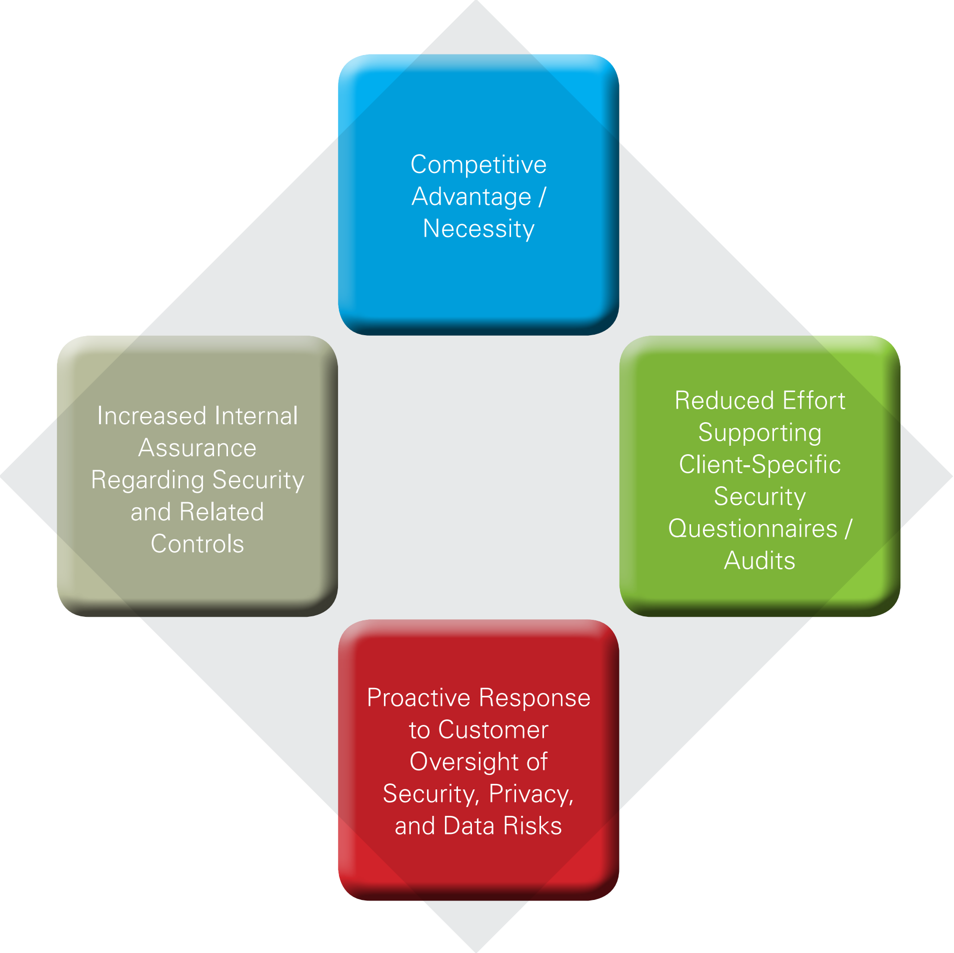
THE CHALLENGE

- New IT technologies (virtualization, cloud computing, mobile computing) are becoming increasingly part of your service offering and/or supporting your operational processes
- Your clients are becoming increasingly demanding to the measures taken to protect their private and/or confidential information and to ensure availability of their systems
- Deficiencies in the security offered by you may result in the release of client information and lead to reputational damage both to you and your clients
- Real or perceived security breaches may cause your clients to believe that your organization is unable to conduct business securely and responsibly
- Your clients' assurance needs are not fully satisfied by currently employed certifications (e.g., ISO 27001).
- Clients are demanding additional insight into the system and related controls, design and control implementation, as well as assurance regarding the operating effectiveness of these controls
- You are confronted with multiple visits from your clients' auditors and requests to complete detailed security questionnaires or checklists about your controls environment
- You must demonstrate your ability to meet your clients' compliance needs and strengthen their confidence in your ability in an increasingly competitive environment.



YOUR BENEFITS

- A traditional SOC 1 report (ISAE 3402 report, formerly known as SAS 70 report) is designed to meet your clients' related needs for financial statement audits, but does not necessarily meet needs related to operations and compliance. A SOC 2 report that focuses on one or more of the trust services principles – security, availability, processing, integrity, confidentiality and privacy – does
- A SOC 2 report has the same look and feel as a SOC 1 report and provides your clients with sufficient information (independent service auditor's opinion, management assertion, system description, tests performed by service auditor and test results) to satisfy their assurance needs
- Under certain conditions, a short form report (a SOC 3 report) may be generally distributed, with the option of displaying a web site seal


Competitive Advantage / Necessity
Increased Internal Assurance Regarding Security and Related Controls
Reduced Effort Supporting Client-Specific Security Questionnaires / Audits
Proactive Response to Customer Oversight of Security, Privacy, and Data Risks

KPMG APPROACH

Diagnostic Review

For service organizations that are new to the SOC 2 examination process, we recommend that a "SOC 2 Diagnostic Review" be performed. The purposes of the review are to focus on key areas that will be covered in the upcoming SOC 2 examination and identify the control weaknesses that may need to be corrected before the attestation engagement period begins.

In addition, during the Diagnostic Review, we will assist you in identifying and documenting your controls. This is ordinarily a significant component of management's effort during the preparation of the first such report.

Type I report

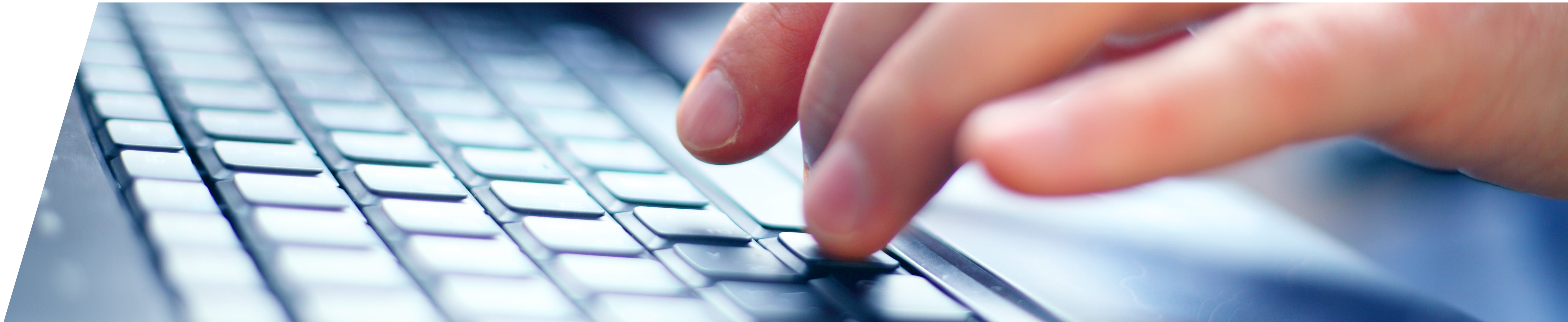
A Type I report contains a description of the service organization's system at a specific point in time. In a Type I report, the service auditor will express an opinion on (1) whether management's description of its system fairly presents the system that was designed and implemented as of a specific date and (2) whether the controls stated in management's description of its system were suitably designed to meet the applicable trust services criteria as of a specified date. An initial Type I report normally serves as the starting point for subsequent Type II examinations.

Type II report

A Type II report contains a description of the service organization's controls for a defined period of time. In a Type II report, the service auditor will express an opinion on the two items included in a Type I report. He/she will also conclude whether the controls were operating with sufficient effectiveness to provide reasonable assurance that the applicable trust services criteria were met during the examined period. A Type II report also includes detailed results of testing of the service organization's control over the specified period of time.

CREDENTIALS

KPMG is a global leader in delivering Service Organization Control (SOC) reporting services. KPMG's IT Attestation practice consists of a globally accredited network of partners and professional staff who provide a range of IT attestation services to help organizations satisfy their third-party assurance requirements. We have established a global accreditation process to help ensure consistency and quality in the delivery of attestation and assurance services including SOC 1, SOC 2 and SOC 3 examinations and Agreed Upon Procedures. We have over 1,000 professionals fully trained in the SOC examination process through our global IT Attestation Instructor network.



CONTACT

Stephan Claes
Partner

KPMG IT Advisory

T: +32)2 708 48 50
E: sclaes3@kpmg.com

Dirk Timmerman

Executive Director

KPMG IT Advisory

T: +32 2 708 43 59
E: dtimmerman@kpmg.com