KPMG

cutting through complexity

IT ADVISORY

KPMG ADVISORY

HOW TO EFFECTIVELY USE ISO 27001 CERTIFICATION AND SERVICE ORGANIZATION CONTROL (SOC2) REPORTS

Increase Assurance over Outsourced controls regarding Security, Availability and Confidentiality.

You are a service organization managing clients' mission critical systems, storing and processing confidential client information for multiple clients

THE CHALLENGE | YOUR BENEFITS | KPMG APPROACH | CONTACT

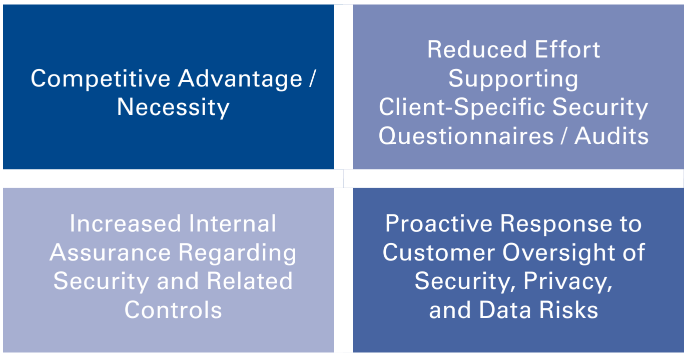
THE CHALLENGE

- Information security is front page news across the globe, with a constant flow of new breaches, hacks and incidents undermining public confidence in the ability of organizations to keep their data safe.
- Industry regulators are focusing their energies on ensuring that organizations take the emerging threats seriously and that information security is scrutinized at the highest level in an organization.
- Your clients are becoming increasingly sensitive to the measures taken to protect their 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.
- Clients are demanding insight in your 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 of clients' auditors and requests to complete detailed security questionnaires or checklists about your controls environment.
- You must demonstrate your capability to meet your clients' compliance needs and strengthen their confidence in your ability.

YOUR BENEFITS

- An ISO 27001 certification is proof of your capability of maintaining an effective Information Security Management System to a broad public, including Industry Regulators and your current and future clients.

- A SOC2 report based on the ISO 27001 Control Objectives has the same look and feel as a SOC1 report (ISAE 3402 report, formerly known as SAS 70 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 meet their assurance needs.
- The integration of the ISO 27001 certification with the SOC2 reporting allows us to perform the audit in a more efficient manner ("multi-purpose testing") and enables us to pass on these cost savings and reduction in number of audit days to you; in addition this will significantly reduce the burden on your internal resources.



Competitive Advantage / Necessity

Reduced Effort Supporting Client-Specific Security Questionnaires / Audits

Increased Internal Assurance Regarding Security and Related Controls

Proactive Response to Customer Oversight of Security, Privacy, and Data Risks

KPMG APPROACH

KPMG offers an integrated assurance approach that allows us to efficiently perform the ISO 27001 certification and SOC2 reporting in a single assessment. This integrated approach has the following phases:

Diagnostic Review

For service organizations that are new to the ISO 27001 certification and/or SOC2 reporting process, we recommend that a "Diagnostic Review" be performed. The purposes of the review are to perform a gap analysis against ISO 27001 and identify areas that require attention prior to beginning the formal certification.

In addition, during a Diagnostic Review, we will assist you in identifying and documenting your controls for the SOC2 report. This is ordinarily a significant component of management's effort during a first year report.

ISO 27001 certification

We have a tried and tested methodology to perform certification audits efficiently. There is an initial certification assessment that includes auditing all of the controls in the standard, followed by regular surveillance audits over a three year period. To maintain the certification there is a full re-assessment every three years.

SOC 2 Type I report on management's description of the system and the suitability of design of controls

Based on the work performed for the initial ISO 27001 certification, a SOC2 Type I report is prepared.

A Type I report contains the service organization's description of its 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 ISO 27001 control objectives as of a specified date. An initial Type I report normally serves as the starting point for subsequent Type II examinations.

SOC2 Type II report on management's description of the system and the suitability of the design and operating effectiveness of controls.

A Type II report contains the service organization's description of controls during 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, as well as whether the controls operated effectively throughout the specified period to meet the applicable ISO 27001 control objectives. A Type II report includes not only the service organization's management assertion and description of its system but also detailed results of testing of the service organization's control over the specified period of time.

ISO 27001 Surveillance Audits and Re-Assessment Audits

The ISO 27001 Surveillance Audits and Re-Assessment Audits (every three years) will leverage to a large extent on the work done as part of the annual SOC2 Type II reporting.

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 SOC1 and SOC 2 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.

KPMG has a team of trained ISO 27001 lead auditors with extensive experience of performing certifications across all industry sectors. KPMG has a Certification Body that is accredited by the United Kingdom Accreditation Service (UKAS) to perform ISO 27001 certifications globally.

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