Defining the difference between ISO27001 and ISAE 3000/SOC 2 in infosec

For many organisations ISO 27001 has been seen as the benchmark for information security, but with the threat landscape continually evolving and the punishments for getting it wrong ever increasing, many organisations are now looking for greater levels of assurance and over broader areas. This flyer sets out why this is an issue and where it is going....
The evolution of assurance

Formal assurance opinions over controls related to financial statements have existed for many years in the form of standards such as ISAE 3402 and ISAE 3000, but it is only since the launch of the SOC 2 framework that we have seen similar levels of assurance specific for information security.

SOC 2 started in the U.S. and it is now making its mark in the rest of the world.

The ISAE 3000/SOC 2 framework was designed to complement existing controls reports. **Unlike ISO 27001 which focuses only on the design of controls, ISAE 3000/SOC 2 also allows for the testing of the operating effectiveness of security controls over a period.** While these controls may not impact directly an entity’s financial statements, they are now hugely significant to organisations both from an operational and reputational perspective.

How does it work?

Within the ISAE 3000/SOC 2 framework there are five Trust Principles: **Security, Availability, Confidentiality, Processing Integrity and Privacy.** With only the Security principle being mandatory this standard also provides organisations with a degree of flexibility, allowing them to target the specific domains that are most important to them and their customers.

Similarly, the selection of applications in scope for the review is also at the discretion of the organisation, allowing them to target those which are most important to them and their clients.
What’s the difference between ISO 27001 and ISAE 3000/SOC 2?

1. With a ISAE 3000/SOC 2 there’s a formal attestation at the end of it, not just a certificate of compliance.

2. ISAE 3000/SOC 2 is more flexible: whilst the Security principle has to be covered, the remaining principles can be scoped-in as desired – covering the principles that are relevant to you and your clients.

3. ISO 27001 only focuses on an organisation’s information security management system, but an ISAE 3000/SOC 2 can cover the applications that are important to you and your clients.

4. ISO 27001 is at a point in time, but a ISAE 3000/SOC 2 can cover a period, therefore providing a greater level of assurance.

Does ISO 27001 still have a role?

ISO 27001 has been and will continue an important standard, allowing organisations to demonstrate that they have implemented a solid internal information risk management framework. But the world has changed – threats have evolved, and assurance requirements, both internally and externally have grown, with the ISAE 3000/SOC 2 framework providing the platform to address these needs.

The bigger picture

As we now move towards ever greater levels of regulation over security and data privacy, including the EU General Data Protection Regulations (GDPR), the penalties for failing to protect your data and that of your customers is increasing. With the potential fines reaching 4% of a corporation’s global turnover the cost of failure is crippling and service providers will undoubtedly face ever increasing scrutiny and requests from their clients.

Having an ISAE 3000/SOC 2 report not only avoids duplicating effort servicing multiple audit request, but it puts you firmly on the front foot with your existing clients, your Board and your Regulator and may even help to differentiate you against your competitors.

For those organisations who are engaging with service providers or sharing data, the message is clear: whilst services can be outsourced, accountability cannot. It is imperative that they can demonstrate how they are gaining comfort over security controls across their supply chain.
What does all this mean?

Organisations should reassess the adequacy of current forms of assurance in place – both in terms of depth and breadth of coverage.

In completing this assessment different lenses should also be used:
• from the perspective of the Board;
• from the perspective of the regulator;
• from the perspective of clients’; and,
• from the organisation’s own perspective on its suppliers and service providers.

Contact us

Constantinos Taliotis
Partner
Assurance
c.taliotis@pwc.com
T: +357 - 22 555 522

Sophie Solomonidou
Director
Risk Assurance
sophie.solomonidou@pwc.com
T: +357 - 22 555 150

Demos Demou
Senior Manager
Risk Assurance
demos.demou@pwc.com
T: +357 - 22 555 056

PwC Cyprus

PwC Central, 43 Demostheni Severi Avenue,CY-1080 Nicosia, Cyprus
P O Box 21612, CY-1591 Nicosia, Cyprus
Tel: +357 - 22 555 000