

Round table programme

SOC2 - Assurance's silver bullet?

Summary

- ▶ SOC2 is an opportunity to provide assurance on a wider range of service provision than just financial reporting.
- ▶ It may provide a more efficient way to deliver wider assurance to different stakeholders (e.g., regulators, ISO, PCI) by streamlining the process.
- ▶ The SOC2 approach is already being mapped to other frameworks (e.g., ISO 27001, Cloud Security Alliance).
- ▶ SOC2 provides a more 'checklist-type' approach that may help users compare service organisations more easily.

The latest Ernst & Young Service Organisation Controls Reporting (SOCR) round table was held in London in June 2011, with participants drawn from a range of private and public sector organisations. We would like to thank all those who attended for their contributions during the discussion. The round table discussed the new SOC2 standard and considered whether it could indeed be a silver bullet in terms of allowing service organisations to commission one audit that could be the basis of meeting various requirements for assurance that regulators and user organisations submit, or whether it was just another certification that service organisations might be expected to obtain.

What is SOC2?

The Service Organization Controls (SOC) framework was launched in 2010 by the American Institute of Certified Public Accountants (AICPA) and includes the following reporting frameworks:

- ▶ SOC1 – intended to provide user organisations and their auditors with independent assurance on controls over processes related to financial reporting. SOC1 replaces SAS70.
- ▶ SOC2 – similar in look and feel to SOC1, but provides independent assurance based on the Trust Services Principles and Criteria on processes not related to financial reporting.
- ▶ SOC3 – independent assurance to any user of a web-based service that the Trust Services Principles and Criteria are being met.

The AICPA's guide to the SOC framework can be downloaded from the AICPA's website.

SOC2 reports thus provide assurance in relation to one or more of the five Trust Services Principles, which are:

- ▶ Security
- ▶ Privacy
- ▶ Confidentiality
- ▶ Availability
- ▶ Processing integrity

Each Principle has associated Criteria, and service organisations must identify the controls which they have implemented, and which meet the requirements of each criterion. In a Type II report, the independent auditor describes how each control was tested, and the result of the test, as well as providing the independent opinion on the operating effectiveness of controls for the period covered by the report. Participants felt that this structure provided a level of consistency that would be useful – they recognised the challenge that user organisations sometimes raised in terms of SAS70 not having a defined control framework against which they could then assess service organisations. The Principles and supporting Criteria were seen as a sensible half-way house – the Criteria provides a common assessment framework, but allow a necessary variation in terms of the controls each service organisation has implemented to meet the Criteria.

As with a SOC1 report, a SOC2 report will contain the following:

- ▶ Independent service auditor's opinion
- ▶ Management assertion
- ▶ Description of the system providing the in-scope services
- ▶ Description of the controls delivering each of the in-scope Criteria, based on the Principles selected
- ▶ Description from the independent auditor of the tests performed and the results of those tests

Why would a service organisation want a SOC2 report?

Round table participants recognised a number of issues with the current independent assurance framework based on SAS70, including:

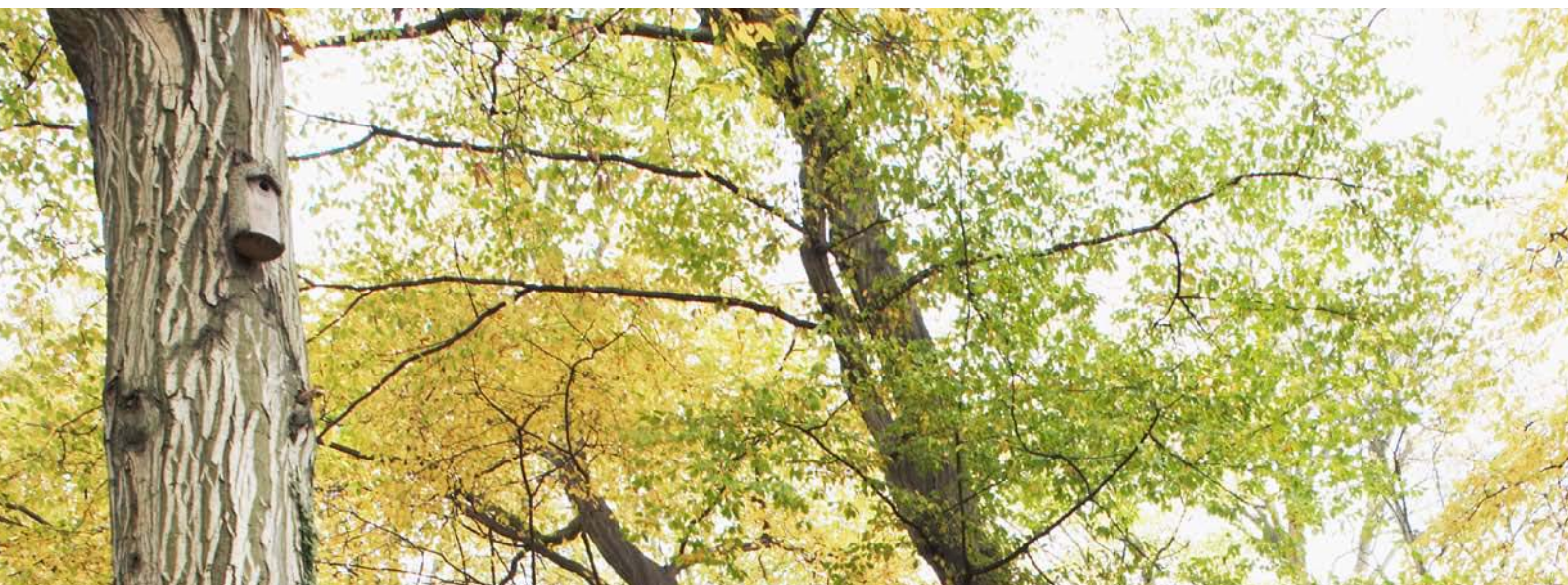
- ▶ Requests for assurance in areas where SAS70 historically could not be used to provide assurance (e.g., business continuity, data privacy)
- ▶ Multiple clients all asking roughly the same questions
- ▶ The number of different certifications that user organisations look for, including SAS70, PCI-DSS and ISO 27001 to name but a few

The discussion then considered whether participants felt SOC2 could realistically address some or all of these issues.

Requests for assurance in areas where SOC1 reports cannot provide assurance

Participants felt that of the five Trust Services Principles, the ones that would add most value to user organisations would be Security, Confidentiality and Privacy. These were felt to be the areas where service organisations were most likely to have generic processes and hence a single SOC2 report could be provided covering those processes and provide assurance to multiple user organisations. Processing integrity and Availability were seen as being more likely to be client-specific, and hence less likely to offer the cost and benefit advantages of the other three Principles. This partially matches our experience in talking to other service organisations on a global basis, where Security is definitely seen as offering value, but Availability is also seen as a useful Principle.

Privacy and Confidentiality are both areas that were not usually covered in a SAS70 report, and would not be covered by a SOC1 report. They can clearly be covered by a SOC2 report; the challenge for service organisations is to assess what user



organisations are looking for in these areas in terms of assurance, and to work with their service auditor to show how a SOC2 report could address these needs. If this can be done, and the user organisations accept the SOC2 as an alternative to their own audits, then SOC2 could indeed be used to provide independent assurance in areas where this has not previously been possible. The level of detail included in a SOC2 report was also seen as helpful by one participant: “users want to see exactly how we do things, and what the controls are and how they were tested, not just that we have a certification.” Providing this level of detail is exactly what SOC2 has been designed to do.

This emphasises a key message; there must be a sound business reason to provide a SOC2 report, which is usually grounded in one of two reasons:

- ▶ Cost savings because the number of client audits drop
- ▶ SOC2 report is seen as helping win new clients, or is key to retaining existing ones

Multiple clients all asking the same questions

Participants recognised common themes being covered in the audits being carried out by user organisations. We see this as predictable, given user organisations will typically have similar concerns around areas such as privacy and confidentiality, because they have the same obligations in these areas. SOC2 offers the chance to do one audit in these areas (for example) and then offer this to user organisations in place of their own audit questionnaires. We discuss below how service organisations could explain this approach and get the necessary user organisation commitment to replace their own audits with the SOC2 report, but participants did feel that SOC2 had the potential to replace these user organisation audits.

Multiple certifications

One participant asked how a SOC2 report could build on existing certifications such as ISO27001. The answer, we believe, is that it is more likely that other certifications can build on the work done for a SOC2 report. This is because the level of testing needed to support a SOC2 engagement may well be beyond that needed for other certifications (one reason why user organisations have historically valued SAS70 reports, for example). So rather than building a SOC2 report on the back of other certifications, the aim would be to use the SOC2 testing to support other certifications. We believe that this offers a more streamlined approach to testing, since even if there is not a huge reduction in the overall volume of testing, the fact it is being done by one provider in an integrated fashion will reduce disruption to service delivery teams. One participant also felt that SOC2 would gain wider acceptance if it could in some way be tailored for specific industries, to meet their specific needs. This may be possible since custom criteria can be added, and this would be an interesting area to explore.

“The mapping is key” was how one participant expressed the need to show how work done for a SOC2 report can provide assurance across multiple certifications. Another participant explained how they agreed with user organisations which of their controls should be in the SAS70 report by agreeing first of all which Controls Objectives for Information Related Technology (COBIT) controls needed to be covered by the SAS70 report. Both these examples show how interested user organisations are in exactly what a report covers, and how it maps to their own chosen assurance framework(s).

We are currently mapping the Trust Services Criteria to a range of other standards including ISO27001, PCI-DSS and the Cloud Security Alliance’s Common Control Matrix. One participant observed that this would be much stronger if regulators themselves would endorse this mapping, and this is certainly an area we would be keen to explore.

The mapping is key, and should be shared with user organisations so that it gains wide support as being a valid basis for assuming that the one set of testing can provide assurance against multiple standards; we discuss how this might work in more detail below.

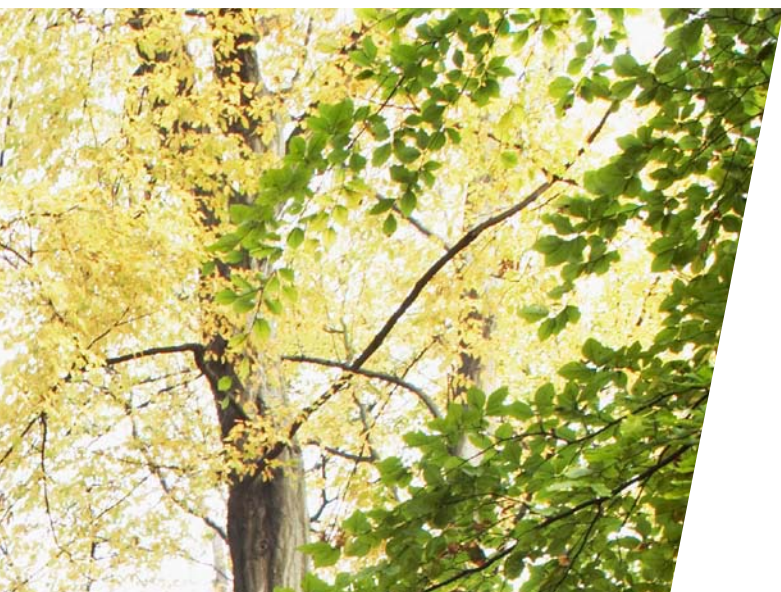
What might prevent SOC2 fulfilling its potential as a silver bullet?

Participants saw three major issues preventing SOC2 becoming a silver bullet:

- ▶ A refusal by user organisations to accept that it meets their needs
- ▶ A refusal to accept that it can be used to cover other certifications
- ▶ SOC2 being perceived as a US framework and so resisted by non-US user organisations

SOC2 not meeting user organisation needs

As long as the user organisations rely on their compliance teams to manage the process of obtaining assurance about how effective controls are at a service organisation, there may always



be challenges in replacing user organisation audits with one SOC2 report. This is, to put it bluntly, because if a user organisation compliance team just accepts a SOC2 report, why does the user organisation then need that team? Ways for service organisations to mitigate this resistance may include:

- ▶ Trying to promote to wider user organisation management the provision of a SOC2 report when the contract is signed so they challenge the need for additional compliance work
- ▶ Presenting the results of the SOC2 work to wider user organisation management

SOC2 not covering other certifications

We have discussed above how the work on a SOC2 report could also be used to support and streamline work on other certifications. We do not believe SOC2 will replace other certifications; the opportunity is to do one core set of audit work and use this as the basis for multiple certifications, with each additional certification then only requiring a minimum of further work specific to that certification.

SOC2 being resisted by non-US organisations

One participant raised the risk that since the SOC2 framework came from the US, it might be resisted, or not recognised by non-US user organisations. This is an interesting challenge, but we do not believe it is a significant barrier to the success of SOC2. After all SAS70 was a US standard and was accepted globally. How should service organisations assess whether SOC2 will add value?

We believe service organisations should go through the following steps to help assess whether a SOC2 project would add value to them:

- ▶ Identify the current user organisation audits they have to support and try to estimate the cost of supporting these
- ▶ Look at the areas covered by these audits, and identify if:
 - They are covering the same sorts of areas, and
 - Whether these areas would be covered by the SOC2 Principles and Criteria
- ▶ If there is a match, develop a proposed SOC2 scope
- ▶ Discuss this with key user organisations who send in their own auditors and identify whether they would be prepared to replace their audits with an independent assurance report
- ▶ At this point, SOC2 is revealed as the framework that will be used

Only if user organisations value the SOC2 report, and will reduce their level of audits, would the service organisation then proceed with a SOC2 report – unless they believed there were other reasons to provide such a report, such as wishing to be ahead of competitors in terms of the approach to providing independent assurance.

Conclusion

Overall, participants felt that SOC2 could help them streamline the process of providing assurance to their user organisations, but that much would depend on whether those organisations would be receptive to the idea of replacing their own questionnaires and audits with one provided by the service organisation, albeit with an independent audit opinion included in it. We understand these potential issues, and look forward to monitoring the progress of SOC2 over the coming months.

Contact

Paul Durkin

+44 (0)20 7951 3692
pdurkin@uk.ey.com

Mark Russell

+44 (0)117 981 2204
mrussell@uk.ey.com

Ernst & Young LLP

Assurance | Tax | Transactions | Advisory

About Ernst & Young

Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 141,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit www.ey.com

The UK firm Ernst & Young LLP is a limited liability partnership registered in England and Wales with registered number OC300001 and is a member firm of Ernst & Young Global Limited.

Ernst & Young LLP, 1 More London Place, London, SE1 2AF.

© Ernst & Young LLP 2011. Published in the UK. All Rights Reserved.



In line with Ernst & Young's commitment to minimise its impact on the environment, this document has been printed on paper with a high recycled content.

Information in this publication is intended to provide only a general outline of the subjects covered. It should neither be regarded as comprehensive nor sufficient for making decisions, nor should it be used in place of professional advice. Ernst & Young LLP accepts no responsibility for any loss arising from any action taken or not taken by anyone using this material.

www.ey.com/uk

1136140.indd (UK) 06/11. Creative Services Group.