



ISACA Northern Chapter

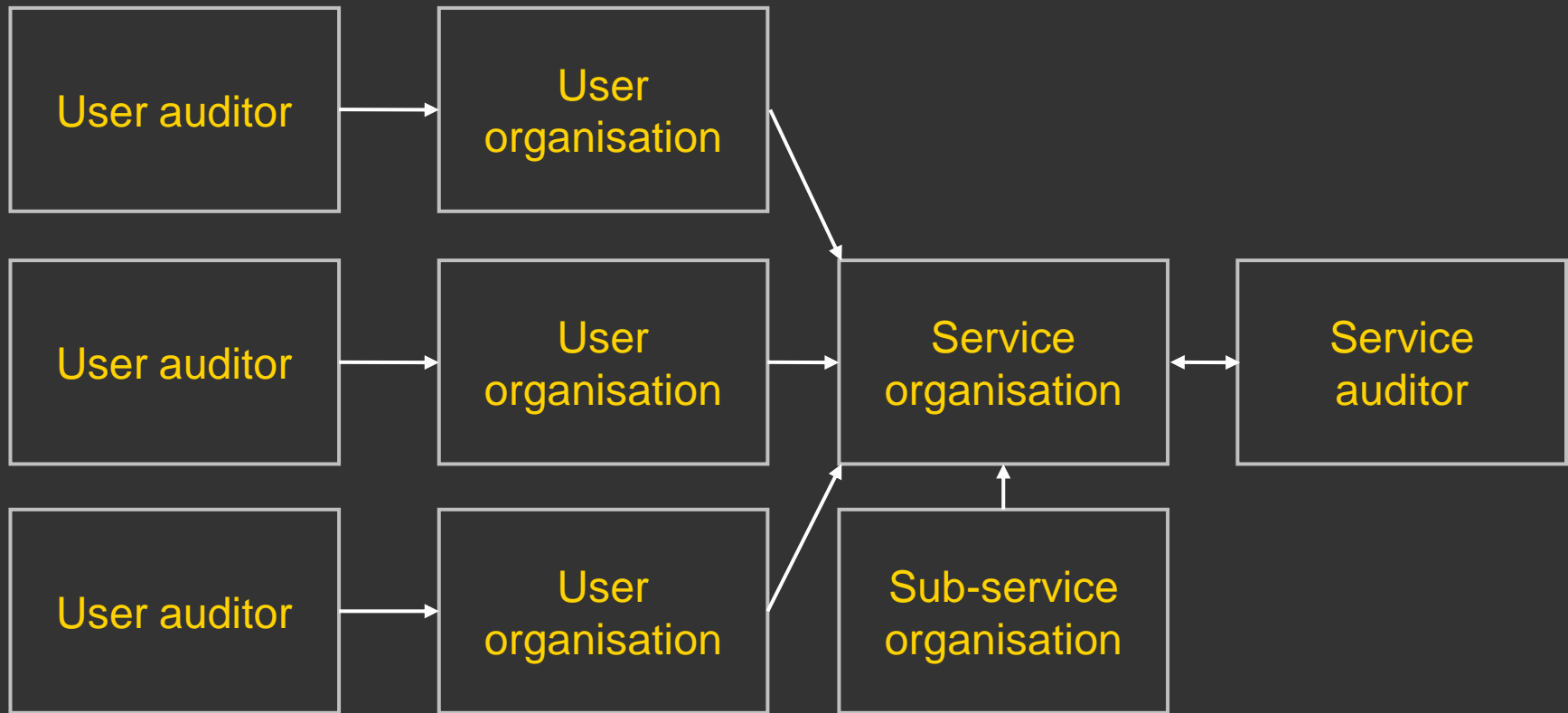
Assurance on outsourcers

Agenda

- ▶ Who's who in a SOC report?
- ▶ Where have we been?
- ▶ Where are we going?
- ▶ What is a SOC report?
- ▶ What does a SOC report give the user?
- ▶ What are the key questions a user needs to ask?
- ▶ Questions/discussion

Who's who in a SOC report?

SOC = Service Organisation Controls



Who's who in a SOC report? (cont'd)

Glossary

- ▶ Service organisation – the outsourcer
- ▶ Service auditor – the independent auditor opining on information provided by management
- ▶ User organisation – the user of the services provided by the service organisation
- ▶ User auditor – the user organisation's financial statement auditor who will be expected to rely on the SOC report in their audit, instead of testing at the service organisation
- ▶ Control objective – *“Controls exist to provide reasonable assurance that...”*

Where have we been?

- ▶ SAS 70 was the global ‘gold standard’
- ▶ Not available for periods ending on/after 15 June 2011
- ▶ It covered processes and controls that supported the financial reporting of user organisations
- ▶ Type I opined on
 - ▶ Accuracy of description of process and controls
 - ▶ Whether controls have been placed into operation
 - ▶ Whether control design is complete
- ▶ Type II added testing and opinion on operating effectiveness of controls
- ▶ Type II is what user organisations usually asked for – and so is what service organisations usually provided

Where have we been? (cont'd)

- ▶ Other standards existed
 - ▶ AAF 01/06 / ITF 01/07
 - ▶ Trust Services – Webtrust/Systrust
 - ▶ ISO27001
 - ▶ Other ISO/security certifications
- ▶ Some standards provide assurance but no opinion
 - ▶ Agreed Upon Procedures (AUP)
- ▶ Internal audit do own testing based on right of audit access

Where are we going?

- ▶ ISAE3402 and US implementation SSAE16 replace SAS70
- ▶ AICPA Service Organization Controls (SOC) standards
 - ▶ SOC1 is overall name for SSAE16/ISAE3402 reports
 - ▶ SOC2 = Trust Services Principles plus SOC1 Description of the System
 - ▶ SOC3 = Systrust/Webtrust
- ▶ AAF 01/06 continues but is under review

Where are we going? (cont'd)

- ▶ SOC1 adds following to the SAS70 report
 - ▶ Management assertion on description, control design and operating effectiveness
 - ▶ Separate one from sub-service organisation – so inclusive reports will be much rarer?
 - ▶ More detail in the description – process, not just controls
- ▶ What does SOC1 not do?
 - ▶ Provide assurance on non financial processes – use SOC2 for this
 - ▶ Enforce a standard set of control objectives on service organisations – use SOC2 / AAF 01/06 for this

Where are we going? (cont'd)

- ▶ SOC2 reports – include at least 1 Trust Services Principle
 - ▶ Security
 - ▶ Privacy
 - ▶ Confidentiality
 - ▶ Availability
 - ▶ Processing integrity
- ▶ Can cover non financial reporting related processes
- ▶ Gives you the detail about how processes work, as well as operating effectiveness
- ▶ Being mapped to other frameworks (e.g., ISO27001, CSA)

What is a SOC report?

Five sections (typically)

- ▶ Section 1 – Management's assertion
- ▶ Section 2 – Independent Service Auditor's opinion
- ▶ Section 3 – Management's description of process/controls
- ▶ Section 4 – Management's description of controls and auditor's description of tests and results
- ▶ Section 5 – Other information provided by management – usually BCP/DR, not covered by the opinion

What does a SOC report give the user?

- ▶ Sufficient information on process/controls to allow users to assess the control environment
 - ▶ How does the process work?
 - ▶ What can go wrong?
 - ▶ Do controls address these WCGWs?
- ▶ Detailed description of the way controls were tested, and result of each test (for a Type II)
- ▶ Independent opinion, based on testing, on controls, removing need for users (and their auditors) to test them
- ▶ Clear identification of controls remaining with the user, so user can test these ('Complementary User Entity Control Considerations')

What is a SOC1 report?

- ▶ Designed to provide assurance to financial statement auditors
- ▶ Hence, focuses on financial information systems and assertions
- ▶ May be generic or client-specific
- ▶ Type I = design only, Type II = operating effectiveness
- ▶ Service auditor works for outsourcer, not user – so no direct right of access to service auditor

What is a SOC1 report? (cont'd)

- ▶ Management defines scope based on control objectives and locations/processes covered
 - ▶ But you could drive this through your contract
- ▶ Management describes processes and controls
- ▶ Includes description of 'Complementary User Entity Control Considerations'
- ▶ Usually covers at least a six month period (if Type II)
- ▶ Independent auditor opines on accuracy of management descriptions, adequacy of controls design, whether controls are placed into operation, and on operating effectiveness of controls (if Type II)

How does a SOC2 report differ from SOC1?

- ▶ V. like SOC1 – key differences are below
- ▶ Intended to be used for non financial reporting areas
 - ▶ Security
 - ▶ Privacy
 - ▶ Confidentiality
 - ▶ Availability
 - ▶ Processing integrity
- ▶ Control objectives are actually the Trust Services Principles and associated criteria
 - ▶ Organisations must use at least one of these
 - ▶ They then describe their controls that deliver each of the criteria, and the service auditor tests these controls

Key questions a user needs to ask

- ▶ When letting an outsourcing contract
- ▶ At the start of the SOC project
- ▶ As the report progresses
- ▶ Once the report is received

Key questions a user needs to ask (cont'd)

When contracting, in relation to assurance consider these

- ▶ Understand the nature of the services being outsourced, how they impact on your responsibility to report on controls and what controls you expect to retain
- ▶ Clearly identify what you want assurance on, so you can specify this in the contract, and the type of assurance you want for each area (SOC1/SOC2/AUP)
- ▶ Do they already have a SOC report you can see, and is it unqualified?
- ▶ Does it cover the proposed in-scope services?
- ▶ If they do not have a report, and it is important to you, suggest your negotiators build this into the contract

Key questions a user needs to ask (cont'd)

At the start of the SOC project

- ▶ Type I or Type II – does the approach meet your needs?
- ▶ Period
 - ▶ When does period end – close enough to your year end?
 - ▶ Period covered long enough for your needs?
 - ▶ When will report be delivered – early enough for your needs?
- ▶ Is the service auditor credible/acceptable?

Key questions a user needs to ask (cont'd)

At the start of the SOC project (cont'd)

▶ Scope

- ▶ Does it cover the services you are using – data centres, processes, teams providing services, and has the service model changed since prior year?
- ▶ Are you comfortable that, if the report is generic, the processes are those being used to support you?
- ▶ Are you clear on which controls remain with you, and what you will do about them?

▶ Control objectives

- ▶ Do these cover the areas you need?

Key questions a user needs to ask (cont'd)

As the report progresses

- ▶ Is it the project on track to deliver to the agreed dates?
- ▶ What issues/deviations are emerging?
- ▶ Consider requesting regular updates/calls
 - ▶ Keeps you aware of the likely final opinion
 - ▶ Allows you to look for compensating controls that you may have that could mitigate a qualified SOC report
- ▶ Ask for an early view of the controls being tested, to map to your internal framework – or ask service organisation to map their controls to your framework

Key questions a user needs to ask (cont'd)

Once the report is received – Section 2, independent opinion

- ▶ Scope is the agreed locations?
- ▶ Period/end date are the agreed ones?
- ▶ Qualified opinion?
 - ▶ Not immediately obvious – need to read opinion paragraphs carefully – *“In our opinion, **except for the deficiency in operating effectiveness and the non-achievement of the related control objective noted in the preceding two paragraphs**, the controls that were tested, as described in the Description, were operating with sufficient effectiveness...”*

Key questions a user needs to ask (cont'd)

Once the report is received – Section 3, Description

- ▶ Scope
 - ▶ Does it cover the agreed scope – and is this still enough?
- ▶ Control objectives
 - ▶ Do these still cover the areas you need?
- ▶ Process descriptions/controls
 - ▶ Do these have enough detail?
 - ▶ Are the controls appropriate/do they map to what you expect to see?
- ▶ Complementary User Entity Control Considerations
 - ▶ How will you test these? Are you operating them?

Key questions a user needs to ask (cont'd)

Once the report is received – Section 4 Description of testing

- ▶ Controls tested
 - ▶ Do the controls properly deliver all the key words in the control objective
- ▶ Approach to testing
 - ▶ Is it thorough enough – not just observation/inquiry?
 - ▶ Are the controls tested in a sensible way?
 - ▶ Should not need to know if items were tested relating to your company – but can ask?

Key questions a user needs to ask (cont'd)

Once the report is received – Section 4 Description of testing (cont'd)

- ▶ Results of testing
 - ▶ Are deviations acceptable to you in supporting final opinion?
 - ▶ Do you want extra work in specific areas based on deviations noted?
 - ▶ Can ask if deviations were on items relating to your company – should not matter, but can ask?
 - ▶ What do the deviations means from a SOx reporting perspective?

Questions/discussion

What more do you want to know?

Mark Russell

mrussell@uk.ey.com

+44 777 570 4639

Disclaimer

The information in this pack is intended to provide only a general outline of the subjects covered. It should not be regarded as comprehensive or sufficient for making decisions, nor should it be used in place of professional advice.

Accordingly, Ernst & Young LLP accepts no responsibility for loss arising from action taken or not taken by any party using this information.

The information will have been supplemented by matters arising from any oral presentation by us, and should be considered in light of this additional information.

If you require any further information or explanations, or specific advice, please contact us and we will be happy to discuss matters further.



Thank you

 **ERNST & YOUNG**
Quality In Everything We Do