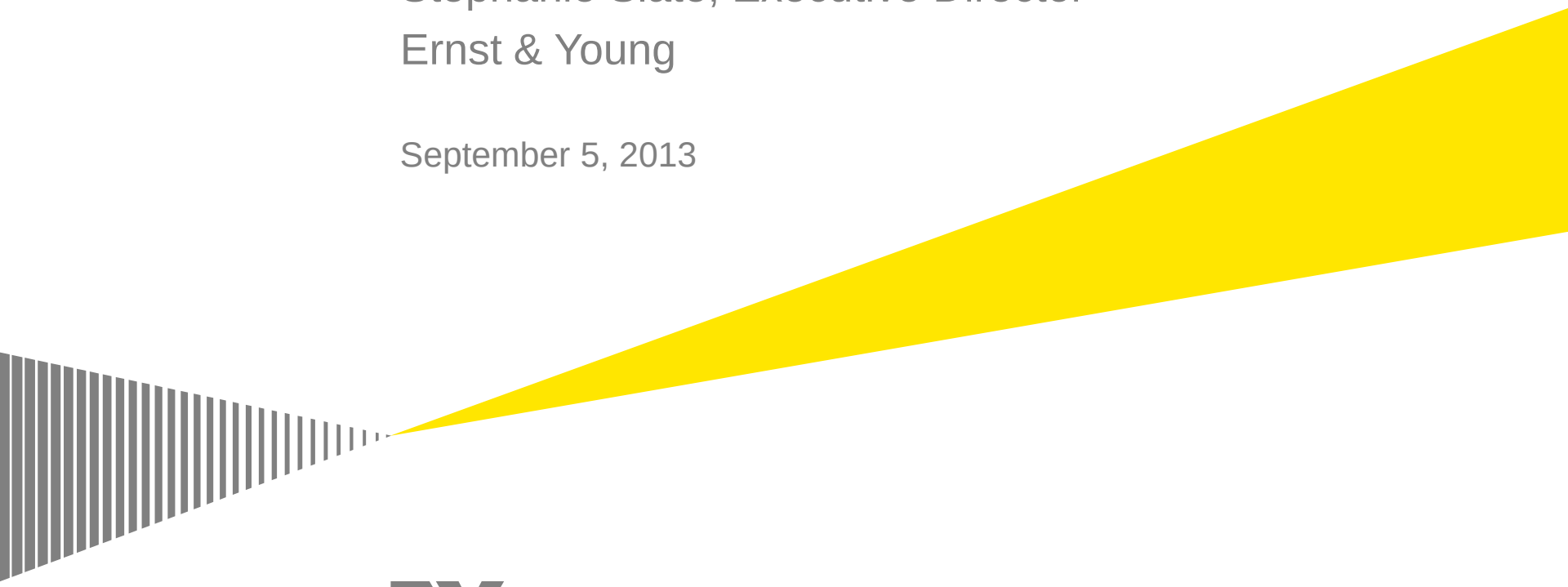
So You Think You Know SOC?

Institute of Internal Auditors
Stephanie Slate, Executive Director
Ernst & Young

September 5, 2013



EY
Building a better working world

Agenda

- The role of internal controls when outsourcing
- Objectives and risks of outsourcing
- Role of SOC reporting
- Establishing internal controls when outsourcing
- Evaluating SOC reports
- Current State of SOC Reporting – Things are Changing

Internal Control

The role of internal controls when outsourcing

- Internal control should help achieve business objectives
  - Agility—adapting to changing business and operating environments
  - Confidence—mitigating risks to an acceptable level
  - Clarity—providing reliable information supporting sound decision-making.
  - Accountability – provides owners and establishes segregation of duties
  - “Checks and Balances”

Internal control is an objective unto itself

- Sound business practice
- Effectiveness and efficiency of operations
- Reliability of reporting
- Compliance with applicable laws and regulations

Regulatory landscape

- SOX
- PCAOB
- HIPAA
- FISMA/NIST
- FedRAMP
- PCI
- Cloud
- FFIEC
- ISO 27001

Management’s and Internal Audit’s responsibilities do not change if a vendor is used to perform some business functions

User auditor’s responsibilities

The financial auditor also has responsibilities when a user entity outsources.

AU-C 402 .7

The objectives of the user auditor, when the user entity uses the services of a service organization, are to

a. obtain an understanding of the nature and significance of the services provided by the service organization and their effect on the user entity’s internal control relevant to the audit, sufficient to identify and assess the risks of material misstatement.

b. design and perform audit procedures responsive to those risks.

Objectives and Risks of Outsourcing

Some common objectives of outsourcing

- Improve business focus
- Improve capabilities
- Improve use of capital/resources
- Improve operations
- Reduce cost
- Improve compliance
- Reduce risk/share risk with others

Risk of outsourcing

- Financial reporting
- Operational
  - Cost
  - Processing integrity
  - Data security/confidentiality
  - Lack of availability
  - Failure to deliver on requirements
  - Strategic risk
- Compliance

Risk of outsourcing—user auditor POV

- Process understanding
- Control risk
- Audit risk
- Regulatory risk

Role of SOC Reports

Role of SOC reports

- A Service Organization Controls 1 (SOC 1 or SSAE 16) report is designed to help a user entity evaluate the impact of controls at a service organization on its internal control over financial reporting.
- A SOC 2 report is designed to help a user entity evaluate the impact of controls at a service organization relative to many of the other risks of outsourcing.

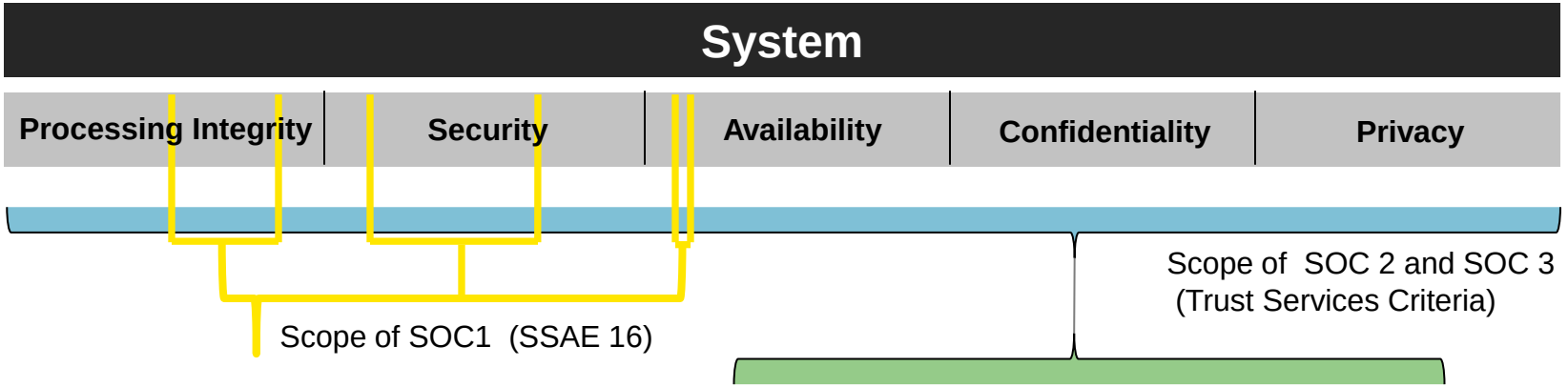
Independent assurance options to enhance service organization communications to its stakeholders

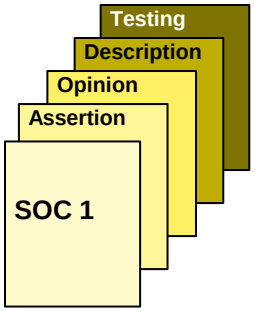
Report type	Intended users	Subject matter /format	Distribution limitations
SOC 1 ▶ **Intl:** ISAE 3402 ▶ **US:** SSAE 16 ▶ **Other countries:** None	▶ Auditor's of the user entity's financial statements ▶ Management of the user entities ▶ Management of the service organization	➢ Type 1 or Type 2 ➢ Long -form report ➢ Description of controls and systems ➢ Tests performed and results of testing	▶ Restricted to current customers ▶ May be shared with prospective customers if third-party access letter is obtained ▶ Not intended for investors or other prospective users
SOC 2 ▶ **Intl:** ISAE 3000 ▶ **US:** AT101 ▶ **Other countries:** None	▶ Management of the user entities ▶ Management of the service organization. ▶ Other relevant parties that require assurance over the subject matter. For example: ▶ Business partners ▶ Regulators ▶ Employees	➢ "SOC1 look-alike report": ➢ Long -form report ➢ Description of controls /systems ➢ Tests performed & results ➢ Controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy. ➢ Organization reports controls in place to meet prescribed principles/criteria ➢ Type 1 or Type 2	➢ Restricted to users with "sufficient knowledge" ➢ e.g., current and prospective customers, business partners, regulators, employees
SOC 3	➢ Same as SOC 2	➢ Short-form report ➢ Limited description of controls/systems	➢ No restrictions ➢ e.g., mass distribution, web-site, current & prospective customers
Agreed-upon procedures	➢ Internal-use ➢ Named business partners	➢ No description of controls/systems ➢ Report includes only results of specific tests performed and findings	➢ Restricted to internal and/or named parties

Trust services principles for SOC2 & SOC3

- **Security** — The system is protected against unauthorized access (both physical and logical).
- **Availability** — The system is available for operation and use as committed or agreed.
- **Processing integrity** — System processing is complete, accurate, timely, and authorized.
- **Confidentiality** — Information designated as confidential is protected as committed or agreed.
- **Privacy** — Personal information is collected, used, retained, disclosed, and disposed of in conformity with the commitments in the entity's privacy notice and with criteria set forth in Generally Accepted Privacy Principles GAPP issued by the AICPA and Canadian Institute of Chartered Accountants.

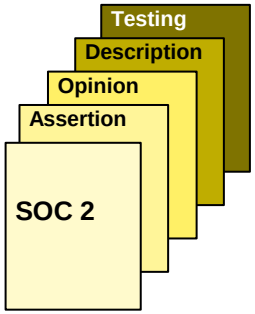
SOC 1, SOC 2, SOC 3 comparison





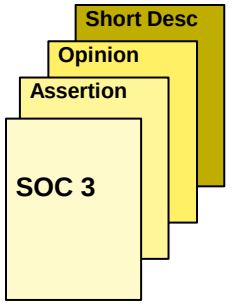
Users:

User entity controller
User entity SOX department
User auditor



Users:

User entity security
User entity compliance
User entity vendor management
Regulators
Prospective user entities



Users:

General public

Establish Internal Controls When Outsourcing

How to Establish Internal Control When Outsourcing – Internal Audit's Role

- Often times, management looks to Internal Audit to ensure internal controls are established by the service organization and to ensure the controls are working properly
- Best solution is to integrate into existing Governance, Risk and Compliance (GRC) processes
  - System process and controls design and implementation
    - Integrate vendor into business processes
    - Evaluate/specify vendor controls
  - Ongoing vendor management
    - SLAs
    - Monitoring
    - Third party reporting (SOC reports)

How to Establish Internal Control When Outsourcing – Internal Audit's Role

- Identify internal stakeholders
- Identify risks
  - Operational
  - Financial
  - Legal and regulatory
- Implement controls, mitigate or accept the risks at the company and the service organization
  - View controls at the vendor as a mitigation technique
  - Need to establish controls over mitigation
- Controls and evidence of controls operation need to be part of service definition in contract
- Evaluate report against expectations

Evaluating SOC Reports

Evaluating the scope

- Internal Audit very frequently leads this effort
- Services, systems, locations covered
  - Does it cover the areas of concern?
  - Does it cover all of the processes outsourced to each vendor?
  - What is missing?
- Control objectives (SOC 1) or principles (SOC 2)
  - Map to areas of concern
  - Match to contractual requirements
  - Evaluate completeness, accuracy, timeliness, etc.

Evaluating control objectives when using a SOC 1 report

- Identify information/reports that flow to the financial statements
- Identify financial statement assertions impacted by the information identified
- Evaluate control objectives
- Underlying process control objectives
- Include disclosures
- Electronic audit evidence

Evaluating the description

- Start with the results/outputs
  - Identification of key reports and data feeds
  - Accuracy of reports
- Work backward
  - Description of process
  - Key controls
  - Inputs and outputs in the flow of transactions
- Does it meet the company's compliance requirements?
- Is it at the right depth?
- Special considerations regarding processing integrity in a SOC 2
- What is missing?
- What strikes you as curious?

Evaluating the controls

- Are they what is expected?
  - Map to your risks
  - Map to known risk models
  - Map to contractual requirements
- Are they described in sufficient detail to permit you to separately evaluate their design?
- What processes, technologies, services are missing or are not described fully?

CUECs

- Are they relevant to internal control or a protection mechanism for the service organization/auditor?
- Do they really describe what you should be doing?
- Is it consistent with documentation/contracts, etc.?
- Have you implemented them?
- Have you evaluated their operation and documented it for your financial auditor?

Management's assertion

- What is the coverage period? Does it meet your needs?
- Are the criteria complete?
- Any subservice organizations? If so are they carved-out or included?
- Anything unusual?

Service auditor’s report

- What standard is used?
- Who is this firm?
- Where was it issued?
- Any carve-out or unusual items noted in the scope description?
- Any qualifications?
- For SOC 2 reports, are there any opinions on subject matter other than internal control (e.g., compliance)?
- Any inconsistencies with professional standards or unusual items?

Service auditor’s test and results

- Are the tests described in a way that lets you understand the nature of what was performed?
- Are they the “right” test for the control?
  - Responsive to the control
  - What would our financial auditor have done
- Are any deviations described sufficiently to permit the evaluation of the impact?
- What is the service organization management’s response?
- Have there been any other communications on the issue?

Current State of SOC Reporting – Things are Changing

Environment observations

- SOC 1
  - Increase in user auditor evaluation of reports as insufficient
  - Regulatory reviews
  - Companies receive the report very late in the reporting cycle so there is little time to analyze impact of deviations and to evaluate CUECs
- SOC 2
  - Experiencing growth but questions on how these fit for financial statement purposes
  - Specific purpose – privacy reports
- SOC 3/SysTrust
  - Renewed growth
  - Common add-on to SOC 2 – leverage same work but can these fit for financial statement purposes

Environment drivers

- PCAOB findings/observations
  - Coverage period insufficient
  - Lack of integration of SOC reports into the audit
  - Lack of detail in the report especially related to electronic audit evidence and how controls directly relate to financial statement assertions
- Users taking a closer look at reports
- Timeliness of receipt of report by users
- **AICPA Audit Risk Alert (ARA) for users issued July 2013**
- **New SOC 1 Guide issued June 2013**

ARA Identified Report Issues

- Management's description does not address the services provided
  - ITGCs only when service is not infrastructure outsourcing
  - Does not describe the procedures and flow
  - Does not describe financial statement accounts affected / electronic audit evidence and reports used or generated in the flow of transactions
- Deviation in opinion language from standard
- Clarity of disclaimed or adverse opinion
- Description is insufficient for user auditor needs
- Design or operation of controls are not sufficient for the particular needs of client

ARA Guidance - User auditor actions in response to report issues

- Request a new report
- Obtain additional evidence from the user entity
- Obtain additional representations regarding completeness and accuracy of the description
- Visit the service organization and perform procedures
- Request the service organization to engage service auditor to perform additional procedures

SOC 1 Audit Guide Changes

- Detail of description of the system
  - Consider flowcharts
- Example of appropriate control objectives
- Sub-service organizations
- Complementary user entity controls
- Controls do not operate during the period
- No forward looking management responses to deviations
- Indirect user entities
- IT-only reports

Subservice organizations

- Significant additions to guidance on determining whether a “vendor” is a subservice organization (3.14)
- Guidance on the whether treatment as a subservice organization is needed (3.34)
- Inclusive method
  - Guidance on assertions of inclusive subservice organizations (3.21)
  - Controls at an inclusive subservice organization presented separately from those of service organization (3.29)
- User auditors must apply new rules in effect 15 December 2012 on reliance upon SOC1 reports (and includes carved-out subservicers)
- May need to obtain SSO report

Subservice organizations

- Carve-out method
  - For carved-out reports, primary service organization is strongly encouraged to identify (name) the subservice organization (3.26)
  - Description contains sufficient information for user to identify the information needed from subservice organization (3.30)
  - Controls at primary service organization include monitoring of subservice organization (3.31)
  - **When a primary service organization has a carved-out subservice organization, the primary service organization is encouraged to clearly document how it addresses subservice organization CUECs (3.32)**
  - **When control objectives listed are partially achieved by subservice organization controls, describe those controls at the subservice organization that are necessary to "complete the loop".(3.71)**

Complementary User Entity Controls

- Make sure that the CUECs align with the control objectives
- Service organization should challenge their current CUECs for completeness and appropriateness
- Preference is now to include CUECs in the actual control / test matrix rather than a separate listing in the description of the system

Controls not operating during the period

- When controls do not operate during the period (4.120-4.126)
  - May be able to be tested through other controls
  - **Amendments to assertion/opinion are necessary if not tested through other controls**
    - **Amend assertion to disclose the facts and circumstances**
    - **Amend service auditor's report scope and add emphasis of a matter paragraph**
  - Service organization may provide additional information in Section 5 which is unaudited and if so is covered by the service auditor's disclaimer paragraph

Testing Deviations

Table 5-1

Information to Be Included in the Description of Tests of Controls

Table 1.

Information to Be Disclosed	*If No Deviations Were Identified*	*If Deviations Were Identified*
The controls that were tested	Required	Required
Whether the items tested represent all or a selection of the items in the population,	Required	Required
The nature of the tests performed	Required	Required
The number of items tested		Required
The number and nature of the deviations		Required
Causative factors (for identified deviations)		Optional[fn 1]

Testing Deviations – changes

- If management's responses to deviations in tests of controls are included in the description of the service organization's system (rather than in the section containing information that is not covered by the service auditor's report), such responses usually are included in the portion of the description that describes the controls and related control objectives. (same as before)
- **In that case, the service auditor should determine through inquiries in combination with other procedures whether there is evidence supporting the action described in the response. (new)**
- **If the response includes forward-looking information, such as future plans to implement controls or to address deviations, such information should be included in the section "Other Information Provided by the Service Organization." (new)**

Management's Responses - Conclusion

- The service auditor needs to validate the current response as part of their procedures.
- Management no longer permitted to include forward-looking responses in Section IV.
- Can add such forward-looking information to unaudited section of the report (auditor also adds disclaimer language to the opinion).

Indirect user entities

- AICPA defined new term: “indirect user entity”
  - a user entity of a service organization is also considered a user entity of the service organization’s subservice organization if controls at the subservice organization are relevant to the user entity’s internal control over financial reporting.
  - **In such case, the user entity is referred to as an indirect or downstream user entity of the subservice organization.**
  - Consequently, an indirect or downstream user entity may be included in the group to whom use of the service auditor’s report is restricted.

Determining an indirect user entity

- Whether the service provided by the subservice organization is relevant to the potential indirect user entity's internal control over financial reporting:
  - The significance of the services provided by the subservice organization to the potential indirect user entity
  - The nature and materiality of the transactions processed or accounts or financial reporting processes affected by the subservice organization's services
  - The degree of interaction between the activities of the subservice organization and those of the service organization
  - Whether the primary service organization implements effective user entity controls and monitoring that are sufficient for the indirect user entity and therefore negate the need for the subservice organization's type 1 or type 2 report

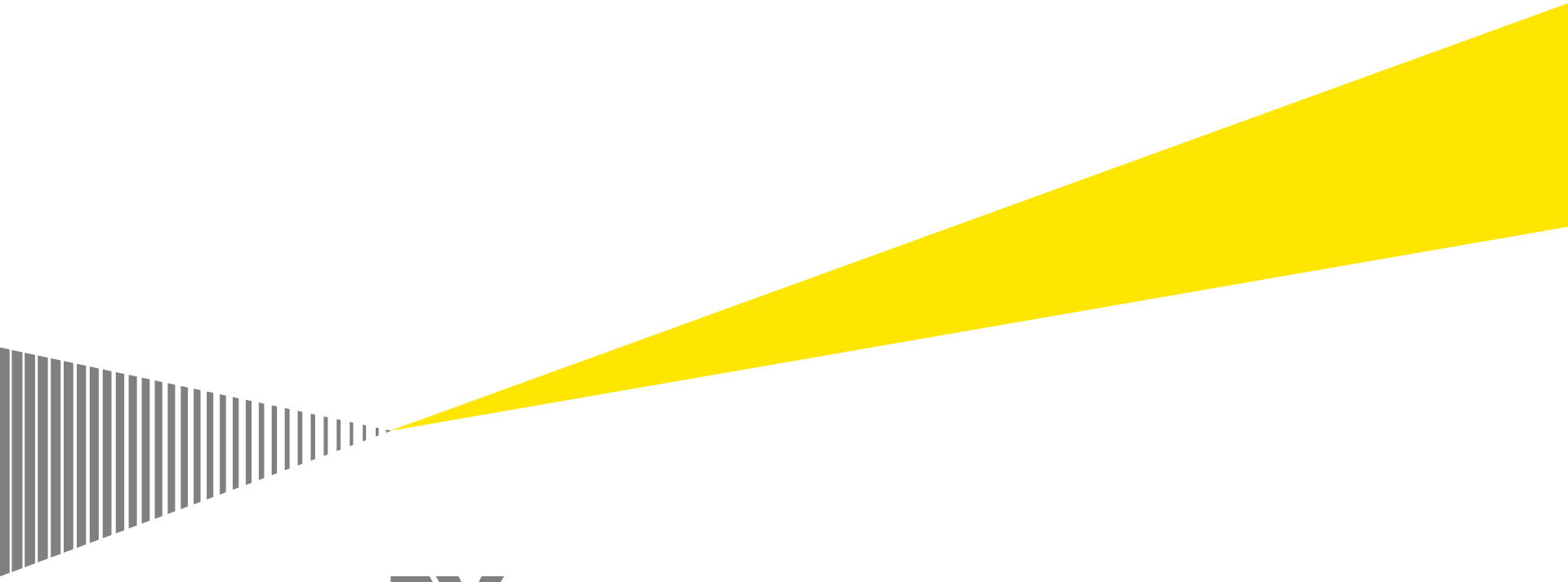
IT Only Reports

- General IT controls only reports are no longer appropriate if the main service being provided is transaction processing. These reports should include transaction processing since it is significant to the user entity's financial statement assertion or move to a SOC 2.
- General IT controls only reports are still appropriate if IT hosting services are the only service that is being purchased.

Changes - SOC 2 Guide / Trust Services Criteria

- Trust Services criteria to be updated in response to identified concerns:
  - Duplicate criteria
  - Clarify wording
  - Add example risks and illustrative controls
- Increase consistency with ISO/NIST
  - Additional focus on organizational risk management
- 2013 - Anticipated exposure draft of updated Trust Services Criteria
- **Anticipated to be effective for reports in 2014**

Questions?



Building a better working world