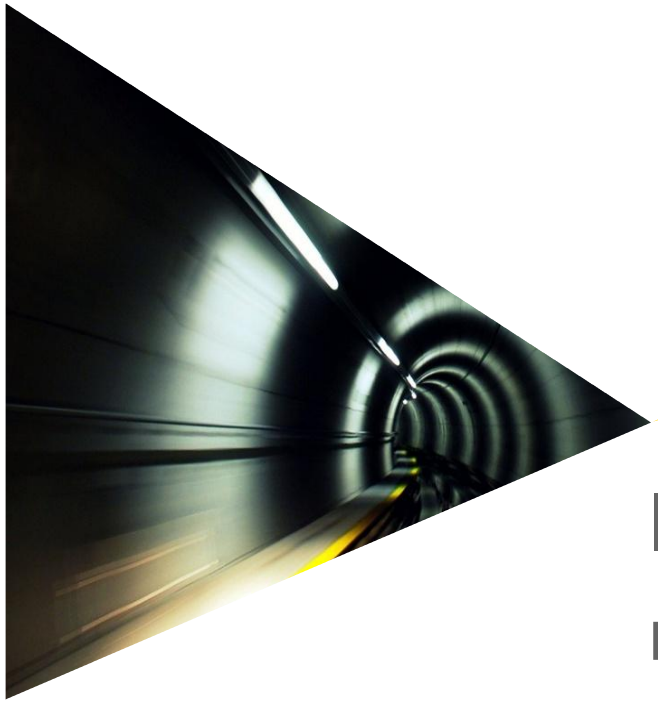


ISAE 3402

How to benefit from early adopters?

Round Table ISACA NL

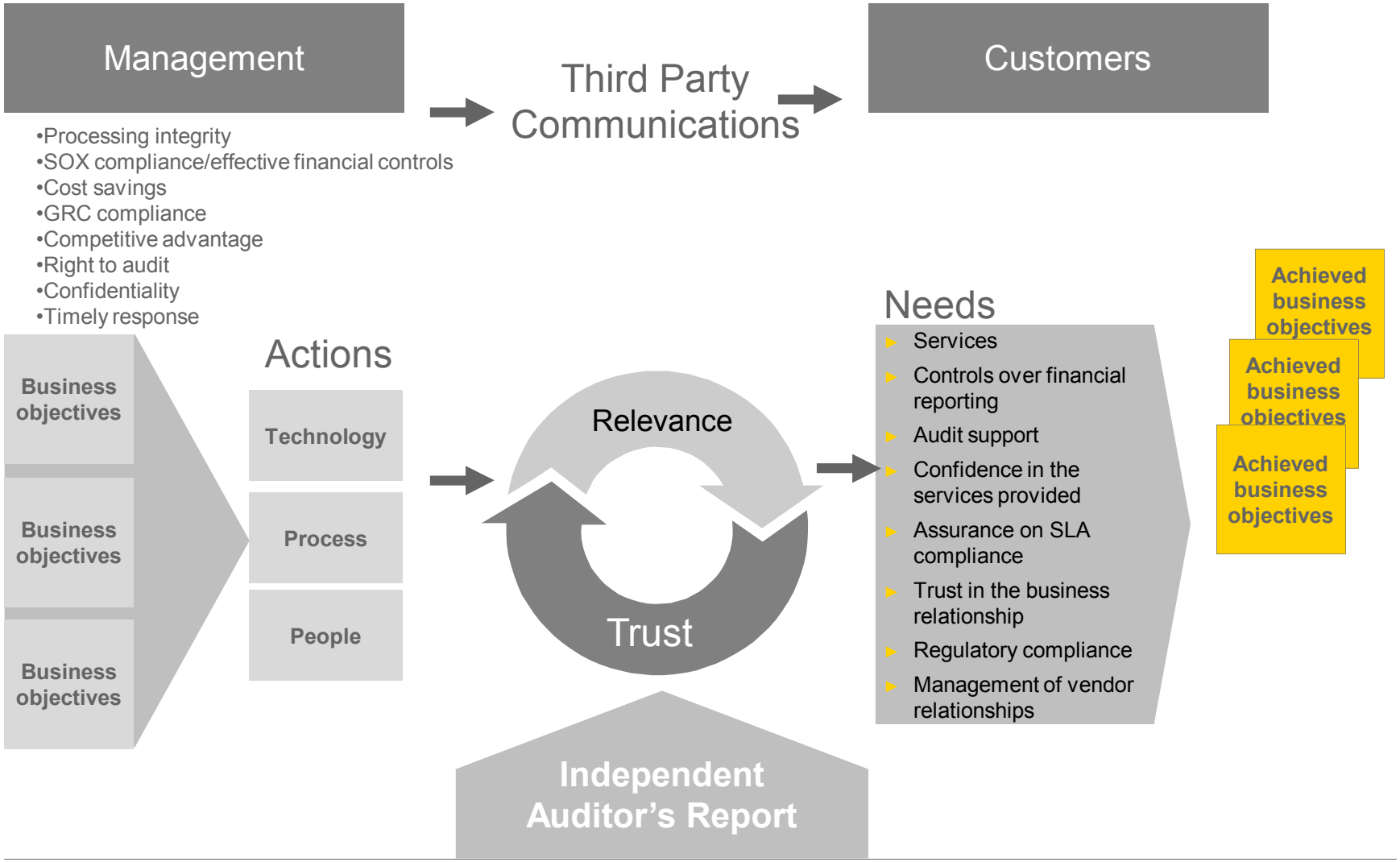
Dennis Houtekamer

Ernst & Young
Quality In Everything We Do

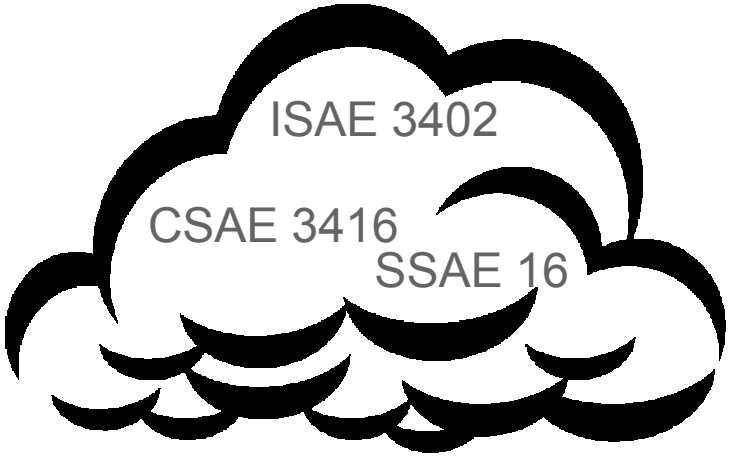
Agenda

- Introduction
- ISAE 3402 /
  SAS No. 70 rapport (type II)
- Jaar 2009
- -Report dated early 2010
  -Combination of ISAE 3402 and SAS 70
  -ISAE 3402 assurance opinion for the year 2009
  -Applicable law?
- -
- -

Service Organization Control Reports



SOC 1 Reports
Quick note on terminology



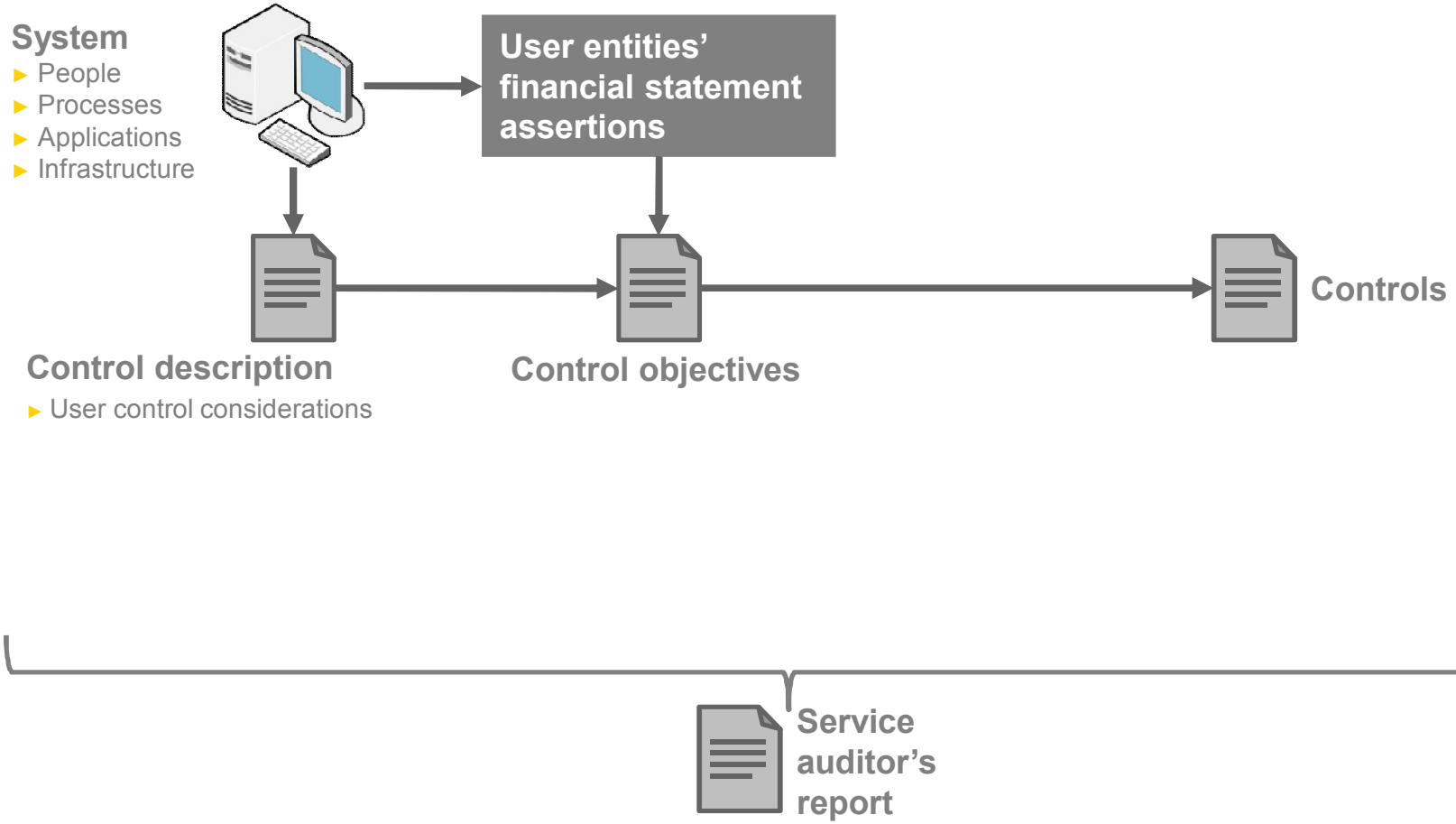
Service Organization Controls (SOC) 1 Reports

Why SOC 1?

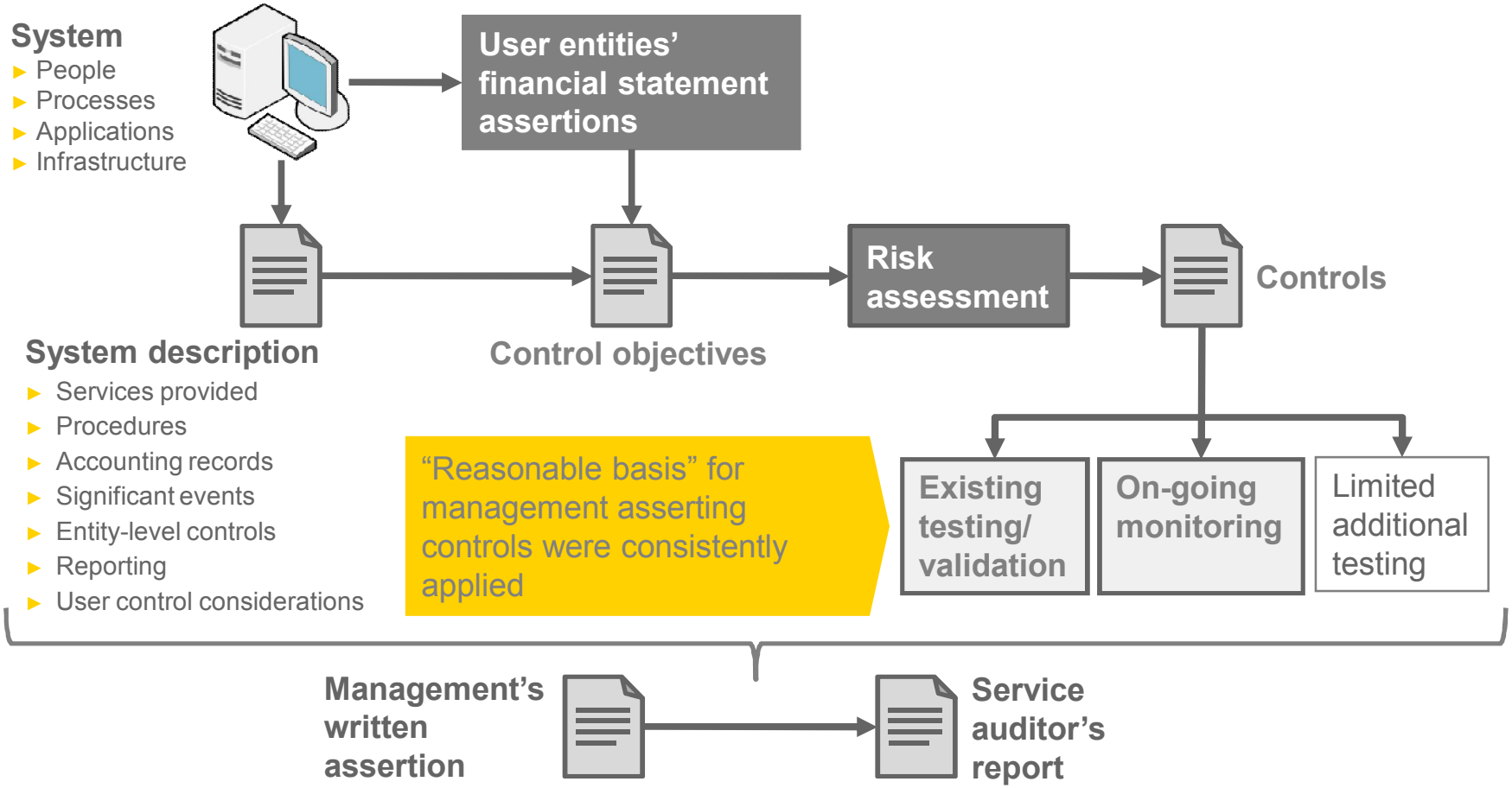
- Many differing standard names for substantially equivalent reports
- Will not change as standards get updated
- Easier to say than ISAE 3402/SSAE 16
- Relationship with other SOC reports

Key Drivers of Change for Third Party Reporting:
- Growth of business process outsourcing
- Widely used SAS70 standard is a US Standard
- Growing need for a 'Service Organization Report'

SOC 1 Reports
Quick note on terminology - SAS 70



SOC 1 Reports
Quick note on terminology SOC1 – elements



SOC 1 Reports
Requirements for system description

- Types of **S**ervices provided including the classes of transactions processed
- The **P**rocedures by which services are provided, including, procedures by which transactions are initiated, authorized, recorded, processed, corrected, transferred to the reports and other information prepared
- The **A**ccounting records and supporting information involved and how information is transferred to the reports and other information prepared
- How the system captures and addresses **S**ignificant events and conditions other than transactions
- Relevant **E**ntity-level controls (e.g., control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls
- The process used to prepare **R**eports and other information for user entities

SOC 1 Reports
Requirements for system description (2)

- The specified control objectives and controls
- Complementary user entity controls contemplated in the design of the service organization's controls
- In the case of a type 2 report, details of **changes to the service organization's system** during the period covered by the description
- Whether management's description of the service organization's system **does not omit or distort information** relevant to the service organization's system
- Description of the service organization's system is prepared to meet the common needs of a broad range of user entities and their user auditors

SOC 1 Reports / Risk assessment (1)
Management's identification of risks

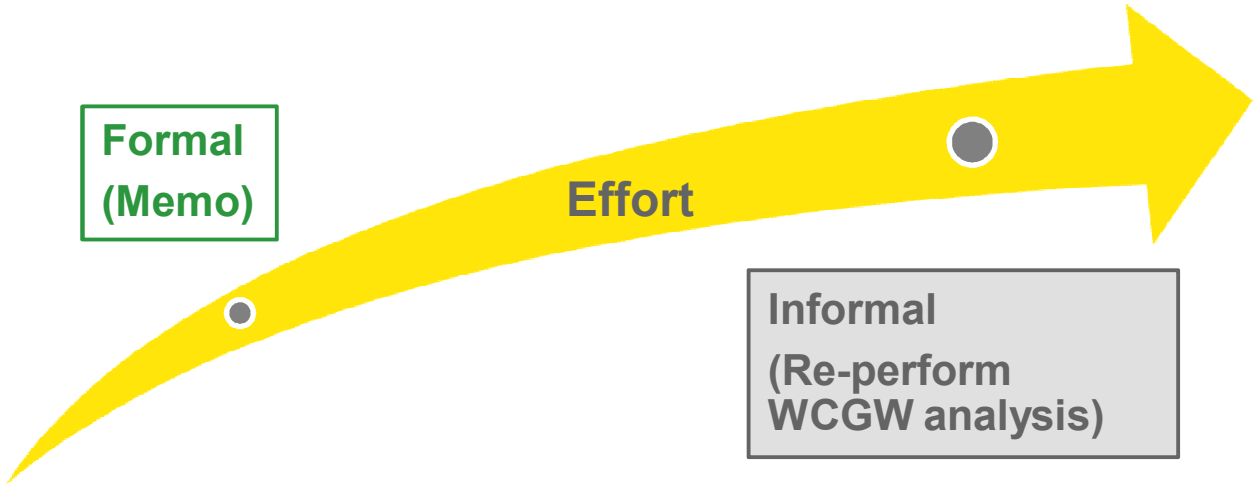
Focused on risks that threaten the achievement of the control objectives:

- Informed by materiality
- User entity financial statement assertions affected

SOC 1 Reports / Risk assessment (2) Assessment of management's process

Determine if management's assertion is fairly stated:

- When a **formal** process is used – obtain the documentation and write a memorandum
- When an **informal** process is used – re-perform the risk assessment (WCGW analysis) and conclude on the results



SOC 1 Reports / Risk assessment (3)
Example risk assessment tool

Process:	
Control objective #1:	

User Financial Statement Assertions Addressed by this Control Objective:

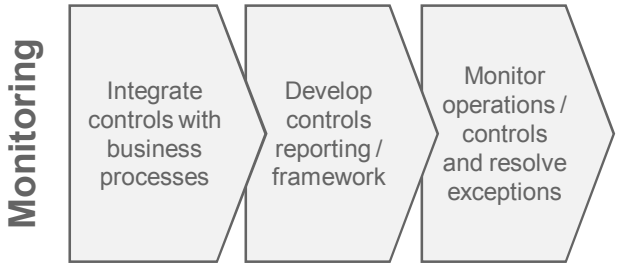
☐ Completeness ☐ Existence/occurrence ☐ Presentation and disclosure
☐ Rights and obligations ☐ Valuation/measurement

Risk	Controls	Basis for asserting control is in place and functioning
Controls at the service organization		
		Choose the nature of the basis.
		Choose the nature of the basis.
		Choose the nature of the basis.

SOC 1 Reports / Risk assessment (4) Integrate Monitoring

Monitoring controls can increase efficiency and transparency:

- Monitoring processes will provide evidence that the underlying controls are operating effectively and can avoid need for direct control testing
- Consider formalizing management monitoring activities so that evidence of these activities is available to support your ISAE 3402 assertion, some examples include
  - Supervisory review of control procedures
  - Quality assurance programs
  - Management reports
  - Service-level agreement reporting
  - Regular internal audits
  - Complaint/incident management



- Monitoring controls provide a ‘catch all’ mechanism to identify and deal with problems and exceptions
- Integrating monitoring controls in your ISAE 3402 framework can help close the gap regarding reporting expectations and provide users with greater transparency

Agenda

- Introduction
- Service Organization Control Reports
- Service Organization Controls 1 – Reports
- Lessons learned
  - General
  - Deviations
  - Testing
- Service Organization Controls 2/3 – Reports
- Closing and other discussion

Lessons learned
General (1)

Service organization process begins by considering the written assertion

- Elements of the assertion
  - The description fairly presents the System made available to customers during some or all of the period [date] to [date] for processing their transactions. Management will need to describe the criteria used in making this assertion
  - The description includes relevant details of changes to the system during the period from [date] to [date].
  - Risks that threaten the achievements of the control objectives have been identified
  - The controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period [date] to [date] to achieve those control objectives.
  - Basis for elements of the assertion, especially operating effectiveness
- Determine who in the organization will authorize the assertion
- What documentation will the approver be provided to evidence that the organization has complied with the elements of the assertion
  - Report description
  - Risk identification (do not enclose assessment in the report)

Lessons learned
General (2)

Develop process for addressing requirements

- Assess current report
  - Common areas for improvement
    - Accounting and other records
    - Error correction processes
    - How reports and other information are created and distributed
  - Other changes to be made
- Determine risk identification process
  - Leverage current process or create new process?
  - Level of formality in process (especially at mid-sized companies)
- Basis for asserting that controls are operating effectively
    - Monitoring and leverage of other types of testing (e.g., SOX and Internal Audit)
    - Minimize direct testing
    - Formal or informal documentation

Lessons learned
General (3)

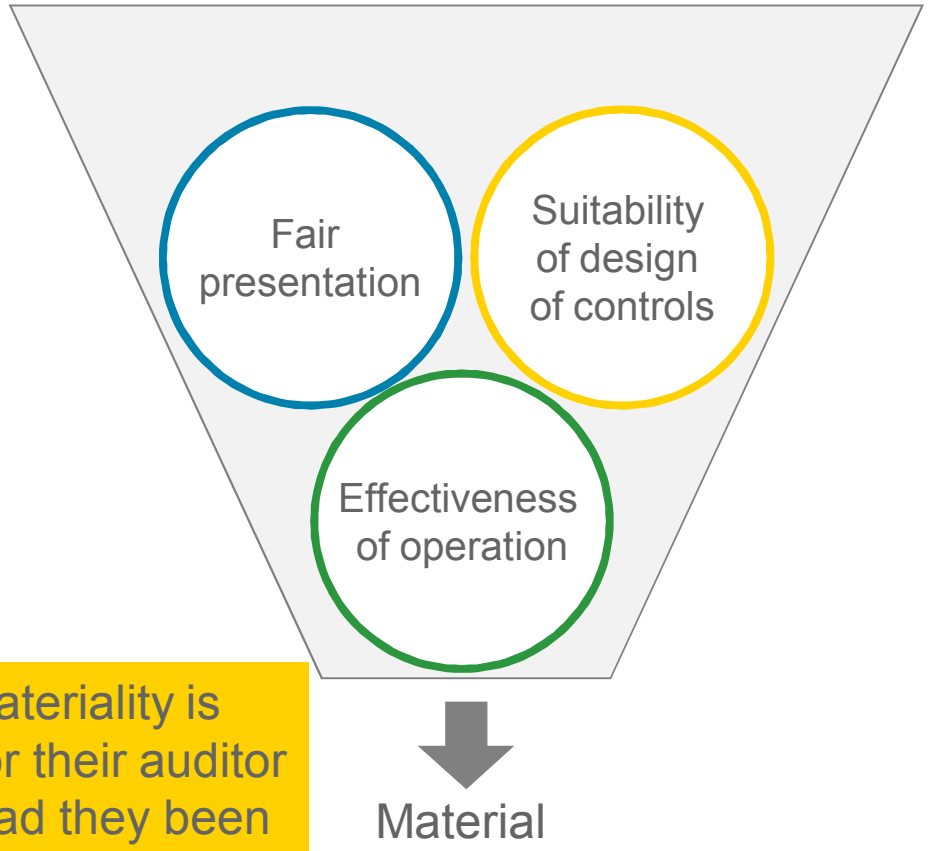
- Subservice organizations can still be treated under the carve-out or inclusive method
- Inclusive method—subservice organization will need to provide a separate management assertion letter for the primary service auditor's report
  - May be difficult to obtain
  - Alternatives to an inclusive report
    - Provide subservice organization's ISAE 3402/SSAE 16 report directly to your customers
    - Report on controls over subservice organization that have been implemented by the service organization
- Carve-out method—obtain agreement to redistribute subservice organization SOC 1 report

Agenda

- Introduction
- Service Organization Control Reports
- Service Organization Controls 1 – Reports
- Lessons learned
  - General
  - Deviations
  - Testing
- Service Organization Controls 2/3 – Reports
- Closing and other discussion

Lessons learned
Deviations

"The service auditor shall consider materiality with respect to the fair presentation of the description, the suitability of the design of controls and, in the case of a Type 2 report, the operating effectiveness of controls when planning and performing the engagement."



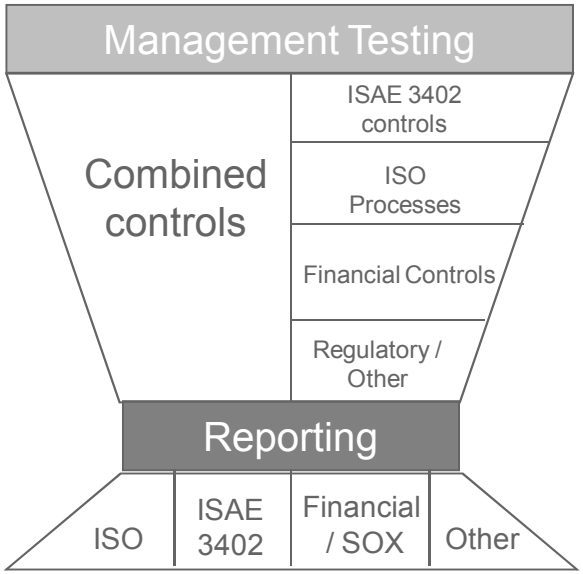
Our basis for evaluating materiality is whether a typical user entity or their auditor would change their actions had they been made aware of the additional information

Lessons learned
Testing

Efficiency and Effectiveness in Testing can be increased through:

- Alignment of Management Testing Activities
  - Review the various control frameworks in place for commonality
  - Develop a management assessment approach that integrates testing procedures and plans for common processes into a single test
  - Leverage existing control reporting testing such as SOx, etc.
  - Align testing activities with internal auditor to reduce effort needed in the external evaluation and to support management assessment

- Evaluation of Current Mix of Controls
  - Expanded use of application controls within the process can reduce the amount of testing work needed because system configurations are often easier to validate than manual reviews
  - Reliance on monitoring controls provide higher level insight into the operating of the underlying controls in the process



Lessons learned - recap

- ISAE 3402 (can) have a significant impact on service organizations
- Project is often too late started
- Set-up/ structure of risk assessment
- Implementation revised (monitoring) controls
- Communication
  - Internal and external stakeholders
- Service organizations do not fully make use of the benefits of ISAE 3402
  - Multi audit approach
  - Internal audit departments
- Harmonization efforts auditors still ongoing

Agenda

- Introduction
- Service Organization Control Reports
- Service Organization Controls 1 – Reports
- Lessons learned
- Service Organization Controls 2/3 – Reports
- Closing and other discussion

Service Organization Control Reports

Quick Links

SOC Brochure

Browse

By Document Type

Article (5)
Overview (4)
FAQ (1)

By Topic

Auditing Standards (4)
Audit and Attest (2)
ASB (2)
Auditing (2)
Internal Control (2)
... Click to view more

Service Organization Control Reports (formerly SAS 70 reports)

Many companies function more efficiently and profitability by outsourcing certain business tasks or functions to other organizations that have the required personnel, expertise, equipment, or technology to accomplish these tasks. Service Organizations Control (SOC) reports are internal control reports on the services provided by a service organization. SOC reports provide valuable information users need to assess and address the risks associated with an outsourced service. The AICPA provides tools and resources to CPAs, service organizations and user entities needed to build trust and confidence in outsourced services.

CPAs
Provides information to user auditors and service auditors on understanding and performing SOC engagements.

Service Organizations
Provides information to service organization on building trust and confidence in the systems.

Users
Provides information to user entities on how to mitigate the risks associated with outsourcing services.

SOC Reports

Service Organization Controls (SOC) reports are designed to help service organizations build trust and confidence in their service delivery processes and controls through a report by an independent Certified Public Accountant. Each type of SOC report is designed to help service organizations meet specific user needs:

AICPA TV

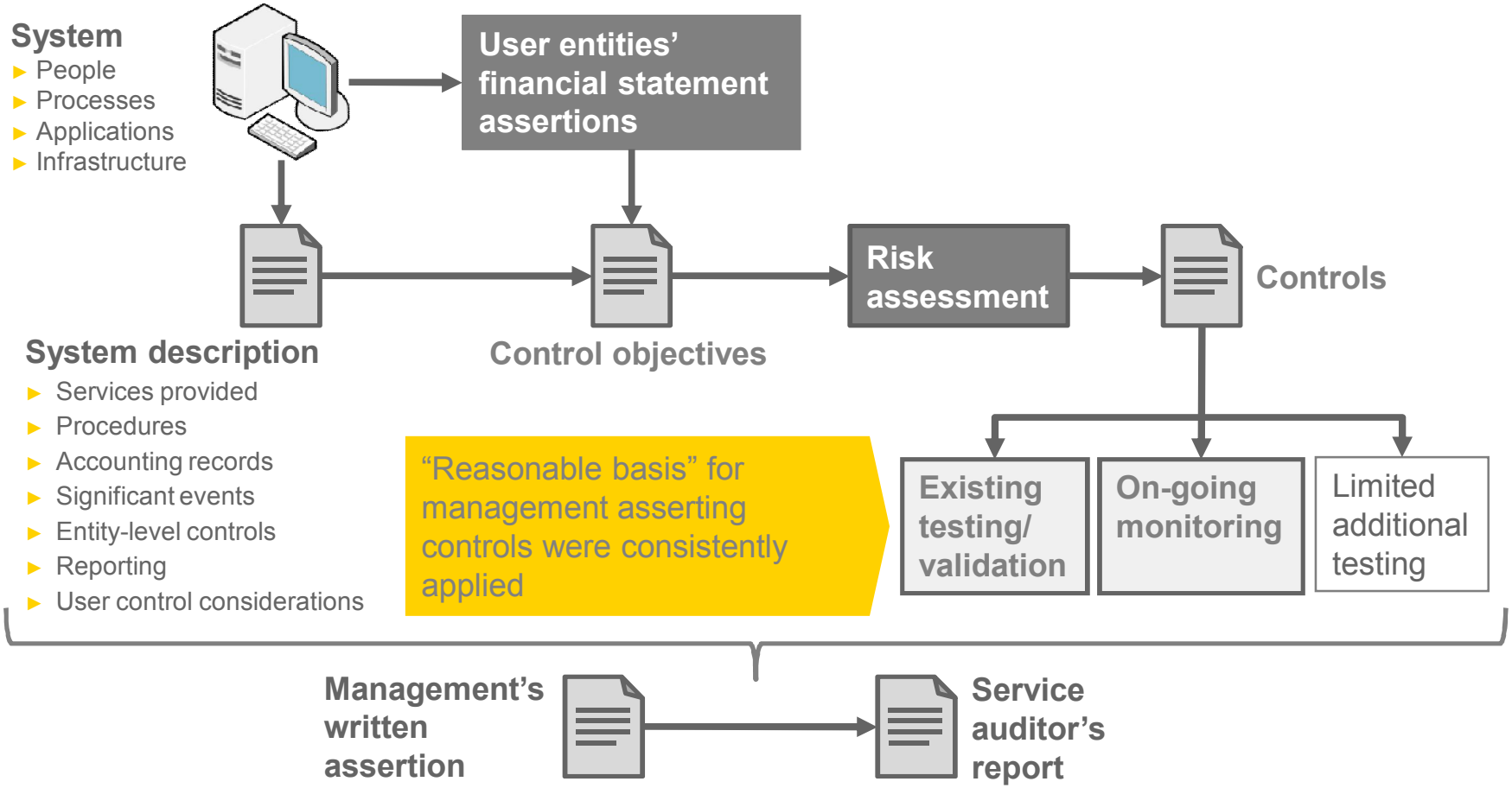
Service Organization Controls 2/3 – Reports (1)

- SOC 2 are reports on internal control related to operating effectiveness and compliance, addressing one (or more) of the following five principles:
  - Security
  - Availability
  - Processing Integrity
  - Confidentiality
  - Privacy
- Report is similar in look and feel of SOC 1 report in format but addresses controls that may not be included in SOC 1
  - SOC 1 & SOC 2 engagements can be “packaged together” as one connected set of activities (but resulting in 2 separate reports)
- SOC 2 can be used as report against common industry standards, such as Cloud Security Alliance framework, ISO 27001, FISAP
- Distribution intended for a broader range of users, including existing users, prospective users, regulators, business partners
- Guidance scheduled for release in May 2011
- U.S. created guidance, but designed for adoption in other countries

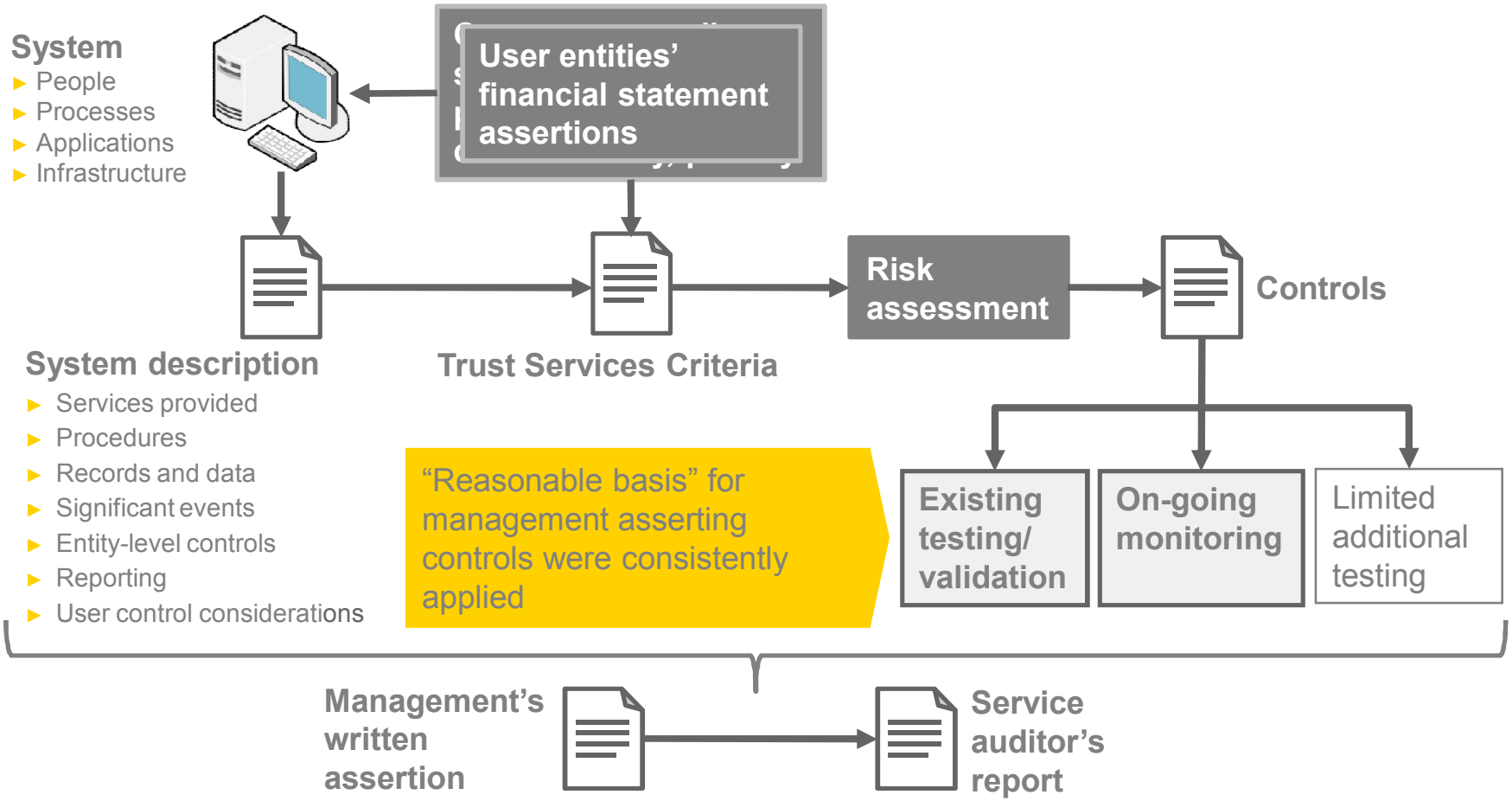
Service Organization Controls 2/3 – Reports (2)
SOC – Overview

Report type	Intended users	Format	Distribution limitations	Example
SOC 1 (SSAE 16, required after 6/15/11, replaces SAS 70)	➢Customers financial statement auditors	➢Long -form report ➢Description of controls and systems ➢Tests performed and results of testing	➢Restricted to current customers	➢Payroll processing ➢Credit card transaction processing
SOC 2 (available after Audit Guide issued – expected May 2011)	➢Users seeking assurance over information handling	➢"SOC1 look-alike report": ➢Long -form report ➢Description of controls /systems ➢Tests performed &results ➢Scope relates to "information handling objectives " (security, availability, processing integrity, confidentiality and/or privacy) ➢Organization reports controls in place to meet prescribed principles/criteria	➢Restricted to users with "sufficient knowledge" ➢e.g., current and prospective customers, business partners, regulators, employees	➢Supply chain information handler reporting on processing integrity ➢Data center outsourcer reporting on security and availability ➢Organization's alignment with ISO 27001 or Cloud Security Alliance framework
SOC 3 (same timing as SOC 2)	➢Same as SOC 2	➢Short-form report ➢Limited description of controls/systems	➢No restrictions ➢e.g., mass distribution, web-site, current & prospective customers	➢Bank reporting on privacy over e-banking application
Agreed-upon procedures (available now)	➢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	➢Compliance with specific controls in vendor contract arrangement

Service Organization Controls 2/3 – Reports (3)
SOC 1 – elements

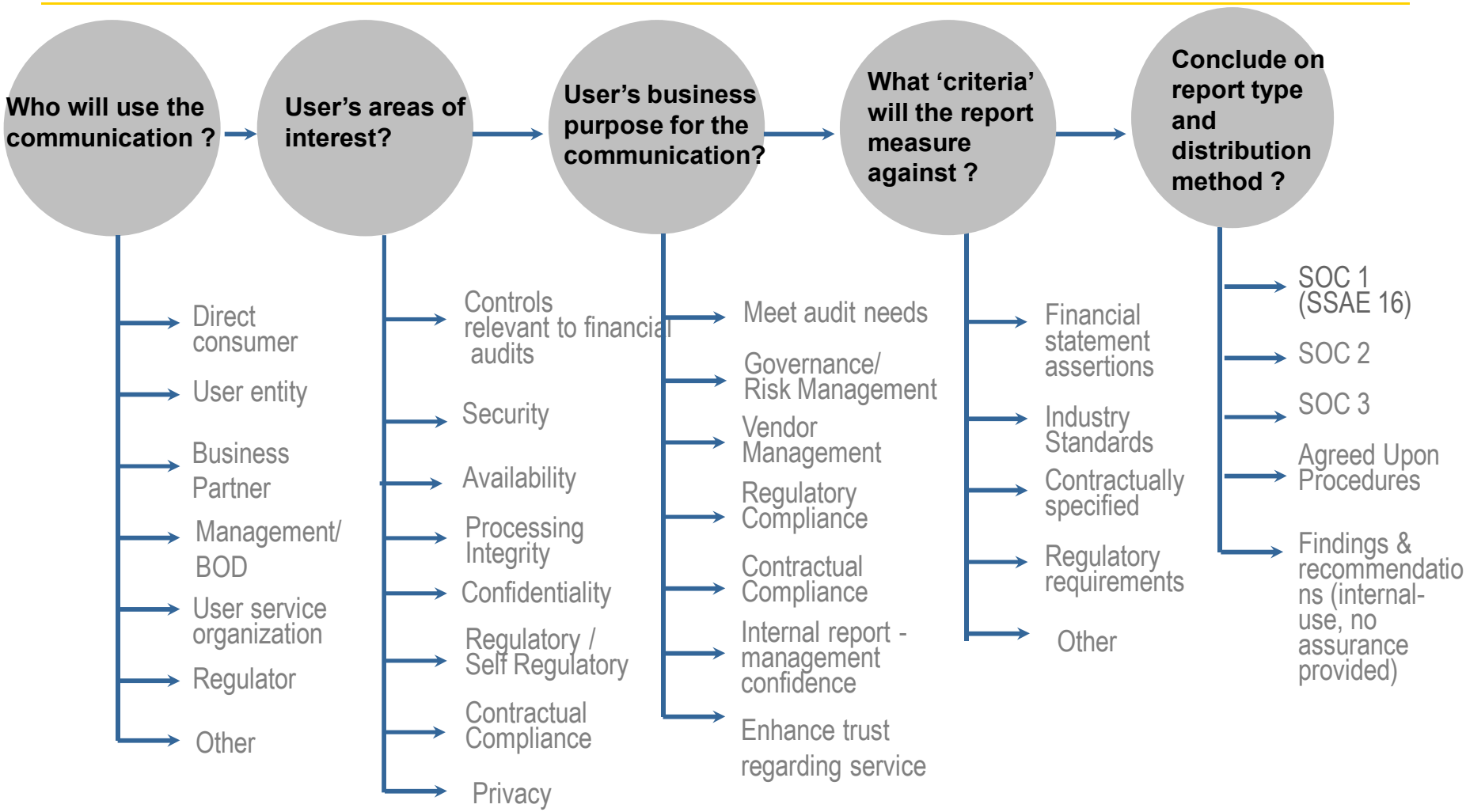


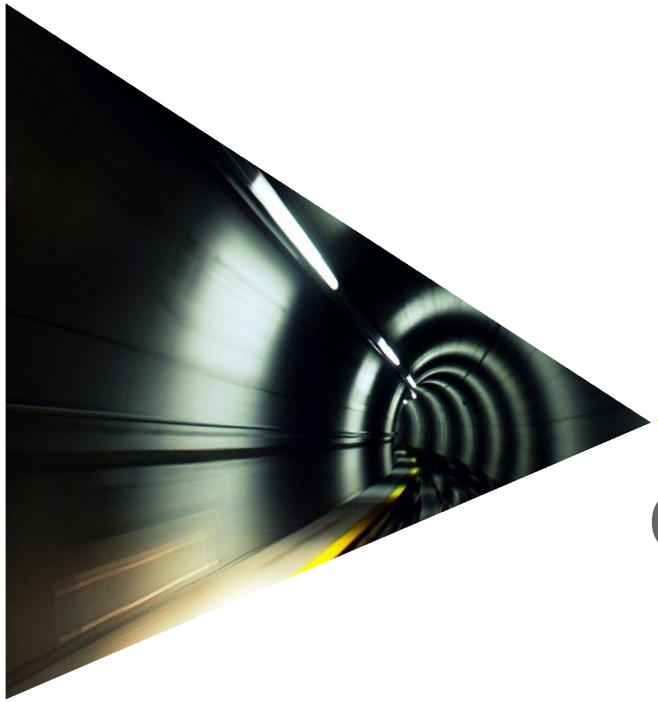
Service Organization Controls 2/3 – Reports (4)
SOC 2 – elements



Service Organization Controls 2/3 – Reports (5)

Five decisions for management





Questions?

Dennis Houtekamer

Ernst & Young Advisory - IT Risk and Assurance
Cell: +31-6-2125 2728 | dennis.houtekamer@nl.ey.com

ERNST & YOUNG
Quality In Everything We Do