Aantoonbare beheersing: SOC2

Platform voor InformatieBeveiliging

10 februari 2026

EY

Shape the future
with confidence

Milan van Helden

Senior Manager, Technology Risk
milan.van.helden@nl.ey.com

SOC1/ SOC2/ SOC3/ ISAE3402 / ISAE3000 / AUP / International Digital Reporting Standards (IDRS)

Attestation & Certification team

- Over 50 professionals;
- Certification services for many standards;
- Attestation services (SOC reporting of which SOC1/ISAE3402, SOC2, ISAE3000 reporting);
- Integrated approach for certification and attestation (SOC reporting).

CERTIFY EY POINT

EY
Shape the future
with confidence

Vraag: **Wat is de ervaring met SOC2?**

A. Ruime ervaring; betrokken (geweest) bij SOC2 project (auditor, consultant of service organisatie).

B. Ervaring; SOC2 rapport gelezen of beoordeeld (auditor of gebruikersorganisatie.

C. Geen of (nog) beperkte ervaring met SOC2.

Agenda

1 Waarom SOC rapportages?

2 Wat is SOC2?

3 Hoe implementeer ik SOC2?

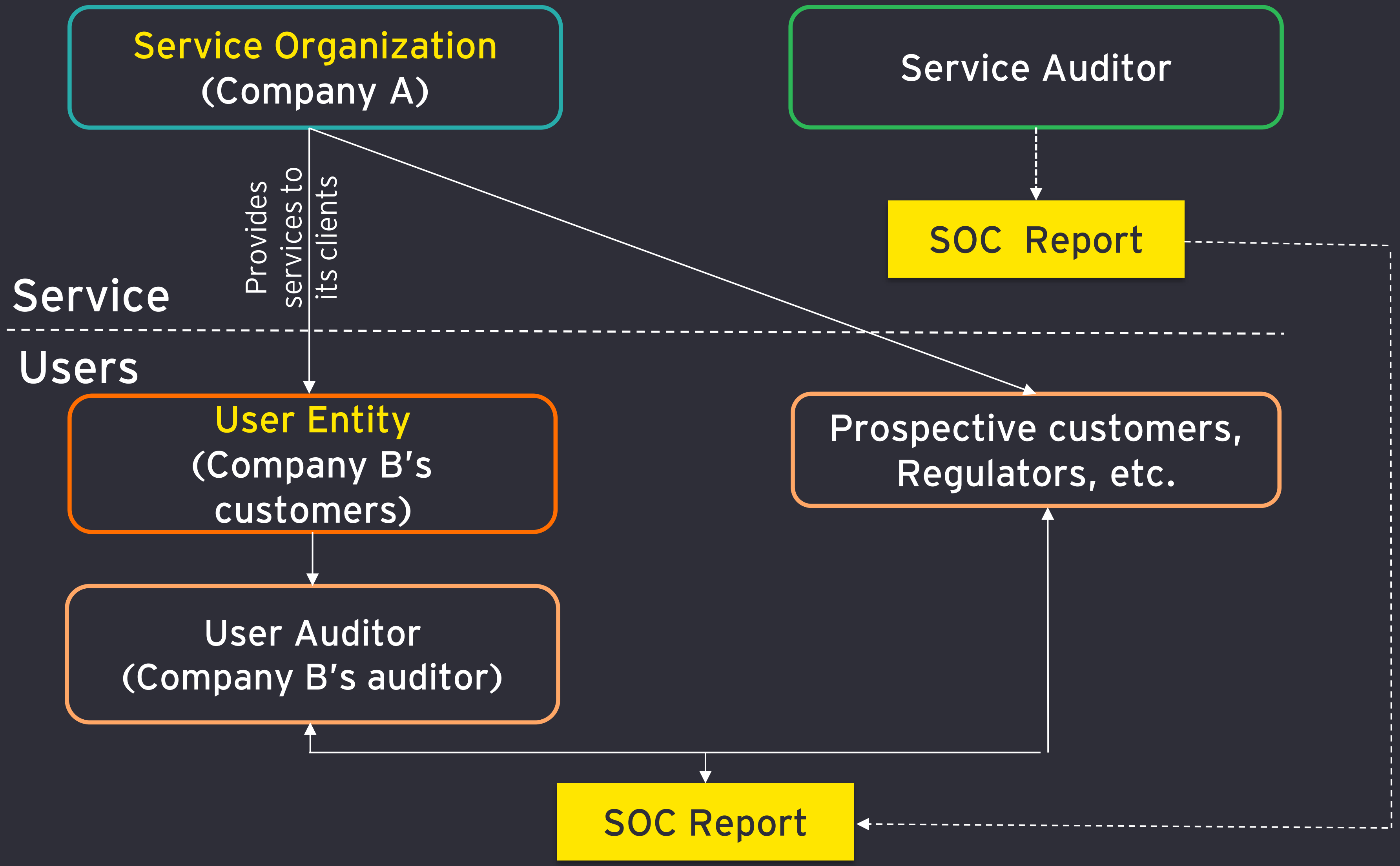
4 SOC2, ISO en SOC2+?

5 Vragen

1

Waarom SOC rapportages?

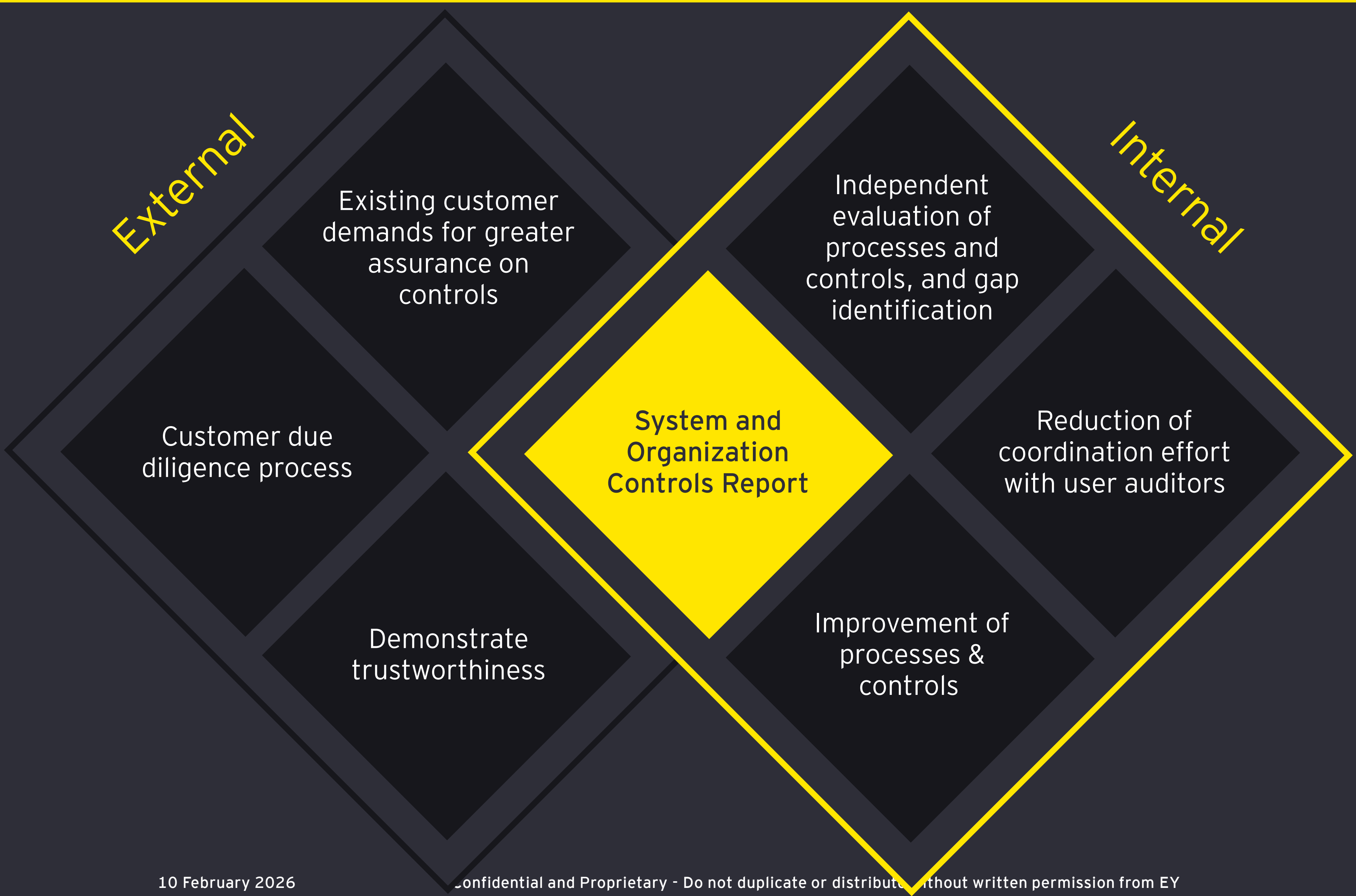
Why SOC reports?



Need for SOC report

- Company B outsources tasks or business functions to Company A
- Company A is organized and operated to provide Company B with the benefits of the services such as software development, hosting services, managing data centers, payroll processing etc. to help accomplish these tasks or business functions.
- Company B may want to understand the effectiveness of controls implemented by the Company A to address the outsourced risks.
- To support their risk assessments, Company B may request a SOC report from the Company A.

Benefits of having a SOC report



System and Organization Controls Report

Existing customer demands for greater assurance on controls

Customer due diligence process

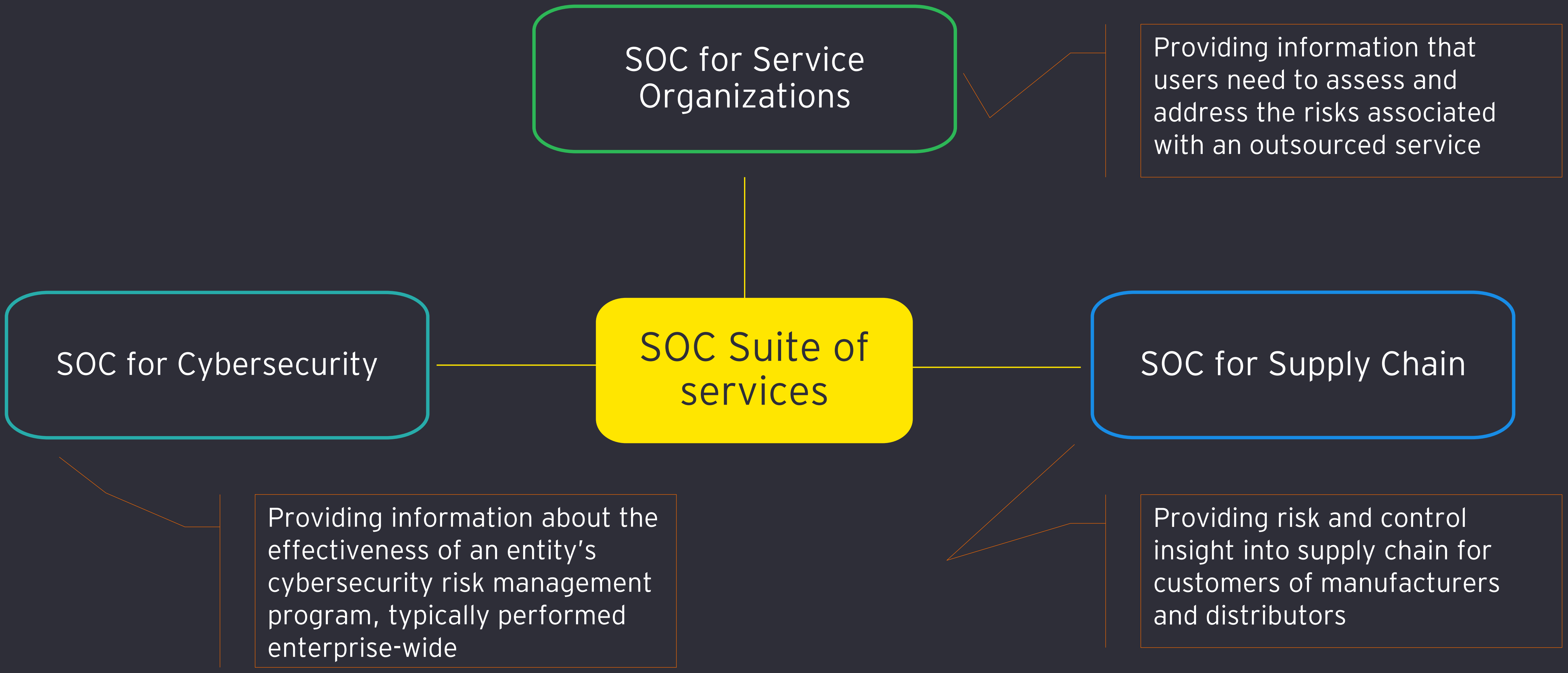
Demonstrate trustworthiness

Independent evaluation of processes and controls, and gap identification

Reduction of coordination effort with user auditors

Improvement of processes & controls

Types of System and Organization Controls (SOC) reports



SOC Suite of services

SOC for Service Organizations

Providing information that users need to assess and address the risks associated with an outsourced service

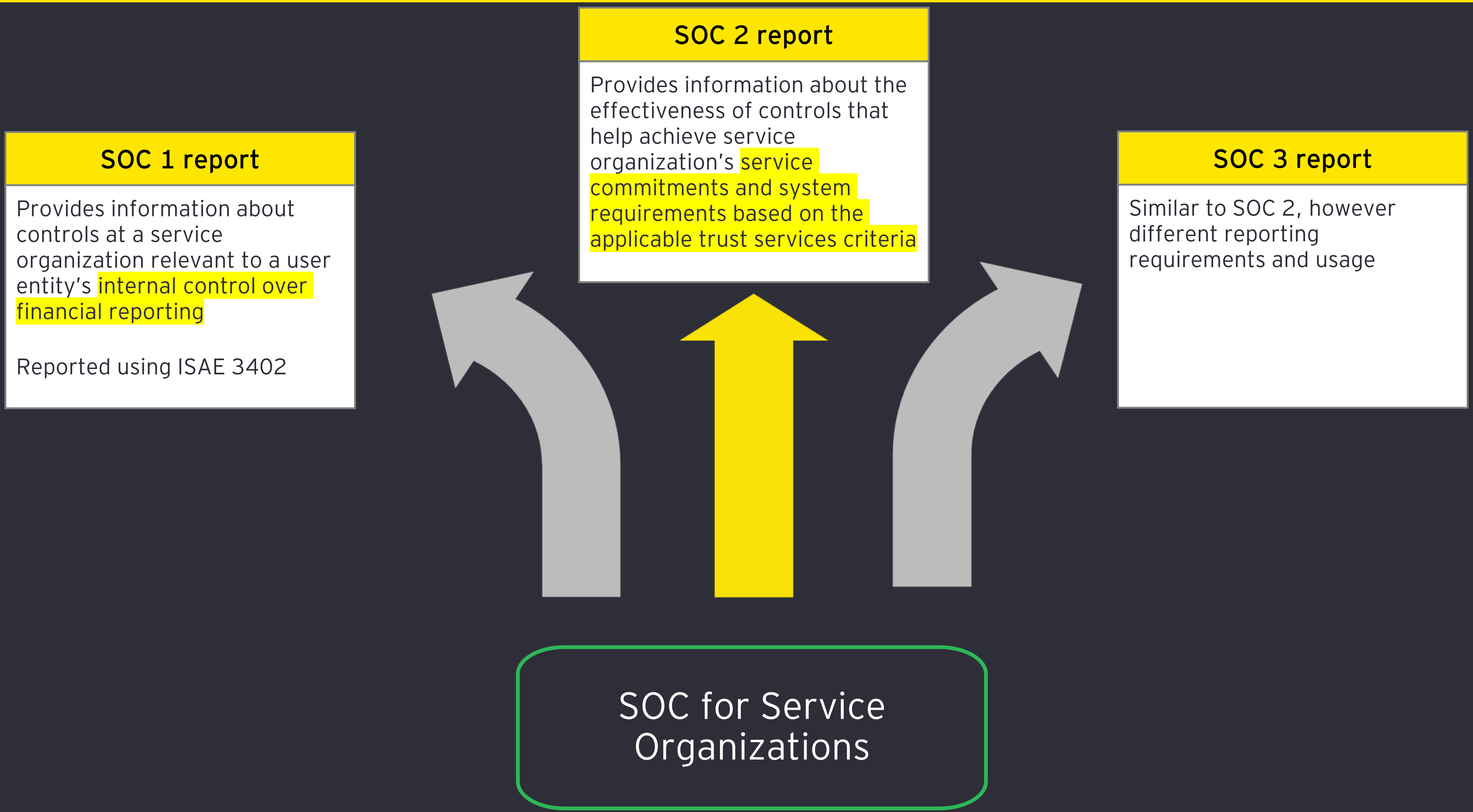
SOC for Cybersecurity

Providing information about the effectiveness of an entity’s cybersecurity risk management program, typically performed enterprise-wide

SOC for Supply Chain

Providing risk and control insight into supply chain for customers of manufacturers and distributors

Types of System and Organization Controls (SOC) reports



SOC 2 report

Provides information about the effectiveness of controls that help achieve service organization’s service commitments and system requirements based on the applicable trust services criteria

SOC 1 report

Provides information about controls at a service organization relevant to a user entity’s internal control over financial reporting

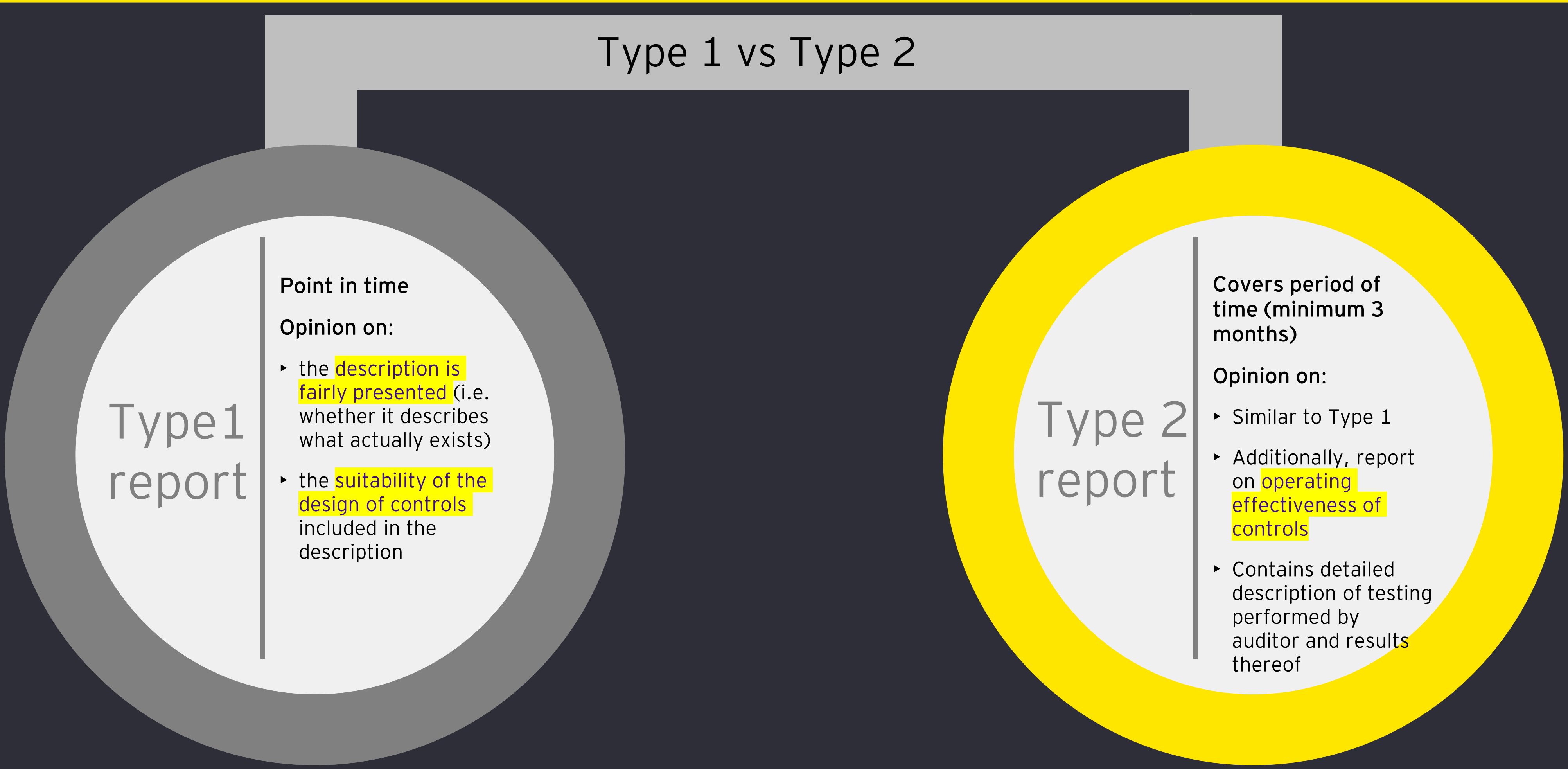
Reported using ISAE 3402

SOC 3 report

Similar to SOC 2, however different reporting requirements and usage

SOC for Service Organizations

Difference between Type 1 & Type 2 SOC reports



Type 1 vs Type 2

Type1 report

Point in time

Opinion on:

- the description is fairly presented (i.e. whether it describes what actually exists)
- the suitability of the design of controls included in the description

Type 2 report

Covers period of time (minimum 3 months)

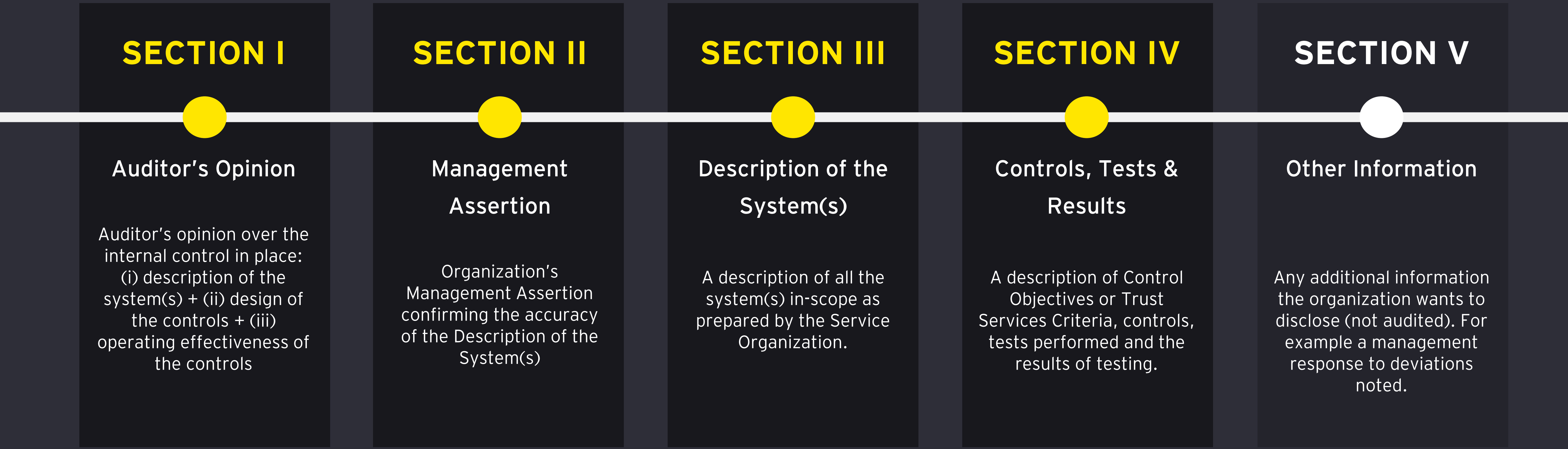
Opinion on:

- Similar to Type 1
- Additionally, report on operating effectiveness of controls
- Contains detailed description of testing performed by auditor and results thereof

Type 1 and Type 2 examinations can be performed for both SOC 1/ISAE3402 and SOC 2

SOC Reporting Structure

A SOC 1/ISAE3402 or a SOC 2 report is composed of 4 mandatory sections and 1 optional section:



SECTION I

Auditor's Opinion

Auditor's opinion over the internal control in place: (i) description of the system(s) + (ii) design of the controls + (iii) operating effectiveness of the controls

SECTION II

Management Assertion

Organization's Management Assertion confirming the accuracy of the Description of the System(s)

SECTION III

Description of the System(s)

A description of all the system(s) in-scope as prepared by the Service Organization.

Partial and limited in SOC 3 Report

SECTION IV

Controls, Tests & Results

A description of Control Objectives or Trust Services Criteria, controls, tests performed and the results of testing.

Not in SOC 3 Report

SECTION V

Other Information

Any additional information the organization wants to disclose (not audited). For example a management response to deviations noted.

2

Wat is SOC2 ?

Introduction SOC2

- SOC 2 is based on attestation standard – AT-C section 205, Examination Engagements issued by American Institute of CPAs (AICPA).

- Audit performed by an independent auditor.

- Where auditor reports on controls within the system were effective to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

Key aspects:

1 Description Criteria (DC) used when preparing description of System

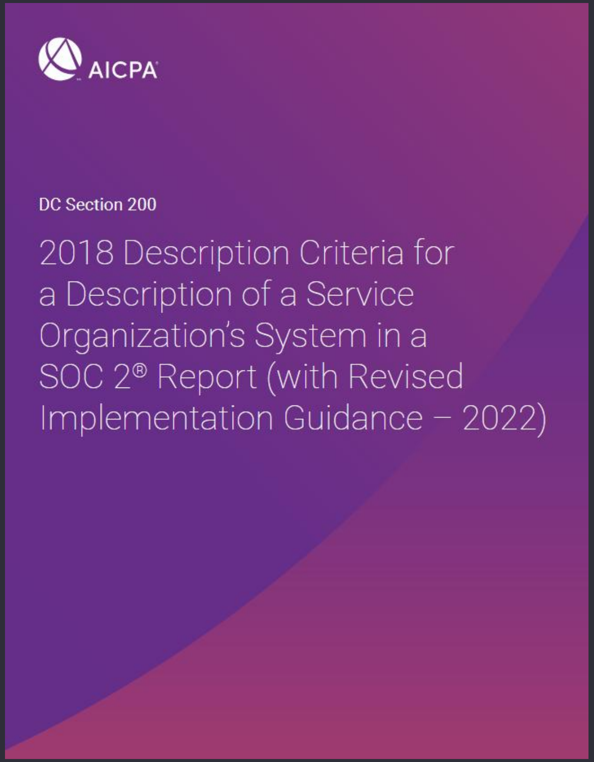
2 Achievement of Service Commitments (SC) and System Requirements (SR)

3 Based on applicable Trust Services Criteria

Description Criteria (DC200) and Trust Services Criteria (TSP100)

The AICPA Assurance Services Executive Committee (ASEC) developed and issued the Description Criteria for a description on service organization's system (DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report*) and a set of criteria (Trust Services Criteria) (TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*).

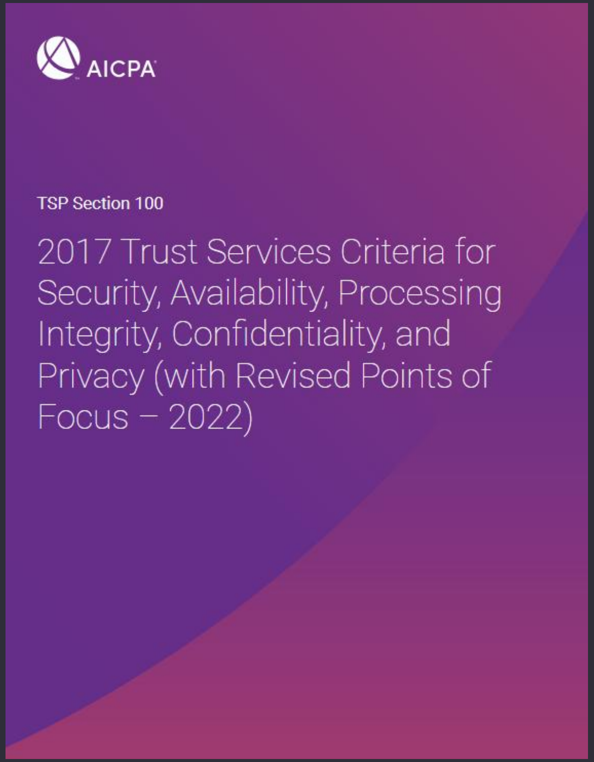
The Description Criteria are used by management when preparing the description of the service organization's system and by the service auditor when evaluating the description. The Trust Services Criteria are criteria used by management to set-up a control framework and by the service auditor to evaluate the design and operating effectiveness of controls.



AICPA

DC Section 200

2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (with Revised Implementation Guidance – 2022)

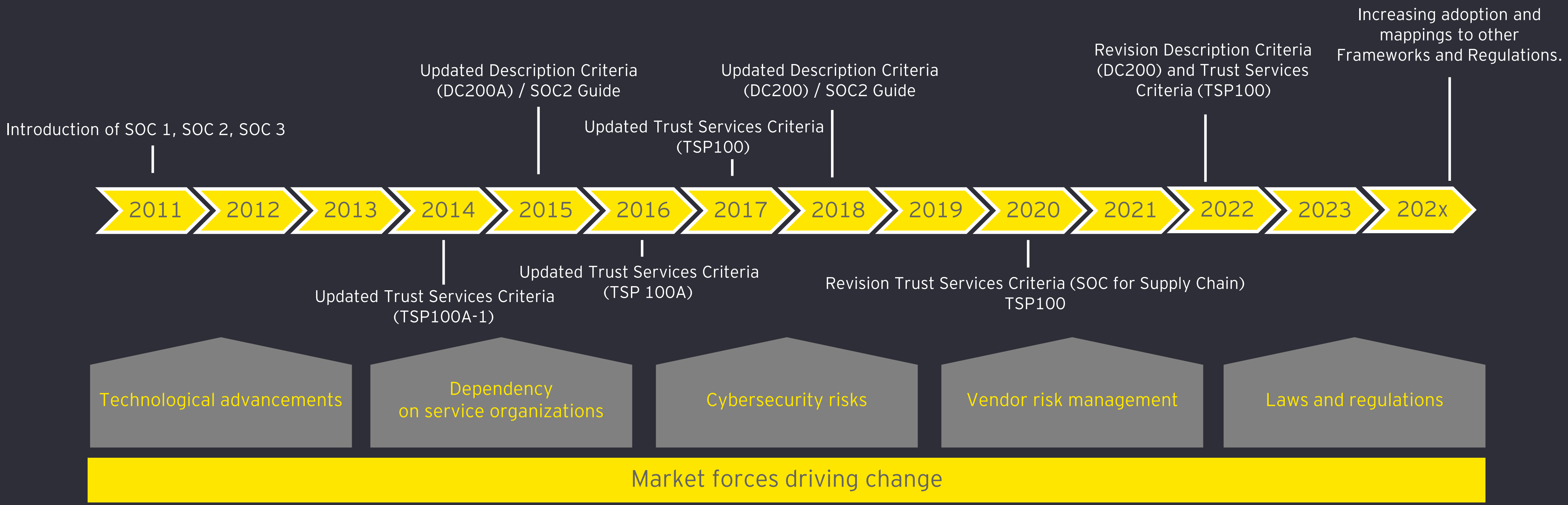


AICPA

TSP Section 100

2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (with Revised Points of Focus – 2022)

SOC2 history



Introduction of SOC 1, SOC 2, SOC 3

Updated Trust Services Criteria (TSP100A-1)

Updated Description Criteria (DC200A) / SOC2 Guide

Updated Trust Services Criteria (TSP 100A)

Updated Trust Services Criteria (TSP100)

Updated Description Criteria (DC200) / SOC2 Guide

Revision Trust Services Criteria (SOC for Supply Chain) TSP100

Revision Description Criteria (DC200) and Trust Services Criteria (TSP100)

Increasing adoption and mappings to other Frameworks and Regulations.

2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 202x

Technological advancements

Dependency on service organizations

Cybersecurity risks

Vendor risk management

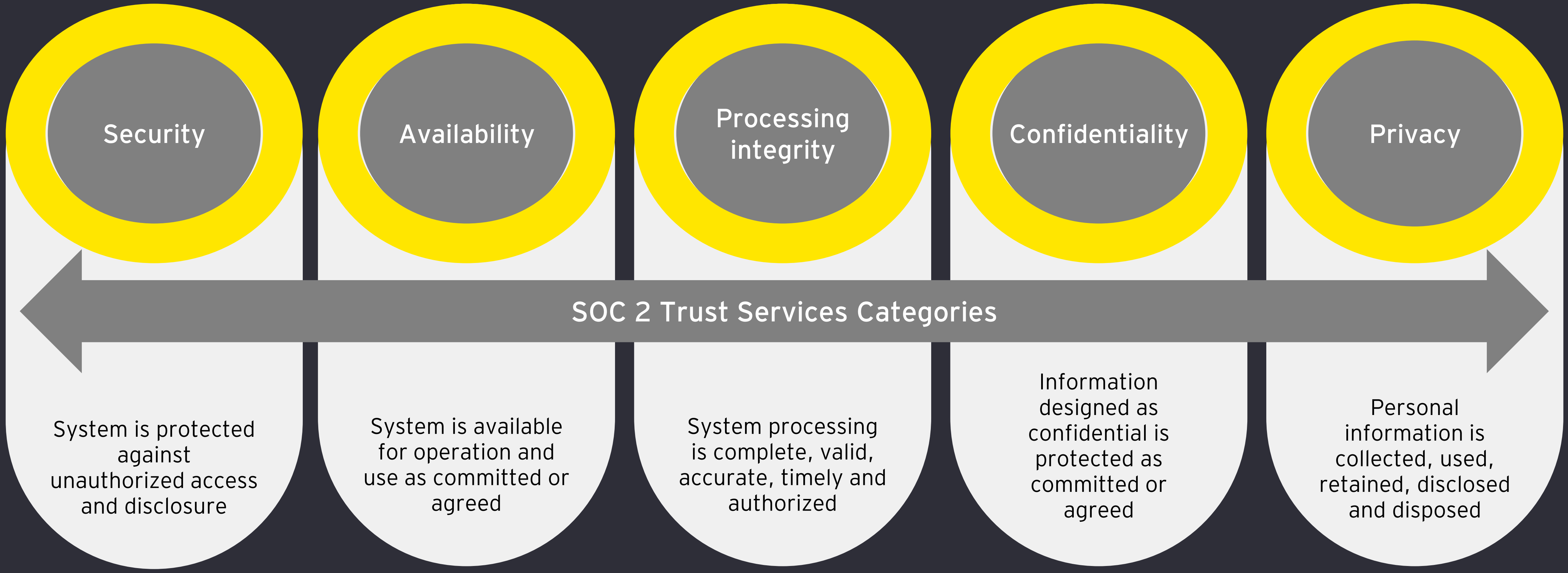
Laws and regulations

Market forces driving change

Before SOC1/ ISAE3402, SAS70 reports (only relevant for Internal Controls Over Financial Reporting (ICFR))

Decision: Trust Services Categories (TSP100)

SOC 2 reports provide assurance in relation to one or more of the five trust services categories. The Trust Services Categories and Trust Services Criteria are available in ‘TSP Section 100 - 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy’.



SOC 2 Trust Services Categories

Security

System is protected against unauthorized access and disclosure

Availability

System is available for operation and use as committed or agreed

Processing integrity

System processing is complete, valid, accurate, timely and authorized

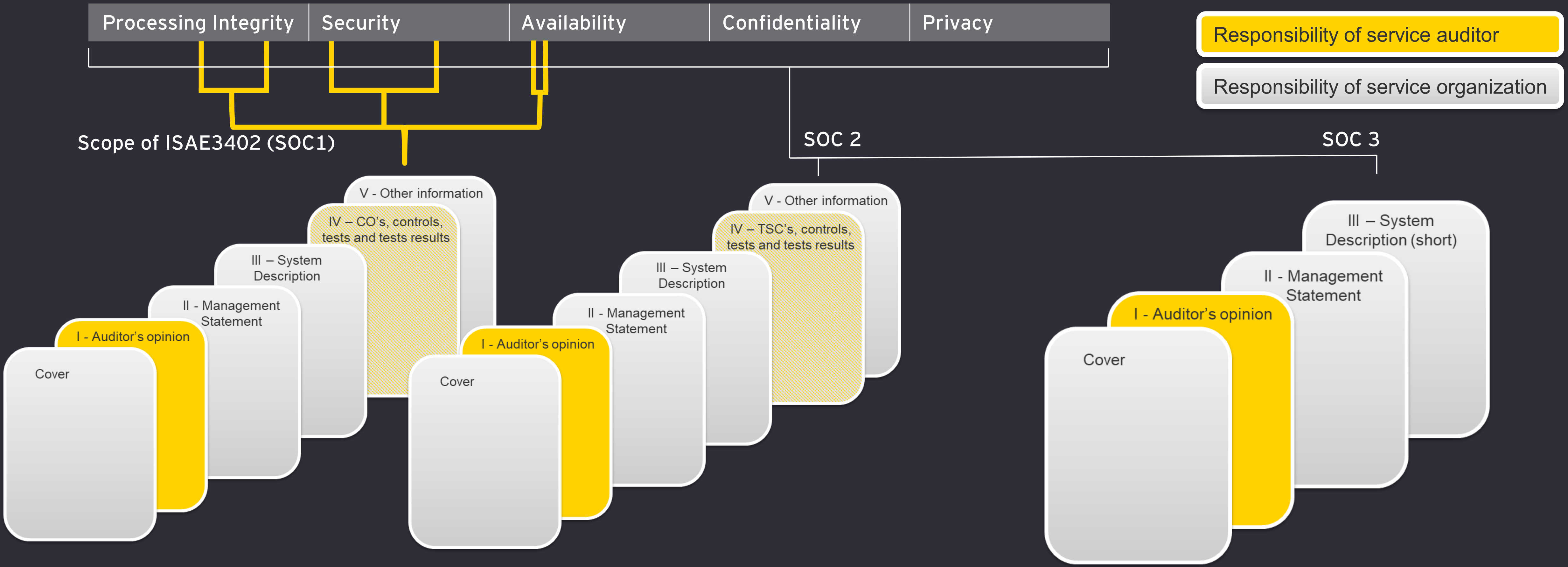
Confidentiality

Information designed as confidential is protected as committed or agreed

Privacy

Personal information is collected, used, retained, disclosed and disposed

SOC1/ISAE3402 vs SOC2 vs SOC3


Processing Integrity
Security
Availability
Confidentiality
Privacy
Responsibility of service auditor
Responsibility of service organization
Scope of ISAE3402 (SOC1)
SOC 2
SOC 3
V - Other information
IV – CO's, controls, tests and tests results
III – System Description
II - Management Statement
I - Auditor's opinion
Cover
V - Other information
IV – TSC's, controls, tests and tests results
III – System Description
II - Management Statement
I - Auditor's opinion
Cover
III – System Description (short)
II - Management Statement
I - Auditor's opinion
Cover

SOC1/ISAE3402 vs SOC2

SOC1/ ISAE3402	SOC2
SOC for Service Organizations: **ICFR** "Internal Control Over Financial Reporting"	SOC for Service Organizations: **Trust Services Criteria** (Security, Availability, Confidentiality, Processing Integrity, Privacy)
We give opinion that control objectives are met	We give opinion that Trust Services criteria are met
Control objectives are set by service organization	**Common criteria** are set by AICPA (Set criteria)
Controls are set by service organizations	Controls are set by service organizations
Less controls	More controls (depending on categories in scope)
Less efforts	More efforts (depending on categories in scope)

Trust Services Categories (TSP100)

The trust services criteria consist of

- criteria common to all five of the trust services categories (common criteria) and
- additional specific criteria for the availability, processing integrity, confidentiality, and privacy categories

Trust Service Category	Description	Common Criteria (CC)	Additional Criteria
Security	*Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to achieve its objectives.*	X	N/A
Availability	*Information and systems are available for operation and use to meet the entity's objectives.*	X	X (A series)
Processing Integrity	*System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.*	X	X (PI series)
Confidentiality	*Information designated as confidential is protected to meet the entity's objectives.*	X	X (C series)
Privacy	*Personal information is collected, used, retained, disclosed, and disposed of to meet the entity's objectives.*	X	X (P series)

Structure and relationships categories of Trust Services Criteria (TSP100) 1

1 Control Environment

2 Communication & Information

3 Risk Assessment

4 Monitoring

5 Control Activities

COSO principle 12: The entity deploys control activities through policies that establish what is expected and procedures that put policies into action

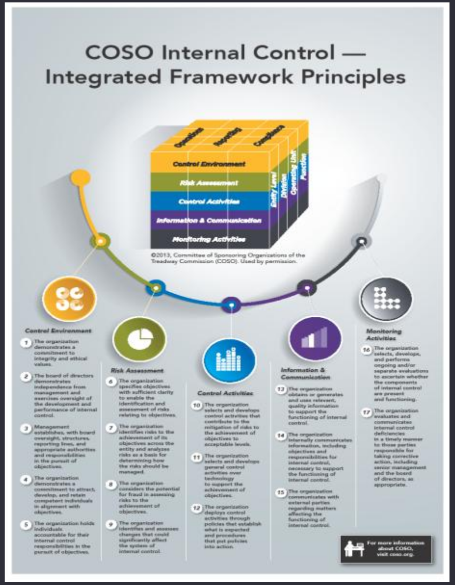
6 Logical and Physical Access Controls

7 System Operations

8 Change Management

9 Risk Mitigation

Additional criteria for availability, confidentiality, processing integrity, and privacy!



COSO Internal Control — Integrated Framework Principles

©2013, Committee of Sponsoring Organizations of the Treadway Commission (COSO). Used by permission.

Control Environment

1 The organization demonstrates a commitment to integrity and ethical values.

2 The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

3 Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

4 The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

5 The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Risk Assessment

6 The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

7 The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

8 The organization considers the potential for fraud in assessing risks to the achievement of objectives.

9 The organization identifies and assesses changes that could significantly affect the system of internal control.

Control Activities

10 The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

11 The organization selects and develops general control activities over technology to support the achievement of objectives.

12 The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

Information & Communication

13 The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.

14 The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

15 The organization communicates with external parties regarding matters affecting the functioning of internal control.

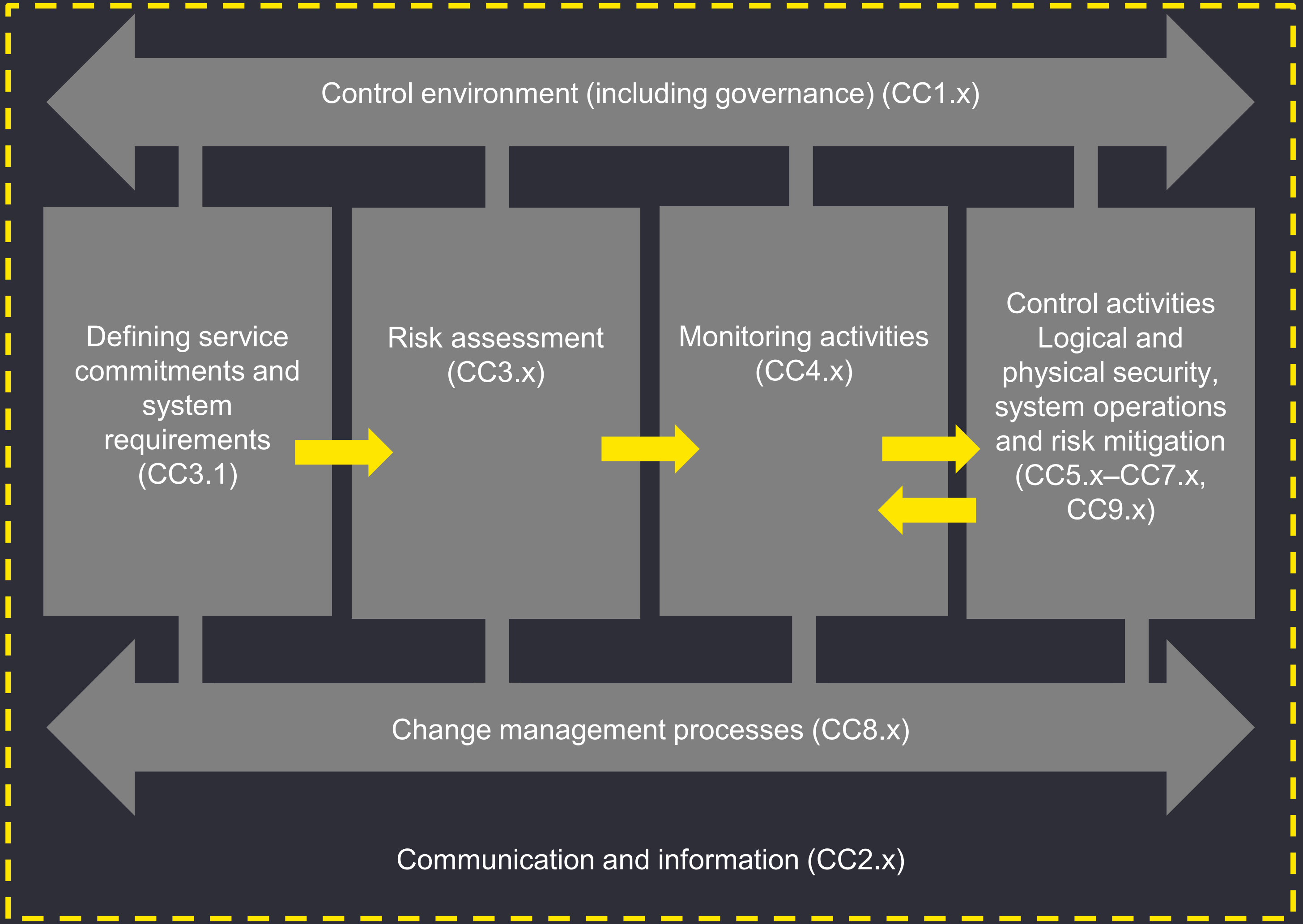
Monitoring Activities

16 The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

17 The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

For more information about COSO, visit coso.org.

Structure and relationships categories of Trust Services Criteria (TSP100) 2



Control environment (including governance) (CC1.x)

Defining service commitments and system requirements (CC3.1)

Risk assessment (CC3.x)

Monitoring activities (CC4.x)

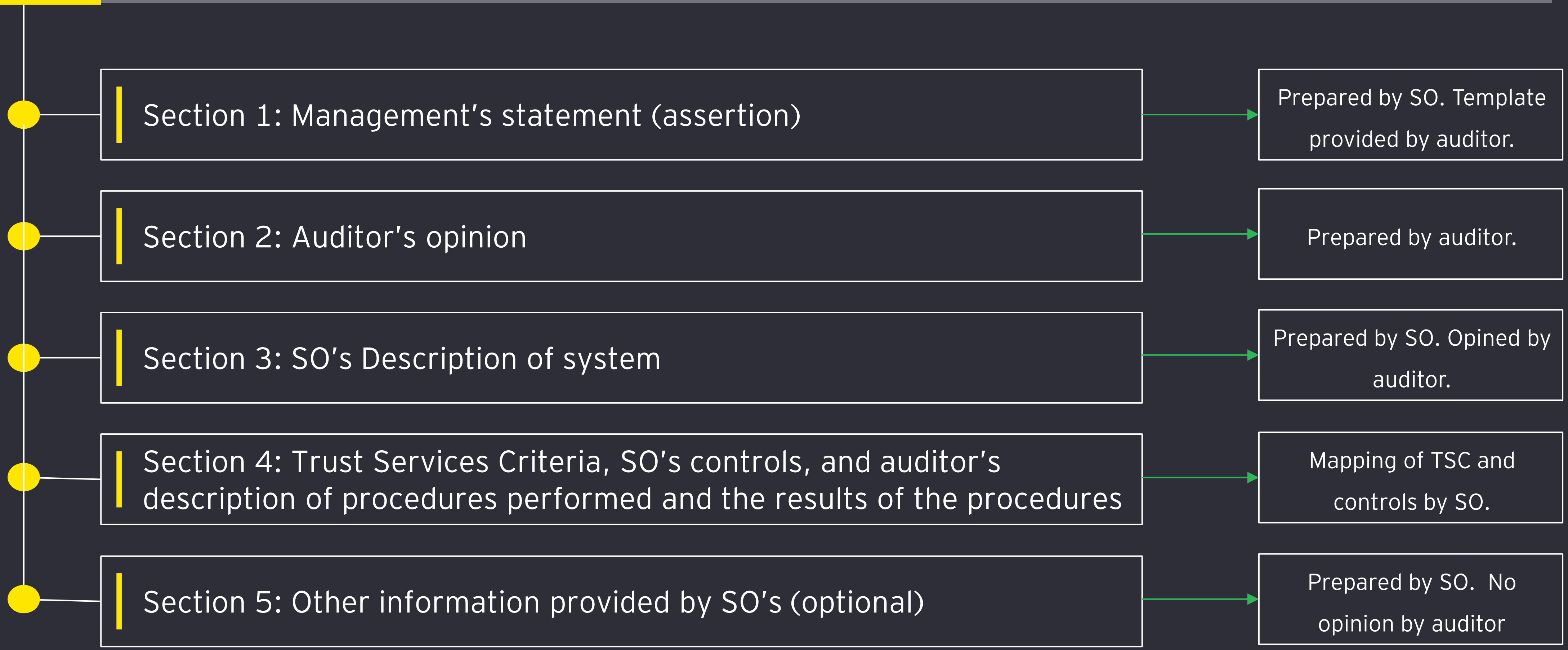
Control activities Logical and physical security, system operations and risk mitigation (CC5.x–CC7.x, CC9.x)

Change management processes (CC8.x)

Communication and information (CC2.x)

SOC Reporting Structure (DC200)

A report prepared to provide reasonable assurance on the service organization's service commitments and system requirements based on the applicable trust services criteria is a SOC 2 report for restricted use. It will have following components (usually in this order):



Section 1: Management's statement (assertion)	Prepared by SO. Template provided by auditor.
Section 2: Auditor's opinion	Prepared by auditor.
Section 3: SO's Description of system	Prepared by SO. Opined by auditor.
Section 4: Trust Services Criteria, SO's controls, and auditor's description of procedures performed and the results of the procedures	Mapping of TSC and controls by SO.
Section 5: Other information provided by SO's (optional)	Prepared by SO. No opinion by auditor

Description criteria (DC200)

Management's description should contain the following information applicable to the system and the trust services category or categories addressed by the description:

DC 1 — The types of services provided

DC 2 — The principal service commitments and system requirements

DC 3 — The components of the system used to provide the services, including the following:

- Infrastructure
- Software
- People
- Procedures
- Data

Description criteria (DC200)

DC 4

For identified system incidents that (a) were the result of controls that were not suitably designed or operating effectively or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements, the following information:

a. Nature of each incident
b. Timing surrounding the incident
c. Extent (or effect) of the incident and its disposition

DC 5

The applicable trust services criteria and the related controls designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved

DC 6

If service organization management assumed, in the design of the service organization's system, that certain controls would be implemented by user entities, and those controls are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved, those complementary user entity controls (CUECs)

Description criteria (DC200)

DC 7

If the service organization uses a subservice organization and the controls at the subservice organization are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements are achieved, the following:

a. When service organization management elects to use the inclusive method:

i. The nature of the service provided by the subservice organization

ii. The controls at the subservice organization that are necessary, in combination with controls at the service organization to provide reasonable assurance that the service organization's service commitments and system requirements are achieved

iii. Relevant aspects of the subservice organization's infrastructure, software, people, procedures, and data

iv. The portions of the system that are attributable to the subservice organization

b. When service organization management decides to use the carve-out method:

i. The nature of the service provided by the subservice organization

ii. Each of the applicable trust services criteria that are intended to be met by controls at the subservice organization

iii. The types of controls that service organization management assumed, in the design of the service organization's system, would be implemented by the subservice organization that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements are achieved (commonly referred to as complementary subservice organization controls or CSOCs)

Description criteria (DC200)

DC 8

Any specific criterion of the applicable trust services criteria that is not relevant to the system and the reasons it is not relevant

DC 9

In a description that covers a period of time (type 2 examination), the relevant details of significant changes to the service organization’s system and controls during that period that are relevant to the service organization’s service commitments and system requirements

Key takeaways on the Description Criteria (DC200)

- Description Criteria is used by -
  - Service organization – to describe its system
  - Service auditor – to evaluate whether system has been described to achieve its SC & SR

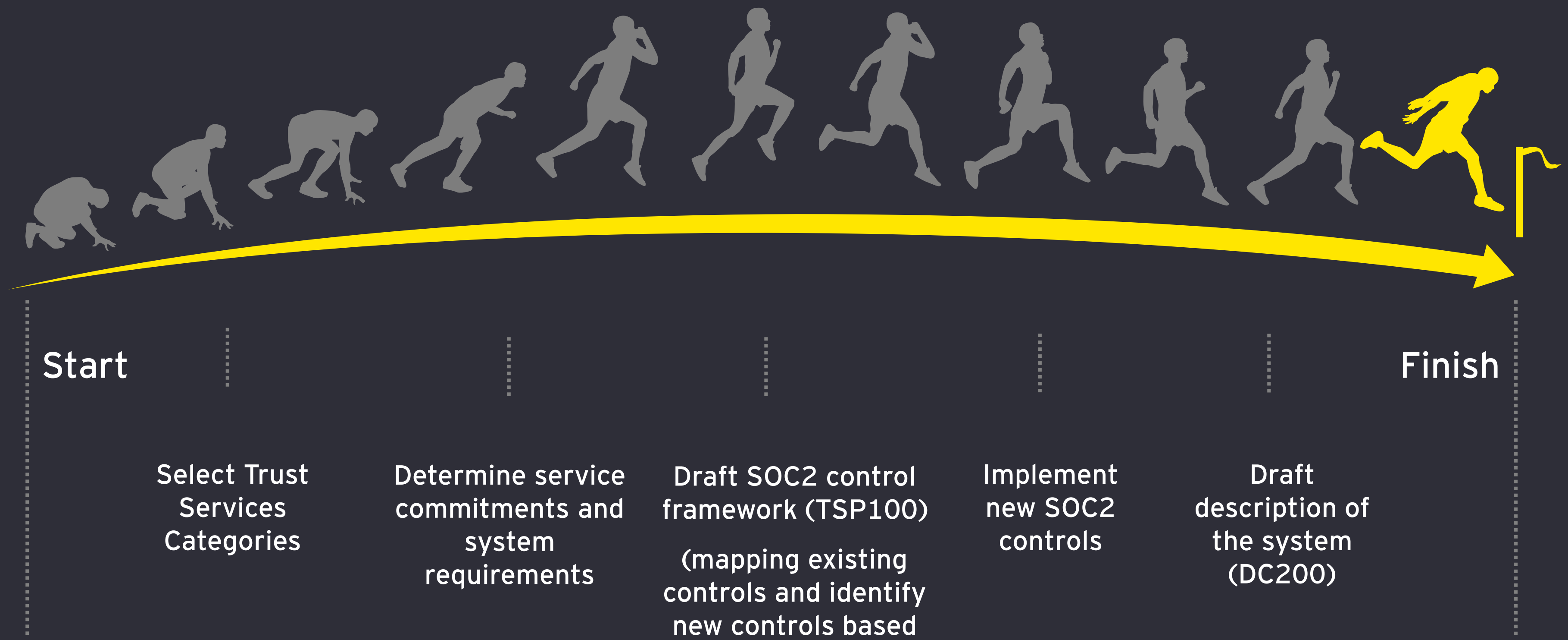
- Description Criteria is mandatory.

- Important aspects of Description Criteria include -
  - Services provided
  - Principal Service commitments and System Requirements
  - Components of system
  - Disclosure of Significant incidents
  - Applicable trust services criteria and related controls
  - Complementary User Entity Controls
  - Subservice Organizations and Complementary Subservice Organization Controls

3

Hoe implementeer ik SOC2?

What steps to take?



Start

Select Trust Services Categories

Determine service commitments and system requirements

Draft SOC2 control framework (TSP100)

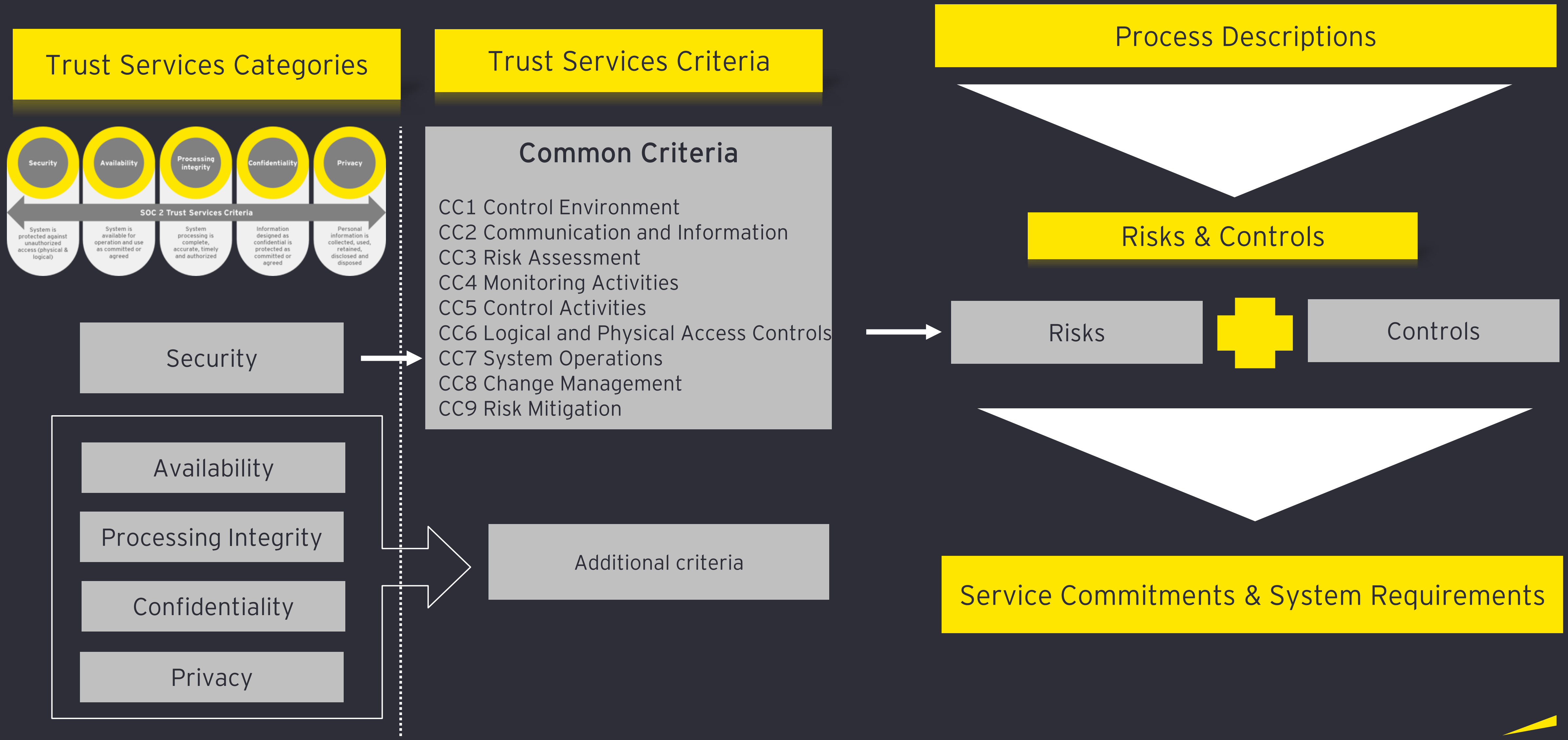
(mapping existing controls and identify new controls based on gap analysis)

Implement new SOC2 controls

Draft description of the system (DC200)

Finish

Relationship between Trust Services Criteria, SC & SR and controls



Trust Services Categories

Security — System is protected against unauthorized access (physical & logical)

Availability — System is available for operation and use as committed or agreed

Processing integrity — System processing is complete, accurate, timely and authorized

Confidentiality — Information designed as confidential is protected as committed or agreed

Privacy — Personal information is collected, used, retained, disclosed and disposed

SOC 2 Trust Services Criteria

Security

Availability

Processing Integrity

Confidentiality

Privacy

Trust Services Criteria

Common Criteria

- CC1 Control Environment
- CC2 Communication and Information
- CC3 Risk Assessment
- CC4 Monitoring Activities
- CC5 Control Activities
- CC6 Logical and Physical Access Controls
- CC7 System Operations
- CC8 Change Management
- CC9 Risk Mitigation

Additional criteria

Process Descriptions

Risks & Controls

Risks

Controls

Service Commitments & System Requirements

Implementation of SOC 2 TSCs

Points of Focus (PoFs)

- Points of Focus (TSP100) represent the important characteristics of each criterion and:
  - Provide transparency into the minimum characteristics;
  - Provide detail on the important characteristics of each criterion;
  - Drive consistency in reporting;
  - Do not appear in the SOC 2 report (explanations regarding PoFs that are not applicable to the environment also do not appear in the SOC 2 report).

With the Points of Focus a service organization should determine which are applicable based on your environment and any custom points of focus that apply, based on the service commitments and service requirements, can be added.

Implementation of SOC 2 TSCs

TSCs and PoF

- Common criteria required for all SOC 2 reports (addresses security)

Criteria		# points of focus
Control environment	CC1.1 - CC1.5	26
Communication and information	CC2.1 - CC2.3	17
Risk assessment	CC3.1 - CC3.4	34
Monitoring activities	CC4.1 - CC4.2	11
Control activities	CC5.1 - CC5.3	16
Logical and physical security controls	CC6.1 - CC6.8	34
System operations	CC7.1 - CC7.5	29
Change management	CC8.1	13
Risk mitigation	CC9.1 - CC9.2	10
	Total	190

Implementation of SOC 2 TSCs

TSCs and PoF

- Additional criteria based on the subject matter (for other categories)

Criteria		# additional points of focus
Availability	A1.1 - A1.3	15
Confidentiality	C1.1 - C1.2	4+ add-ins to the common criteria (4)
Processing integrity	PI1.1 - PI1.5	18
Privacy	P1.1 - P8.1	51+ add-ins to the common criteria (8)

Implementation of SOC 2 TSCs
Example (1)

Availability	
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.

A1.1 Points of focus
Measures Current Usage - The use of the system components is measured to establish a baseline for capacity management and to use when evaluating the risk of impaired availability due to capacity constraints.
Forecasts Capacity - The expected average and peak use of system components is forecasted and compared to system capacity and associated tolerances. Forecasting considers capacity in the event of the failure of system components that constrain capacity.
Makes Changes Based on Forecasts - The system change management process is initiated when forecasted usage exceeds capacity tolerances.

Implementation of SOC 2 TSCs

Example (2)

System Operations	
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.

CC7.5 Points of focus

Restores the Affected Environment – The activities restore the affected environment to functional operation by rebuilding systems, updating software, installing patches and changing configurations, as needed.

Communicates Information About the Event – Communications about the nature of the incident, recovery actions taken and activities required for the prevention of future security events are made to management and others as appropriate (internal and external).

Determines Root Cause of the Event – The root cause of the event is determined.

Implements Changes to Prevent and Detect Recurrences – Additional architecture or changes to preventive and detective controls, or both, are implemented to prevent and detect recurrences on a timely basis.

Improves Response and Recovery Procedures – Lessons learned are analyzed, and the incident response plan and recovery procedures are improved.

Implements Incident Recovery Plan Testing – Incident recovery plan testing is performed on a periodic basis. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of relevant system components from across the entity that can impair availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans and systems based on test results.

Common pitfalls SOC2

Service commitments and system requirements not clear

Responsibilities client, subservice organizations and service organizations not sufficiently clear

Lack of documentation to show the operating effectiveness of SOC2 controls for the period in scope

Points of Focus not addressed but unclear why

4

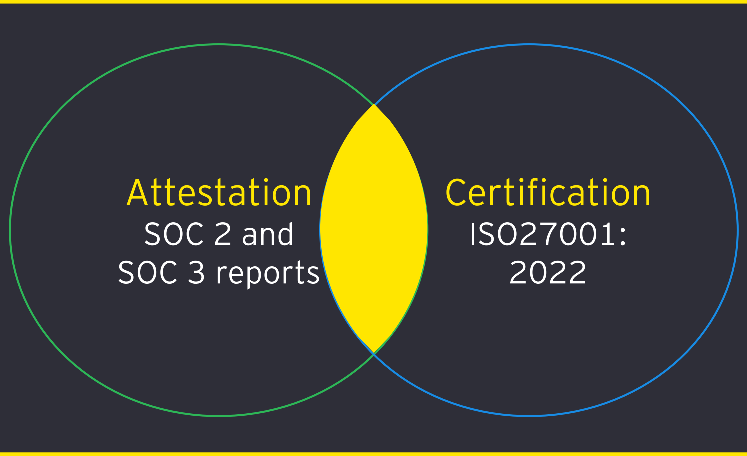
SOC2, ISO en SOC2+?

SOC2 vs ISO (27001)

Parameters	SOC 2 Type 1	SOC 2 Type 2	ISO 27001
Purpose	To provide an organization a way to demonstrate that technology controls (particularly security) are designed effectively	To provide an organization a way to demonstrate that technology controls (particularly security) are designed and operating effectively	To provide a best practice framework for an information security management system.
Nature	Design effectiveness review	Operating effectiveness	Design effectiveness
Period coverage	Point in time	For a period of time, usually a year	Point in time
Recurrence	Done every year (if not moving to a Type 2)	Usually annually	Certification valid for 3 years
Report	Detailed report (usually 50 pages or more), covering description of processes, controls and tests along with auditor opinion	Detailed report (usually 50 pages or more), covering description of processes, controls and tests along with auditor opinion	ISO Certificate
Effort	Comparable to ISO	Time consuming	Less time-consuming
Use	Restricted use	Restricted use	General use

ISO27001 certification & SOC2 examination integrated approach

- ISO27001 & SOC2 controls mapping
- Combined testing for ISO27001 and SOC examination where possible
- On-site testing for ISO27001 and SOC examination will be performed by SOC team
- ISO certification results will be based on the outcome of the SOC testing for the mapped controls



Benefits

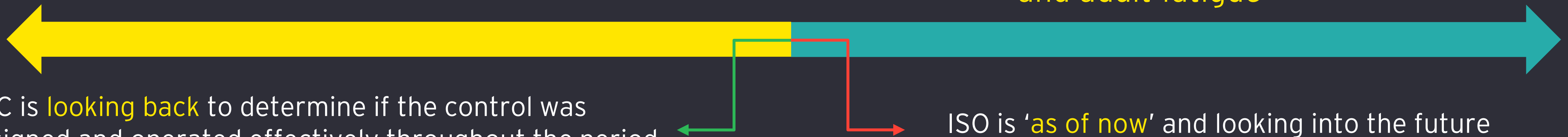
- Reduced auditor footprint
- Simplified communication
- Time savings

Considerations

- Scope differences
- Locations
- Controls mapping
- Deviations (if any)

BENEFITS

- Combined testing of SOC & ISO for fully mapped controls
- For ISO, the results from the SOC were relied upon for the fully mapped controls
- Resulted in reduction of auditor footprint and audit fatigue



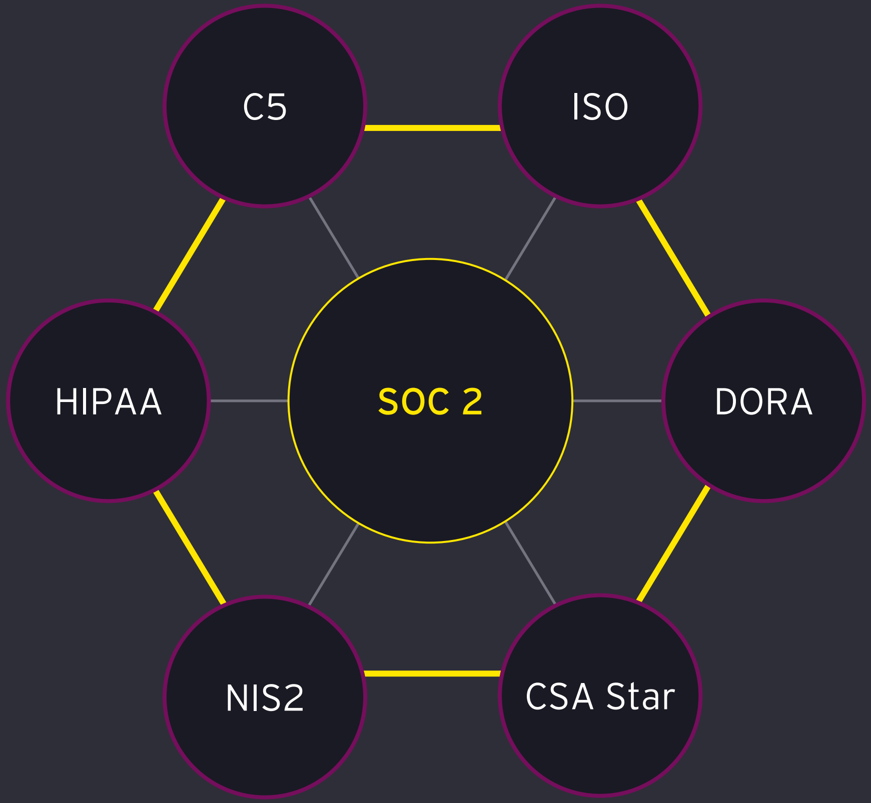
SOC is looking back to determine if the control was designed and operated effectively throughout the period.

ISO is 'as of now' and looking into the future

SOC2+

Complying with multiple control frameworks

- Significant demand to demonstrate compliance with multiple frameworks/standards/regulations
- SOC 2 reports can be leveraged to demonstrate compliance to multiple frameworks/standards/regulations
- “Test one report many”



- Using SOC 2+ report to demonstrate compliance to other / multiple frameworks and regulations
- Using Section V of the SOC 2 report as a communication mechanism to outline the mapping to other frameworks/standards/regulations

5

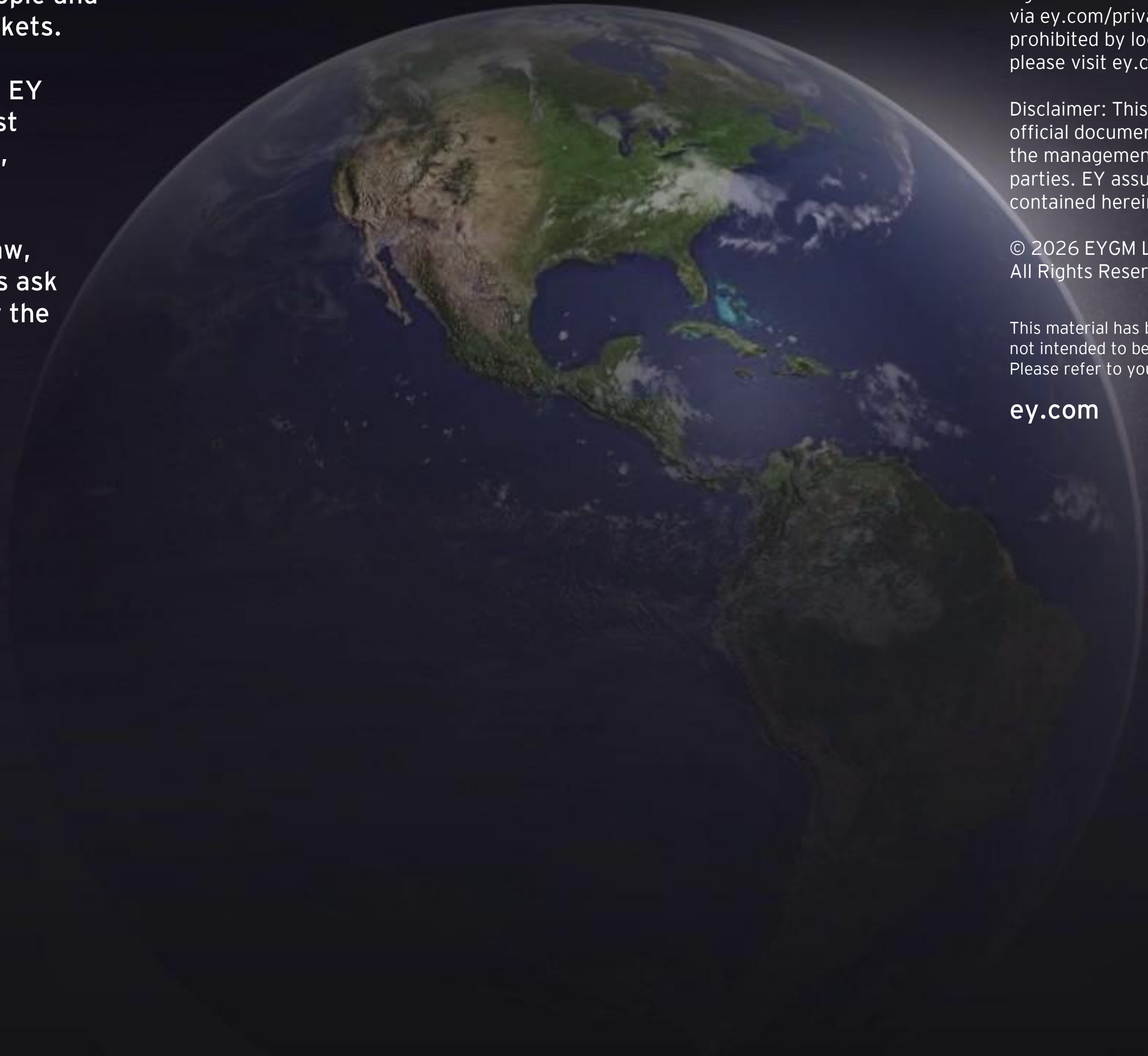
Vragen?

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.



EY refers to the global organization, and may refer to one or more, of the 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. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Disclaimer: This document is intended only for discussion and is not an official document from EY. It is intended solely for the information for the management of SoftServe and should not be shared with any other parties. EY assumes no responsibility to any user of the information contained herein.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com