SOC 2 Compliance & Cyber Attestation

Security Congres – Dennis Houtekamer

The better the question. The better the answer.
The better the world works.

Building a better
working world

Agenda

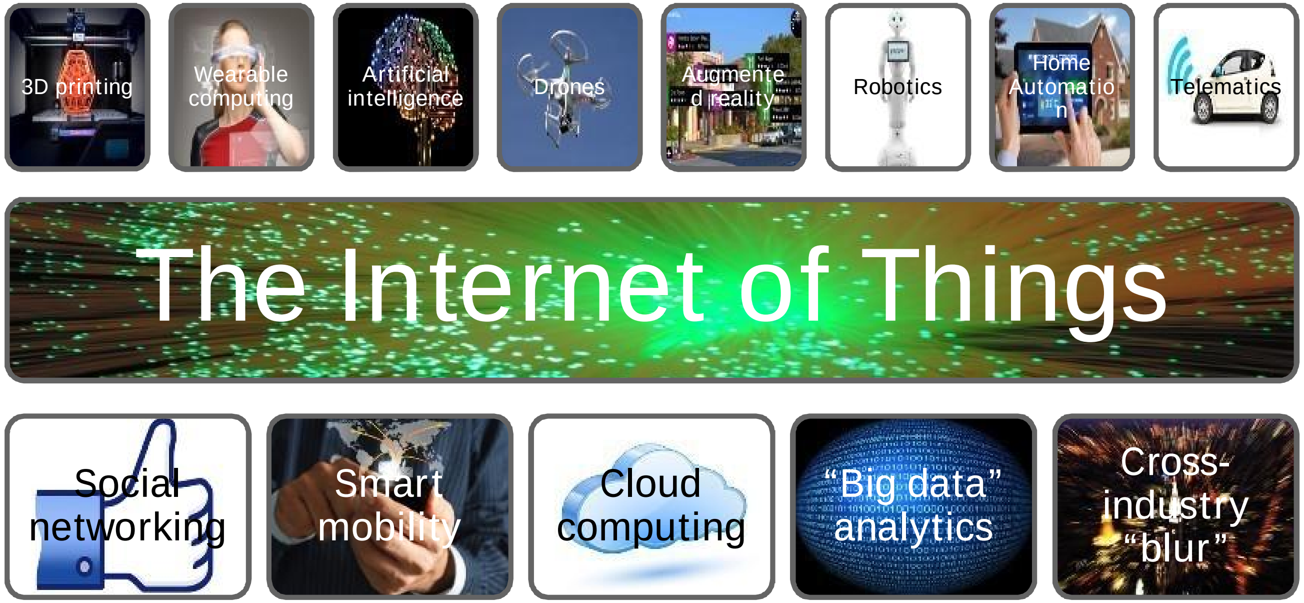
1 Currency of SOC Reporting

2 2017 Trust services criteria update

3 Cyber Attestation standards

The convergence of enabling technologies and industry led solutions is creating a smart, connected world

Disruptive digital technologies and the Internet of Things will continue to drive tech industry growth through 2020 and beyond



3D printing

Wearable computing

Artificial intelligence

Drones

Augmented reality

Robotics

Home Automation

Telematics

The Internet of Things

Social networking

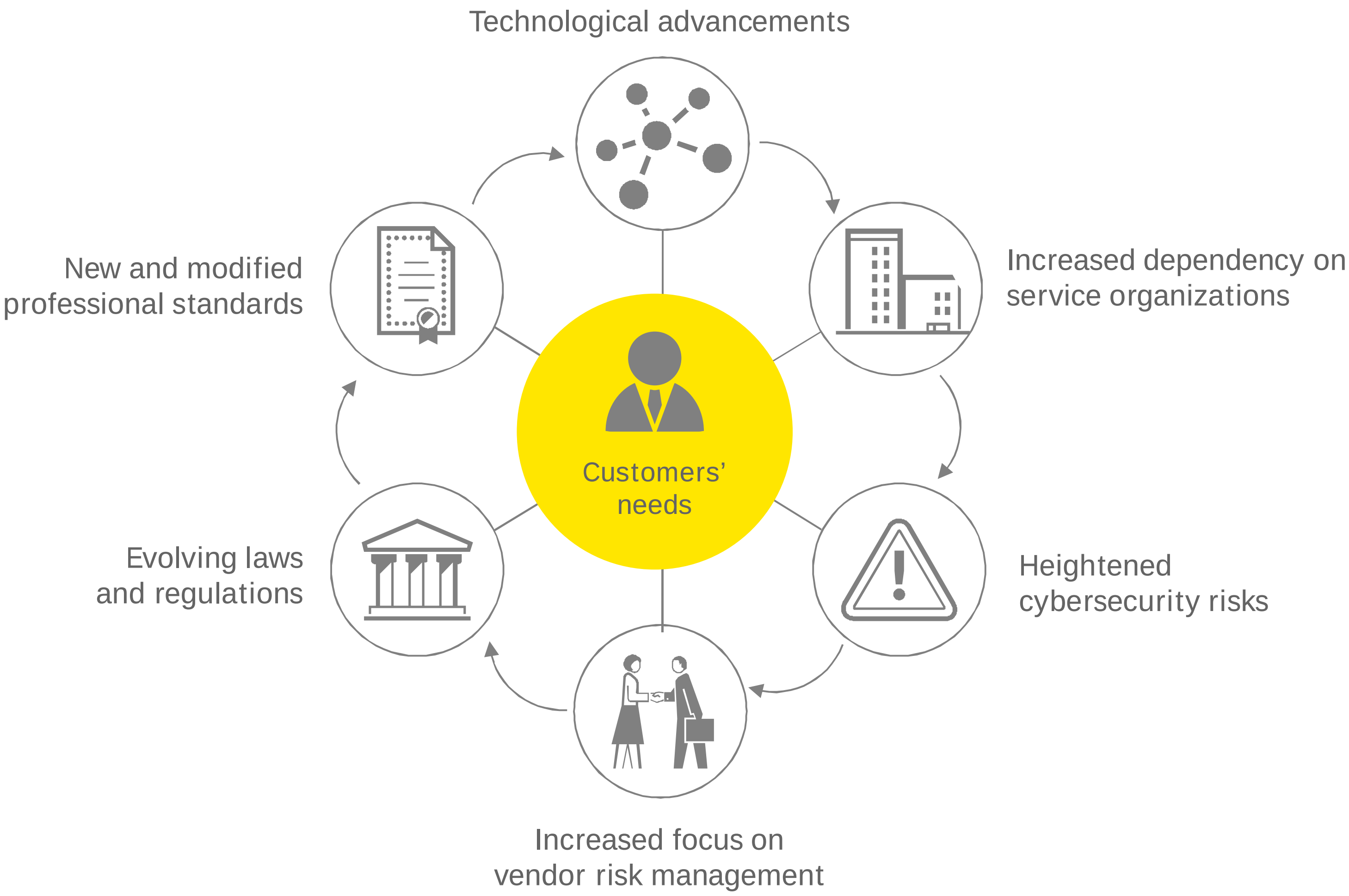
Smart mobility

Cloud computing

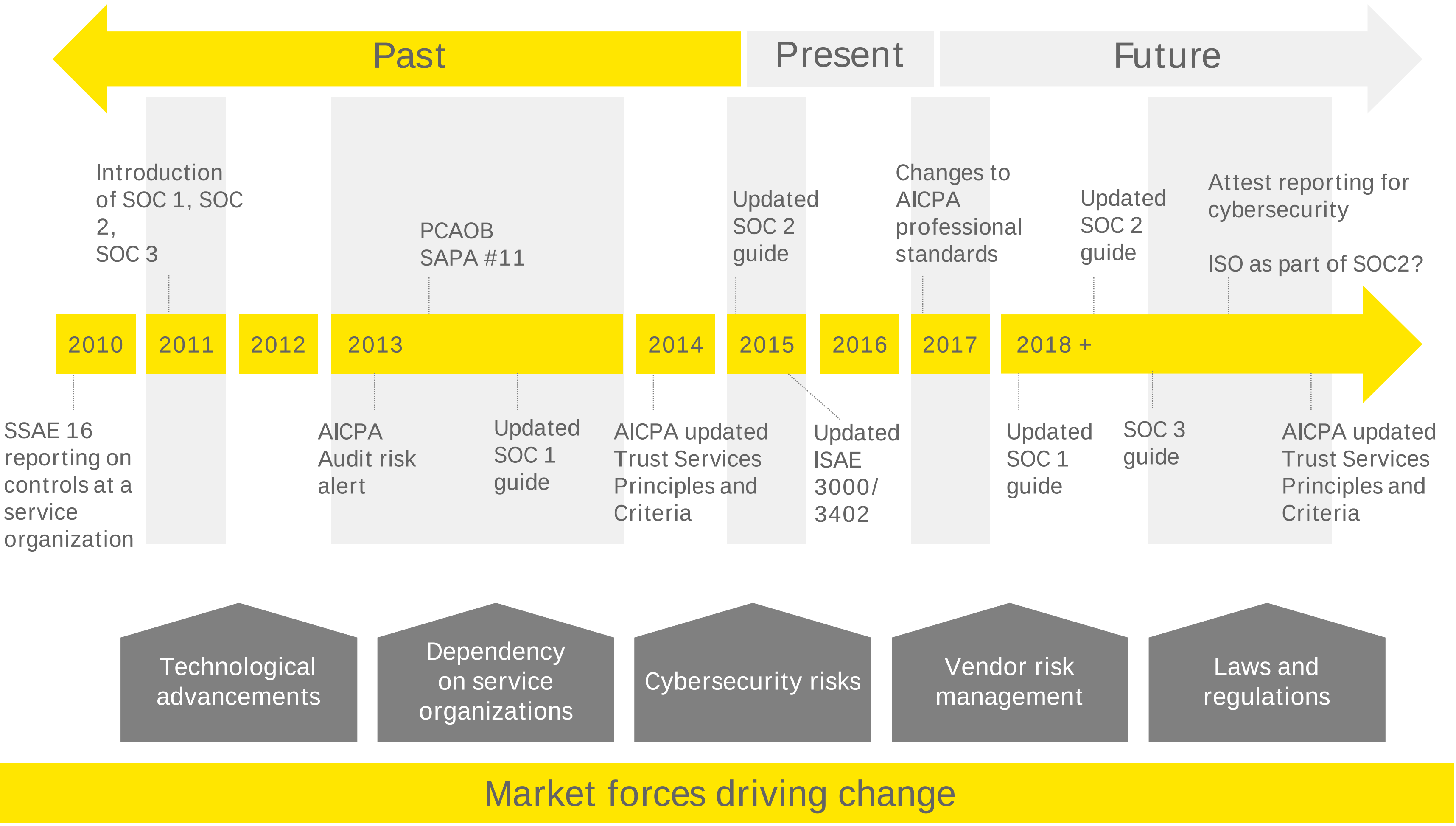
“Big data” analytics

Cross-industry “blur”

How do the market forces work together?


Technological advancements
Increased dependency on service organizations
Heightened cybersecurity risks
Increased focus on vendor risk management
Evolving laws and regulations
New and modified professional standards
Customers' needs

The past, present and future of SOC Reporting



Past

Present

Future

2010

SSAE 16 reporting on controls at a service organization

2011

Introduction of SOC 1, SOC 2, SOC 3

2012

2013

PCAOB SAPA #11

AICPA Audit risk alert

Updated SOC 1 guide

2014

AICPA updated Trust Services Principles and Criteria

2015

Updated SOC 2 guide

Updated ISAE 3000/ 3402

2016

2017

Changes to AICPA professional standards

2018 +

Updated SOC 2 guide

Attest reporting for cybersecurity

ISO as part of SOC2?

Updated SOC 1 guide

SOC 3 guide

AICPA updated Trust Services Principles and Criteria

Technological advancements

Dependency on service organizations

Cybersecurity risks

Vendor risk management

Laws and regulations

Market forces driving change

AICPA reporting options

Overview of System and Organization Controls (SOC)

System and Organization Controls (SOC) suite of services provide independent attestation related to the following subject matter:

1

SOC for service organizations: providing valuable information that users need to assess and address the risks associated with an outsourced service

- SOC 1 – SOC for Service Organizations: ICFR
- SOC 2 – SOC for Service Organizations: Trust Services Criteria (TSC: Security, Availability, Processing Integrity, Confidentiality, Privacy)
- SOC 3 – SOC for Service Organizations: Trust Services Criteria for General Use Report

2

SOC for cybersecurity–Reporting on an Entity's Cybersecurity Risk Management Program and Controls:

communicating relevant useful information about the effectiveness of an entity's cybersecurity risk management program, typically performed enterprise-wide.

3

SOC for supply chains:

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

2017 Trust services criteria update

2017 Trust services criteria update

Why are things changing?

1

Address prevalent cybersecurity risks

2

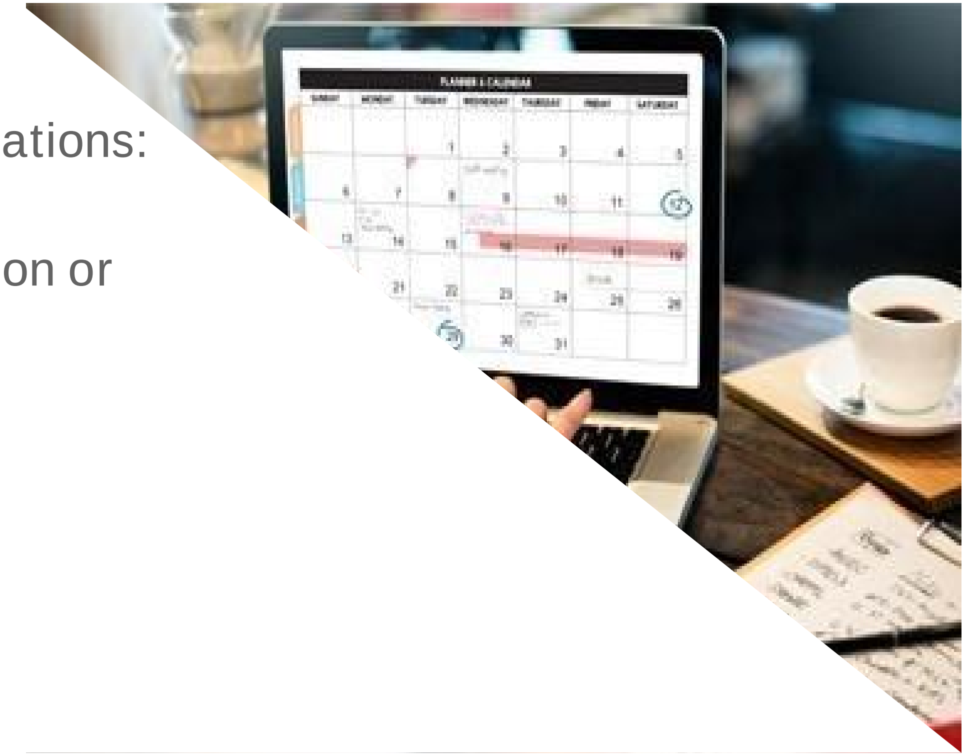
Increase Application Flexibility

- Evaluate a variety of different subject matters
- Apply criteria to entity-wide risks and controls
- Perform traditional SOC 2 engagements
- Recognize that service organizations operate in varying environments with varying risks

2017 Trust services criteria update

When are the 2017 TSC required?

- SOC 2 – SOC for service organizations: trust services criteria
  - Required for periods ending on or after 15 December 2018
  - Early adoption permitted
- SOC for cybersecurity
  - Applies immediately



2017 Trust services criteria update

What were the inputs to the update?

- Committee of Sponsoring Organizations (COSO)'s Internal Control – Integrated Framework
- COBIT 5
- NIST's Special publication 800 series
- NIST's Cybersecurity Framework
- ISO/IEC 27000 series standards
- HIPAA Security Rule
- PCI's Data Security Standard

2017 Trust services criteria update

Key changes

1

Terminology change from principle to category:

- Principles: 17 COSO principles within the five components of internal control

2

Restructure to align with the 17 principles in the COSO 2013 framework

3

Additional SOC 2 criteria organized by functional areas

4

Category-specific criteria address specific subject matter

5

Restructure and reorganization

- Reduction in redundancy
- Flexibility in application

6

Point of focus

- Drive further consistency across reports
- Likely increase granularity for most current reports in some areas

7

Risk assessment process

- Continued area of focus
- Basis for the effectiveness of control design
- Part of mngt's assertion

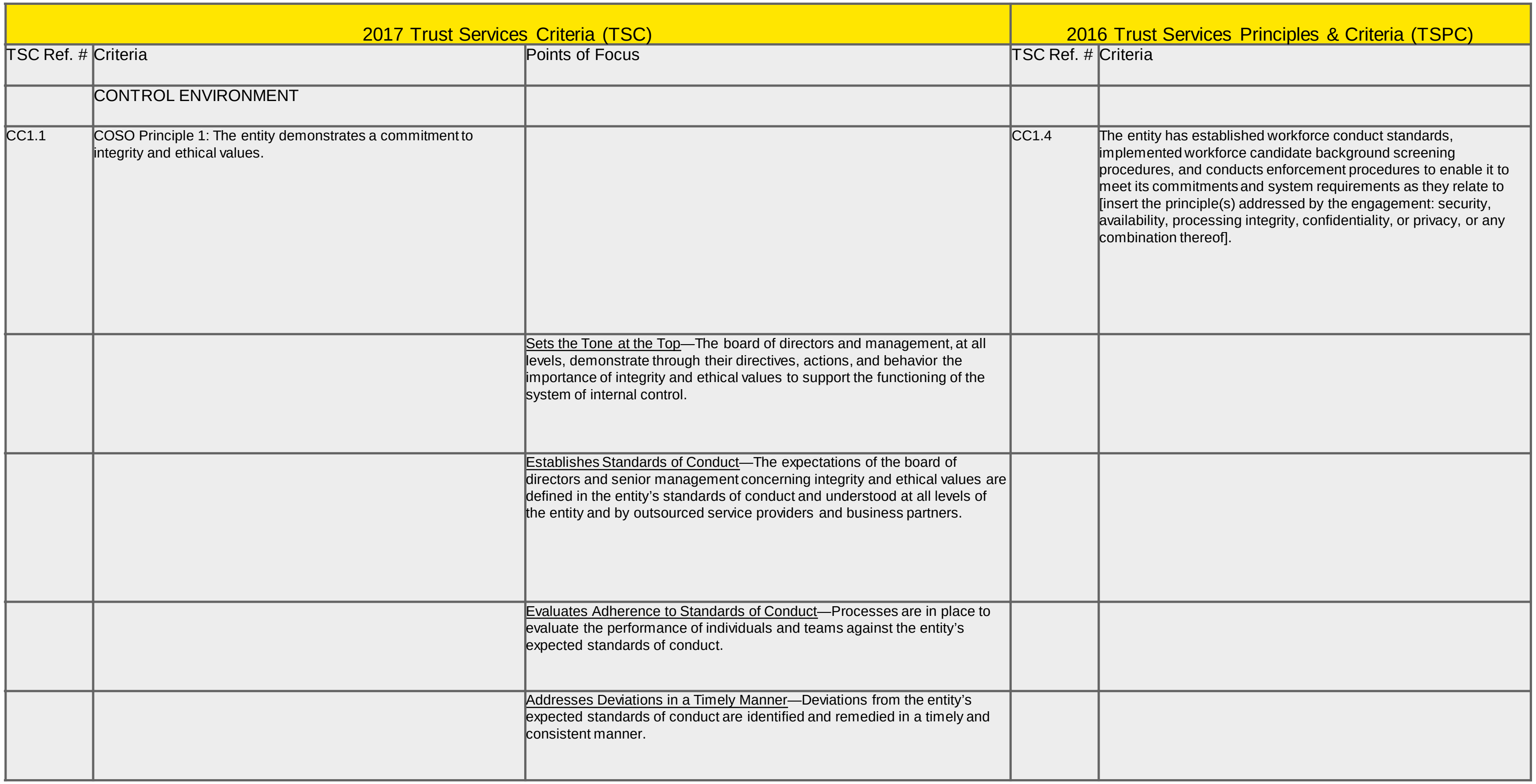
8

Risk mitigation

- Covers areas not addressed by direct controls

2017 Trust services criteria update

Example



2017 Trust Services Criteria (TSC)			2016 Trust Services Principles & Criteria (TSPC)	
TSC Ref. #	Criteria	Points of Focus	TSC Ref. #	Criteria
	CONTROL ENVIRONMENT			
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.		CC1.4	The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to [insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof].
		Sets the Tone at the Top—The board of directors and management, at all levels, demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the system of internal control.		
		Establishes Standards of Conduct—The expectations of the board of directors and senior management concerning integrity and ethical values are defined in the entity's standards of conduct and understood at all levels of the entity and by outsourced service providers and business partners.		
		Evaluates Adherence to Standards of Conduct—Processes are in place to evaluate the performance of individuals and teams against the entity's expected standards of conduct.		
		Addresses Deviations in a Timely Manner—Deviations from the entity's expected standards of conduct are identified and remedied in a timely and consistent manner.		

- Refer to http:// www.AICP.org/soc

Mapping TSC

Impact on SOC 2

Additional upcoming changes

1 SOC 2 Guide revision

2 SOC 2 Description Criteria update

3 Option to issue SOC 2 reports in accordance with ISAE 3000

Cyber Attestation standards

Cybersecurity

Expanding effects on our world today and other marketplace dynamics

- Stakeholders (e.g., board members, investors, regulators, business partners) only recourse has been to accept the minimal comfort provided by other activities that may be performed at an entity.
- These activities, however, have their limitations

Other activities	Limitations
External audit	• Cybersecurity-specific controls are rarely evaluated as part of the audit
Internal auditing	• Organizations are often challenged to the find qualified resources to perform comprehensive assessments
Boutique vendor assessment programs	• These programs generally lack consistency, objectivity and independence, and the deliverables provide no additional transparency into the cybersecurity risk management program
IT-sponsored security assessment against recognized frameworks (e.g., NIST Cybersecurity Framework, ISO)	• Value is affected by: • The scope of the assessment (broad vs. narrow) • The level of effort (extensive time vs. minimal time) • The competency of the resources executing the assessment
Vendor risk management program	• Activities are often high level and rely on feedback provided by the vendor/supplier with little, if any, validation
Supplier risk management program	

Cybersecurity

Stakeholders are looking for more

Given the marketplace's evolving business dynamics, the uncertain regulatory and legislative landscape, and the continued escalation of cybersecurity risks on business activities, stakeholders are looking for:

1 Transparency

More relevant information in the effectiveness of an entity's cybersecurity risk management program

2 Integrity

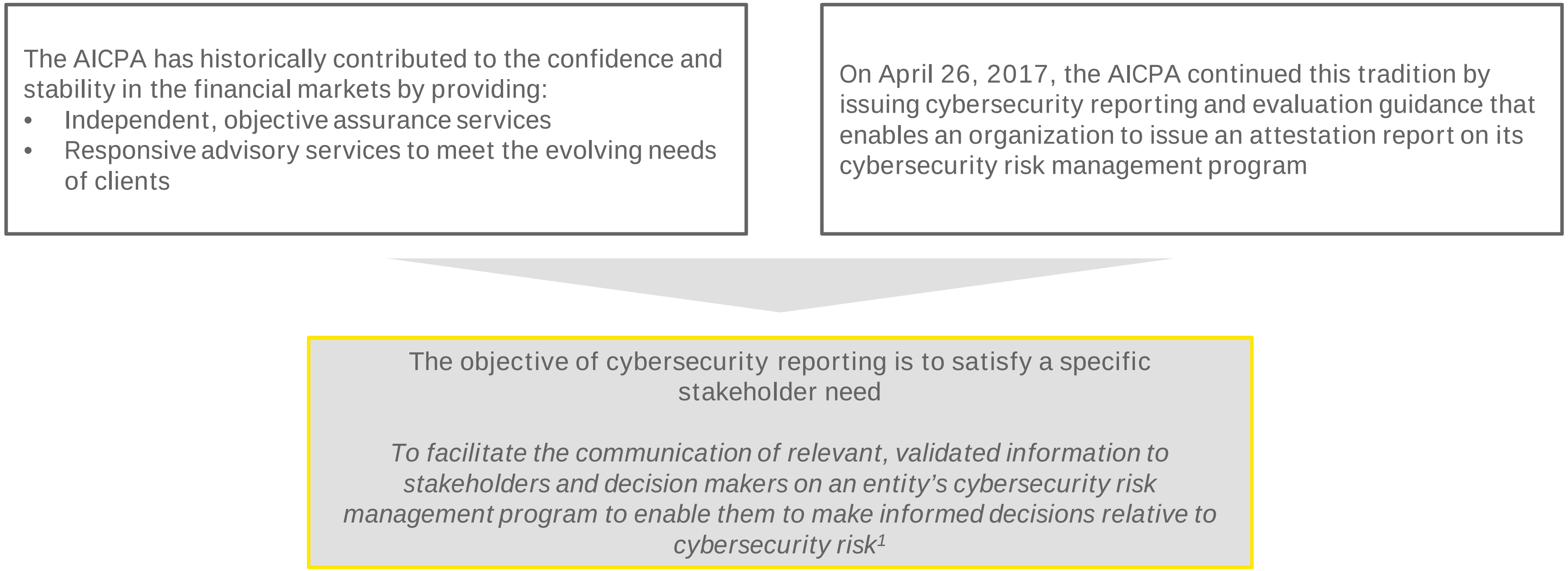
More assurance as to the integrity of the information being provided

3 Reliability

More clarity around the ability of the implemented cybersecurity risk management program to prevent and/or detect a significant cybersecurity breach

New cybersecurity risk management reporting option

Background



The AICPA has historically contributed to the confidence and stability in the financial markets by providing:

- Independent, objective assurance services
- Responsive advisory services to meet the evolving needs of clients

On April 26, 2017, the AICPA continued this tradition by issuing cybersecurity reporting and evaluation guidance that enables an organization to issue an attestation report on its cybersecurity risk management program

The objective of cybersecurity reporting is to satisfy a specific stakeholder need

To facilitate the communication of relevant, validated information to stakeholders and decision makers on an entity's cybersecurity risk management program to enable them to make informed decisions relative to cybersecurity risk[1]

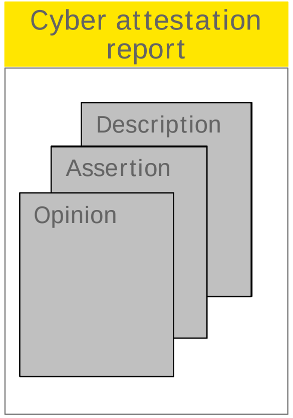
[1] Similar to SOCR, the description is presented as of point-in-time, with compliance testing optionally performed.

New cybersecurity risk management reporting option

Reporting model overview

The new reporting model …

- Includes a management's assertion and auditor's opinion to support the integrity of the information provided:
  - Assurance over: (1) the completeness and accuracy of management's description of its cybersecurity risk management program and (2) the operational effectiveness of the related controls
- Provides transparency into key elements of an organization's cybersecurity risk management program based on the defined criteria; key elements include an overview of:
  - The nature of the entity's business operations
  - The nature of the information at risk
  - The cybersecurity risk management program objectives
  - The factors that have a significant effect on cybersecurity risk
  - The entity's cybersecurity risk governance structure
  - The entity's cybersecurity risk assessment processes
  - The entity's approach to communicating its cybersecurity objectives, exceptions, etc.
  - The entity's cybersecurity processes that protect information and systems against the risks and threats the entity faces



Cyber-risk-management.pdf

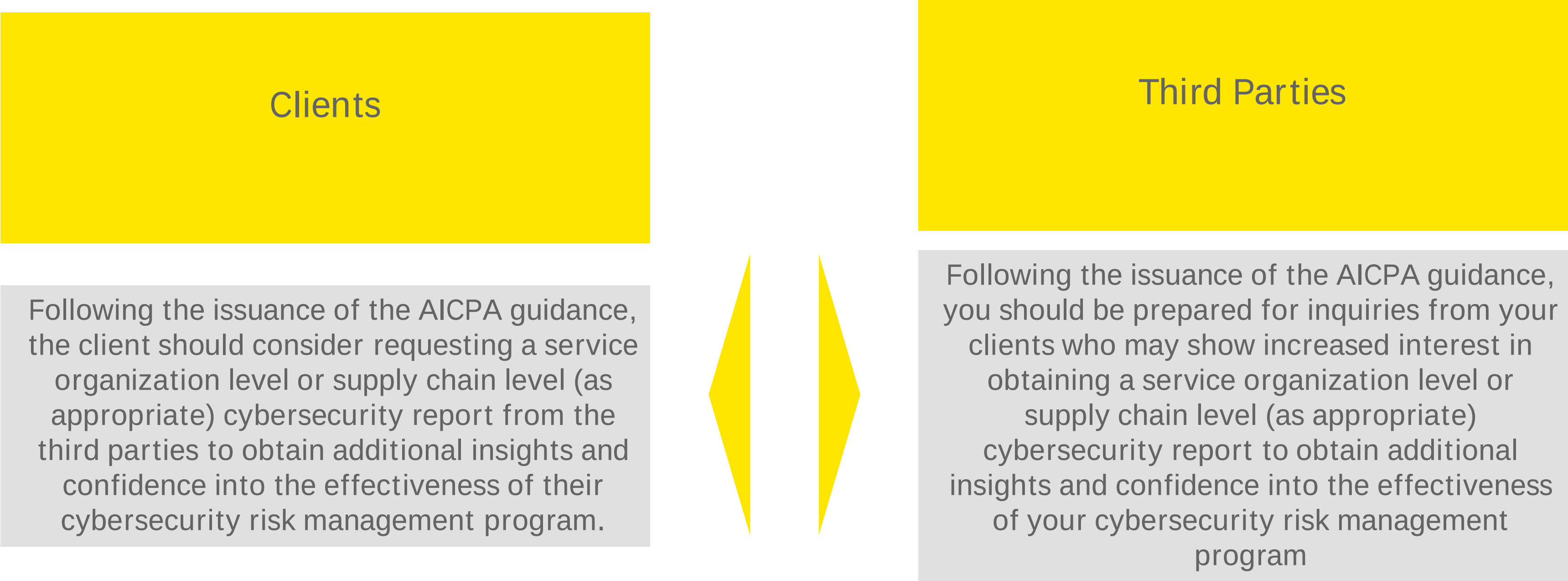
Note: While the new reporting model will address the stakeholders' need for greater visibility and confidence, management's assertion and the related opinion will not provide any form of assurance that a breach will never occur. Entities with a highly mature cybersecurity risk management effort will still retain a residual risk that a material cybersecurity breach can occur and not be detected in a timely manner.

Cybersecurity

Potential effect of cybersecurity reporting on the marketplace

Regulatory mandates

No regulatory mandate or legislative requirement requiring third-party service organization and supply chain level cybersecurity reporting has been put forth to date (and is not expected in the near term)



Clients

Following the issuance of the AICPA guidance, the client should consider requesting a service organization level or supply chain level (as appropriate) cybersecurity report from the third parties to obtain additional insights and confidence into the effectiveness of their cybersecurity risk management program.

Third Parties

Following the issuance of the AICPA guidance, you should be prepared for inquiries from your clients who may show increased interest in obtaining a service organization level or supply chain level (as appropriate) cybersecurity report to obtain additional insights and confidence into the effectiveness of your cybersecurity risk management program

Cybersecurity

Next steps

1

Stay focused on evolving regulatory and legislative initiatives:

- While no changes are currently anticipated, it is difficult to predict the challenging regulatory and legislative climate

2

Consider having a pre-assessment of your cybersecurity risk management program performed, especially those areas that have not been subject to previous audit scrutiny:

- For some companies, significant remediation activity may be required to address identified gaps
- Early identification of these gaps is essential to plan and execute remediation activities in an efficient, balanced and cost-effective manner

Questions?

D. (Dennis) Houtekamer RE
Executive Director

Mobile +31 6 2125 2728
Telephone: +31 88 407 8766
dennis.houtekamer@nl.ey.com

Ernst & Young Advisory
IT Risk and Assurance
Antonio Vivaldistraat 150
1083 HP Amsterdam
The Netherlands

ey.com/nl

Building a better working world

Appendix

AICPA SOC reporting options

Summary of reporting options utilizing trust services criteria

New report name	Old report name	Description criteria	Control criteria	Required trust services categories	Use summary
SOC for service organizations: trust services criteria	SOC 2	SOC 2 Guide	TSP section 100 or 100A*	Any combination of categories	Internal controls report over a system; detailed controls report
SOC for service organizations: trust services criteria for general use report	SOC 3	n/a	TSP section 100 or 100A*	Any combination of categories	Internal controls report over a system; summary controls report
SOC for cybersecurity	n/a	Description criteria for management's description of the cybersecurity risk management program	TSP section 100	Security, Availability, and Confidentiality	Cybersecurity risk management program report; effectiveness of overall program report
SOC for supply chain (future)	n/a	Description criteria for management's description of the supply chain (under development)	TSP section 100	Security, Availability, Confidentiality, and Processing Integrity	Internal controls report over a supply chain component; detailed controls report

* For periods ending on or after December 15, 2018 TSP 100 will be required. For periods ending before that date, either version is permissible.