

Emerging Third-Party Assurance (TPA) reports and other assurance trends

May 2021

Agenda

What is a System and Organization Controls (SOC) report 3

SOC for Cybersecurity 8

TPA for privacy 12

Cloud services and TPA 17

Controls modernization and digitization 22



What are SOC reports



What is a SOC report?

SOC reports represent an independent assessment of internal controls used to build trust and confidence with the recipients of such reports. SOC reports have historically focused on service organizations, however in 2017 the American Institute of Certified Public Accountants (AICPA) redefined the acronym SOC from service organization controls to system and organization controls. By redefining that acronym, the AICPA enabled the introduction of new internal control examinations that may be performed (a) for other types of organizations, in addition to service organizations, and (b) on either system-level or entity-level controls of such organizations.



Type I and Type II reports

Type I

- Testing and reporting over the design and implementation of internal controls at a point in time (e.g., as of June 30, 2019).
- Most often performed only in the first year a client has a SOC report.

Type II

- Testing and reporting over the design and operating effectiveness of internal controls over a period of time (e.g., for the period July 1, 2019 through June 30, 2020).
- Differentiating factor: Includes a description of the testing procedures performed by the user auditor and the results of testing performed.

Differences in SOC 1 and SOC 2 reports

Topic	SOC 1	SOC 2
Purpose of report	To provide information to the auditor of a user entity's financial statements about controls at a service organization that may be relevant to a user entity's internal control over financial reporting. It enables the user auditor to perform risk assessment procedures, and if a type 2 report is provided, to assess the risk of material misstatement of financial statement assertions affected by the service organization's processing	To provide management of a service organization, user entities and other specified parties with information and a CPA's opinion about controls over the service organization's system that may affect user entities' security, availability, processing integrity, confidentiality or privacy
Control Objectives	Determined by the client, in consultation with the Service Auditor	Defined by the AICPA TSC
Meaning of "Security"	Security is generally meant to cover authorization over transactions relevant to financial reporting	Broader concept that means safeguarding of data throughout the life cycle.
Boundary Definition	Largely implicit given the focus on financial reporting	Needs to be a specific emphasis of our procedures so that the reader is clear what is covered or not
Users of the report	Those with financial reporting responsibilities	Those with oversight responsibilities over the service organization; COOs CIOs
Distribution of the Report	Auditors of the user entity's financial statements, management of the user entities, and management of the service organization	Parties that are knowledgeable about <ul style="list-style-type: none"> • The nature of the service provided by the service organization • How the service organization's system interacts with user entities, subservice organizations, and other parties

AICPA SOC

SOC 2 for services organizations: Trust Services Criteria (TSC)

A SOC 2 is a report on controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy. These reports are intended to meet the needs of a broad range of users that need detailed information and assurance about the controls at a service organization relevant to security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems.

Purpose	<ul style="list-style-type: none">• Applicable TSC plus additional subject matter [Health Insurance Portability and Accountability Act (HIPAA), Health Information Trust Alliance (HITRUST), ISO-27001, etc.]
Use	<ul style="list-style-type: none">• Understanding of system components relevant to TSC• Information about operating effectiveness of controls• Information about operating effectiveness of relevant criteria beyond the required TSC
Control criteria	<ul style="list-style-type: none">• Defined by the AICPA TSC• Defined by criteria based on regulatory requirements• Defined by criteria established by an industry group
Intended users	<ul style="list-style-type: none">• Entities operating in particularly sensitive lines of work• Entities with knowledge about the nature of services covered; and how management's controls address the criteria• Entities seeking consolidation and additional efficiencies in overall compliance efforts

The five attributes of a system within a SOC 2 report are known as "Categories".



Common criteria (Security): The system is protected against unauthorized access, use, or modification (both physically and logically).



Availability: The system is available for operation and use as committed or agreed.



Processing integrity: System processing is complete, valid, accurate, timely, and authorized.



Confidentiality: Information designated as confidential is protected as committed or agreed.

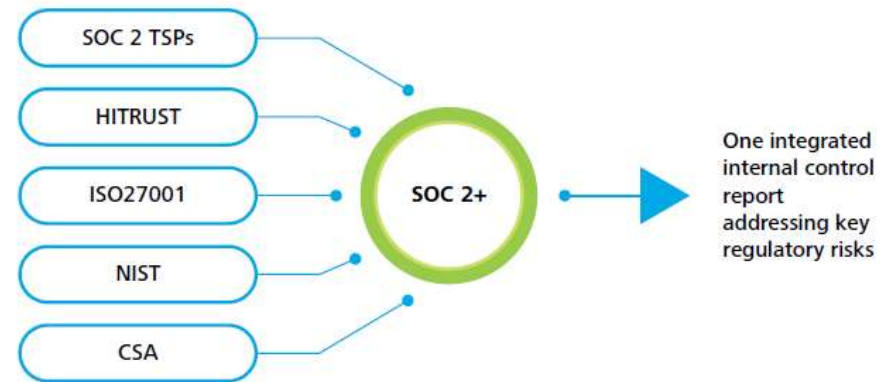


Privacy: Personal information is collected, used, retained, disclosed, and disposed to meet the entity's commitments and system requirements.

Adding other criteria (SOC 2+)

The AICPA has provided a great deal of flexibility with regard to inclusion of other control criteria in a SOC 2 report, creating the concept of a SOC 2+ report. Such a report can be used to demonstrate assurance in areas that go beyond the Trust Service categories and address industry-specific regulations and requirements.

Additional “suitable criteria” added to a SOC 2 report must be objective, measurable, complete, relevant, and available.



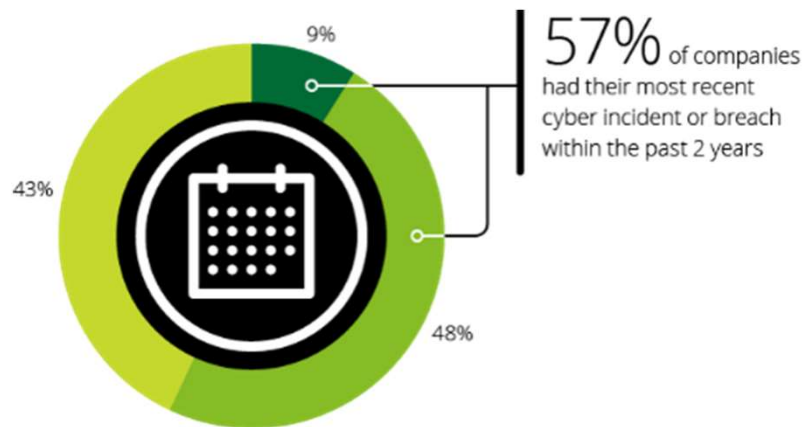
Framework	SOC 2+ Example
CSA (Cloud Security Alliance)	An organization has migrated its legacy applications and building new applications in a cloud environment for processing customer transactions. The organization needs to demonstrate controls in the cloud align to the CSA framework.
HITRUST	An outsourced service provider (OSP) claims processor must have access to HIPAA data in order to execute its responsibilities. To demonstrate that it is adequately safeguarding personal health information, it maps its controls to the HITRUST framework.
NIST (National Institute of Standards and Technology)	A company that maintains governmental contracts for building roads and bridges has contractual obligations to demonstrate how it meets the latest revision of NIST.
PCI-DSS (Payment Card Industry – Data Security Standard)	An OSP payment processor stores credit card information for future payments. Its customers want to know the details of the OSP’s controls beyond the PCI certification. In situations where there is no PCI certification, there is a need to demonstrate what controls are in place.

SOC for Cybersecurity



Cybersecurity incidents are not stopping despite significant investments both globally and in the US

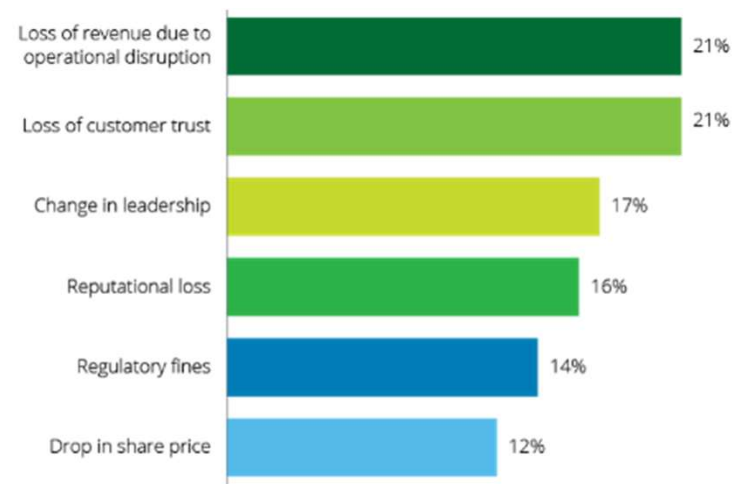
Timing of most recent cyber incident or breach among total participants



Among those who have experienced a cyberattack

- Within past year
- 1-2 years ago
- More than 2 years ago

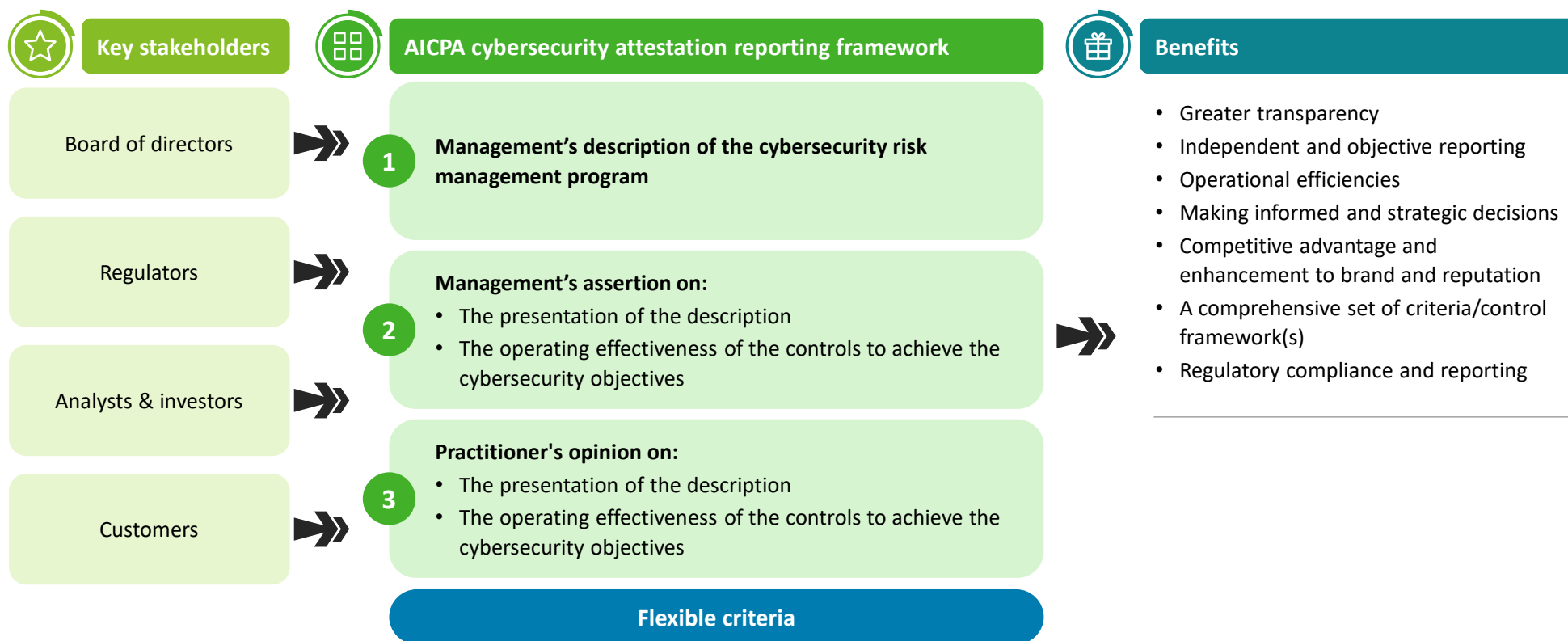
Biggest impacts of cyber incidents or breaches on organizations



Source: The future of cyber survey 2019 | Cyber everywhere. Succeed anywhere. Deloitte Development LLC. See www2.deloitte.com/us/en/pages/advisory/articles/future-of-cyber-survey.html

AICPA's cybersecurity attestation reporting framework

On April 24, 2017, the AICPA released its cybersecurity attestation reporting framework (SOC for Cybersecurity), which is intended to expand cyber risk reporting to address the marketplace need for uniformity and greater stakeholder transparency.



Sources:

Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program
<https://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/AICPACybersecurityInitiative.aspx>

SOC for Cybersecurity readiness considerations

Environment complexity

- What is the nature of the entity's IT control environment?
 - High/medium/low complexity
 - Centralized (i.e., common processes and controls) vs. decentralized
- What is the total number of specific IT risks and related controls?

Program maturity

- What is the level of maturity of the entity's cybersecurity risk management program?
 - Formal assessment of the company's overall IT risk and controls profile/posture
 - Group(s) responsible for performing these assessments across the "three lines model"
 - Risk assessment and reporting to the board and senior management

Control framework adoption

- Has the company adopted a cybersecurity control framework (e.g., control criteria – NIST-CSF, ISO 27001/2, revised AICPA TSCs)?

Asset inventory and risk assessment

- Does a reasonably complete and accurate information system asset inventory (application and infrastructure) exist?
- Has a formal information system asset criticality assessment been performed (i.e., identification of the highest criticality assets)?
- Has mapping of the highest criticality applications to corresponding infrastructure technology elements (databases, operating systems, network, tools/utilities) been performed?

TPA for privacy



Framing today's pressing data privacy challenges

With the roll-out and enforcement of new privacy laws, we will all have additional privacy rights in the near future. The increase in consumer focus on privacy has brought with it fundamental changes to today's privacy marketplace.

Evolving regulatory landscape

Since the introduction of the EU General Data Protection Regulation (GDPR)¹ in 2018, a slew of new data protection regulations have disrupted core sectors ranging from privacy to data localization.

Consistent collection and proliferation of personal data

As the volume and veracity of data collected by businesses grow, so do the costs and complexity around managing and securing that personal data.

54% of US Consumers

will potentially be provided new protections and rights with new privacy regulations, either already enacted or currently under consideration²

20% of companies

are making new privacy technology implementation a priority only after privacy programs have matured³

49% of companies

have made governance of data processing and the formation of a privacy-aware culture a top priority³

Increased operational burden to effectuate privacy compliance

One-off approaches to privacy compliance have resulted in narrowly-focused, scattered, or siloed privacy initiatives, creating operational and financial constraints particularly for businesses with a global footprint.

Digital resilience and excess collection of data due to COVID-19

The ongoing pandemic has forced companies to expand their digital footprint to preserve connectivity and business profitability. At the same time, companies should remain well positioned to protect user privacy.

Increase in customer control and consciousness

Gaining the privacy-conscious consumers' trust has been challenging to many of our clients, and consumer-facing businesses without transparent messaging around privacy can create confusion in the market, further deteriorating consumer confidence.

New and emerging technologies' reliance on personal data

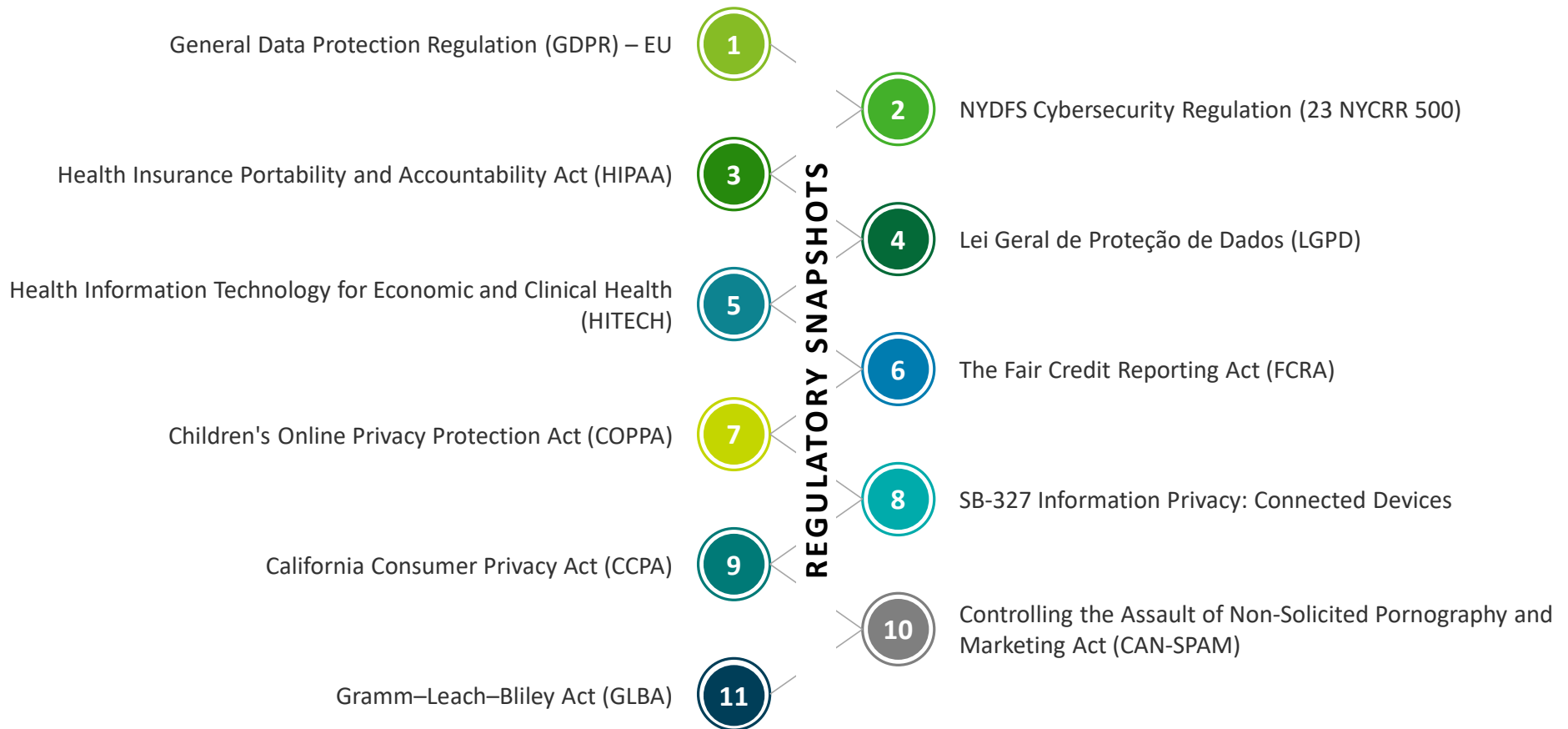
The rapid rise of emerging tech, including artificial intelligence (AI), automation, Internet of Things (IoT), 5G, facial recognition, and cloud technologies, has created unprecedented business opportunities, but also invited new scrutiny around data privacy.

Sources:

1. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>
2. <https://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx>
3. <https://www.prnewswire.com/in/news-releases/acpo-magazine-report-highlights-organization-challenges-and-priorities-as-data-protection-and-privacy-go-mainstream-803202904.html>

Framing today's pressing data privacy challenges (continued)

With the roll-out and enforcement of new privacy laws, we will all have additional privacy rights in the near future. The increase in consumer focus on privacy has brought with it fundamental changes to today's privacy marketplace.



Reporting options

The reporting mechanism can be tailored for each organization as needed.

Report type	Description	Relevant framework(s) addressed		
		SOC 2 common criteria	SOC 2 privacy criteria	GDPR/CCPA/other
SOC 2 privacy	A basic level of privacy assurance may be provided by issuing a SOC 2 report that includes the 18 TSC in the Privacy Trust Service Category promulgated by the AICPA.	Yes	Yes	No
SOC 2+	Building on the SOC 2 report with the Privacy TSC described above, a SOC 2+ report enables the inclusion of additional frameworks, such as GDPR or CCPA, to provide an additional level of assurance.	Yes	Optional	Yes
AT-C 205	Alternatively, an AT-C 205 report, which has a similar look and feel to a SOC 2 report may be issued. Such a report can also address privacy frameworks, such as GDPR or CCPA, without the added requirement of addressing SOC 2 TSC.	No	No	Yes

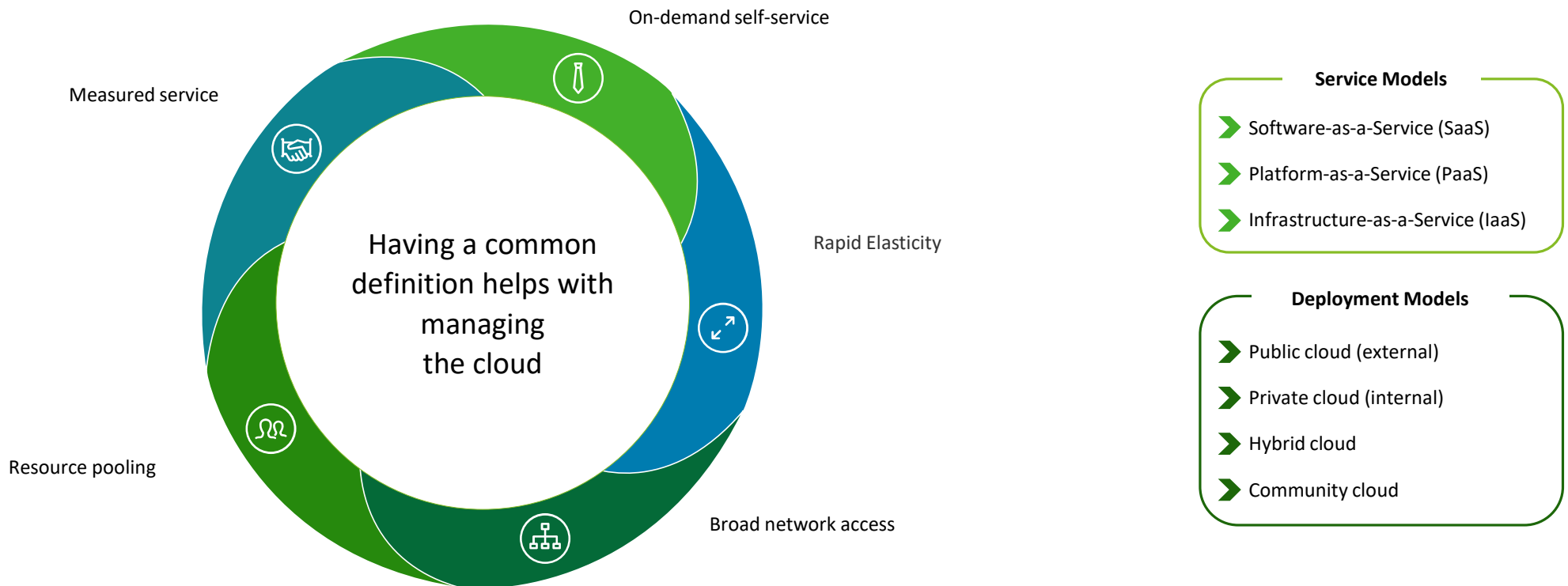
Cloud services and third-party assurance



Overview of cloud computing

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

- *The NIST (National Institute of Standards and Technology) 800-145 Definition of Cloud Computing, Peter Mell and Timothy Grance, September 2011*



Cloud computing risk considerations

There are a variety of cyber risks associated with moving to the cloud, yet there are also opportunities

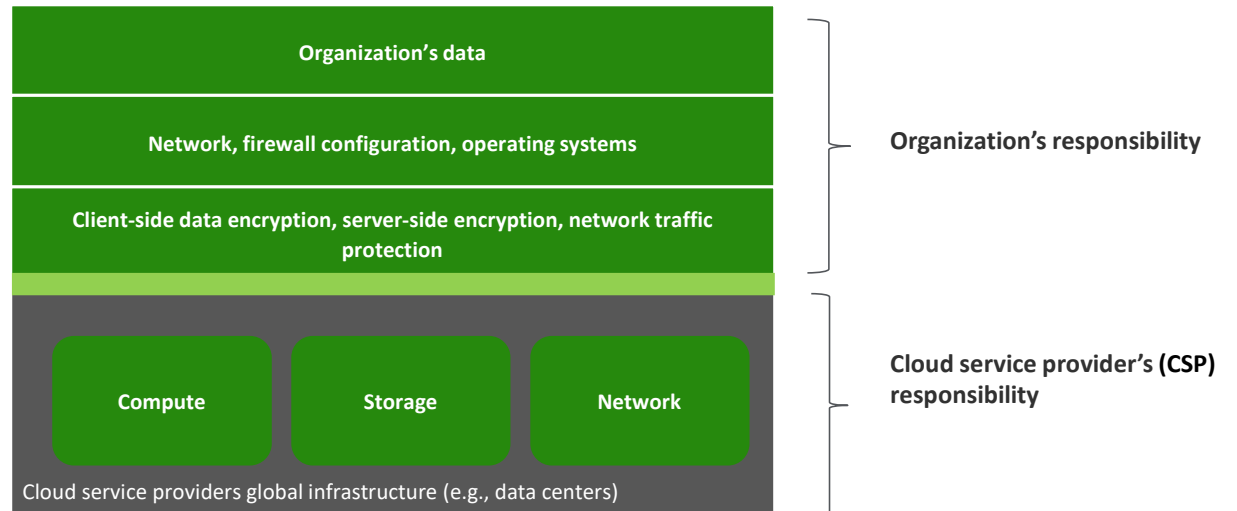


Shared responsibility model and compliance

Managing cyber risks in the cloud is a shared responsibility. Addressing control responsibilities in alignment with technology security and regulatory requirements is an important aspect of cloud adoption

Organizations should be familiar with this shared responsibility model and concept of **security OF the cloud and IN the cloud**, but things get complicated when we have different deployment models, service providers involved.

As a first step, organizations should develop a clear understanding of this shared responsibility and avoid **false sense of security**



Cloud service models—controls tested at different layers

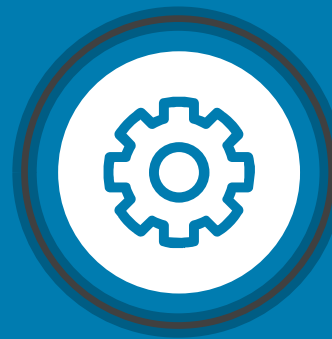
As organizations move up the cloud management stack, the level of ability to audit changes. Below is a typical chart but could vary depending on the CSP.

Technology stack	IaaS on-premise	IaaS CSP	PaaS CSP	SaaS CSP
Application	Audit directly	Audit directly	Audit directly	Audit directly
Middleware/Software stack	Audit directly	Audit directly	Audit directly / Rely on third-party SOC 1 & 2*	Rely on third-party SOC 1 & 2*
Servers and operating systems	Audit directly	Audit directly	Rely on third-party SOC 1 & 2*	Rely on third-party SOC 1 & 2*
Management console**	Audit directly	Audit directly / Rely on third-party SOC 1 & 2*	Rely on third-party SOC 1 & 2*	Rely on third-party SOC 1 & 2*
Hypervisor/Data storage/File storage	Audit directly	Rely on third-party SOC 1 & 2*	Rely on third-party SOC 1 & 2*	Rely on third-party SOC 1 & 2*
Physical	Audit directly	Rely on third-party SOC 1 & 2*	Rely on third-party SOC 1 & 2*	Rely on third-party SOC 1 & 2*

* - Need to perform typical audit procedures over the SOC 1 & 2 reports (scope, opinion, exceptions, control mapping, CUECs, etc.)

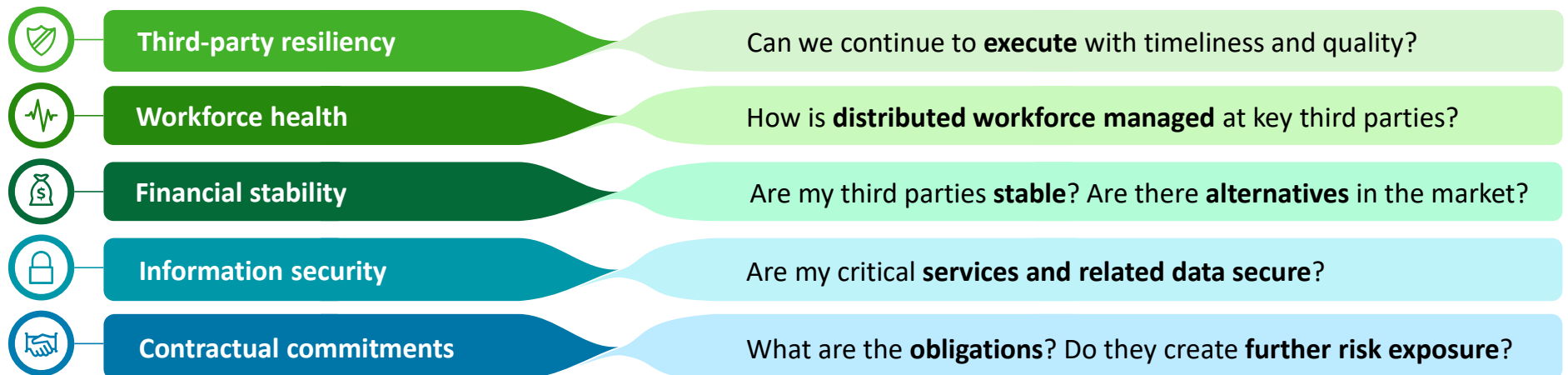
** - Refers to the hypervisor management console managing the underlying virtualized infrastructure for on-premise. IaaS scenarios would also include a management console for the cloud customers while the underlying hypervisor console is managed by the CSP.

Resilience meets controls modernization and digitization
























The impact of the COVID-19 pandemic on the extended enterprise

Now that 2021 is here, there continues to be a heightened focus on third-party service providers, leading to critical questions being asked of the extended enterprise:

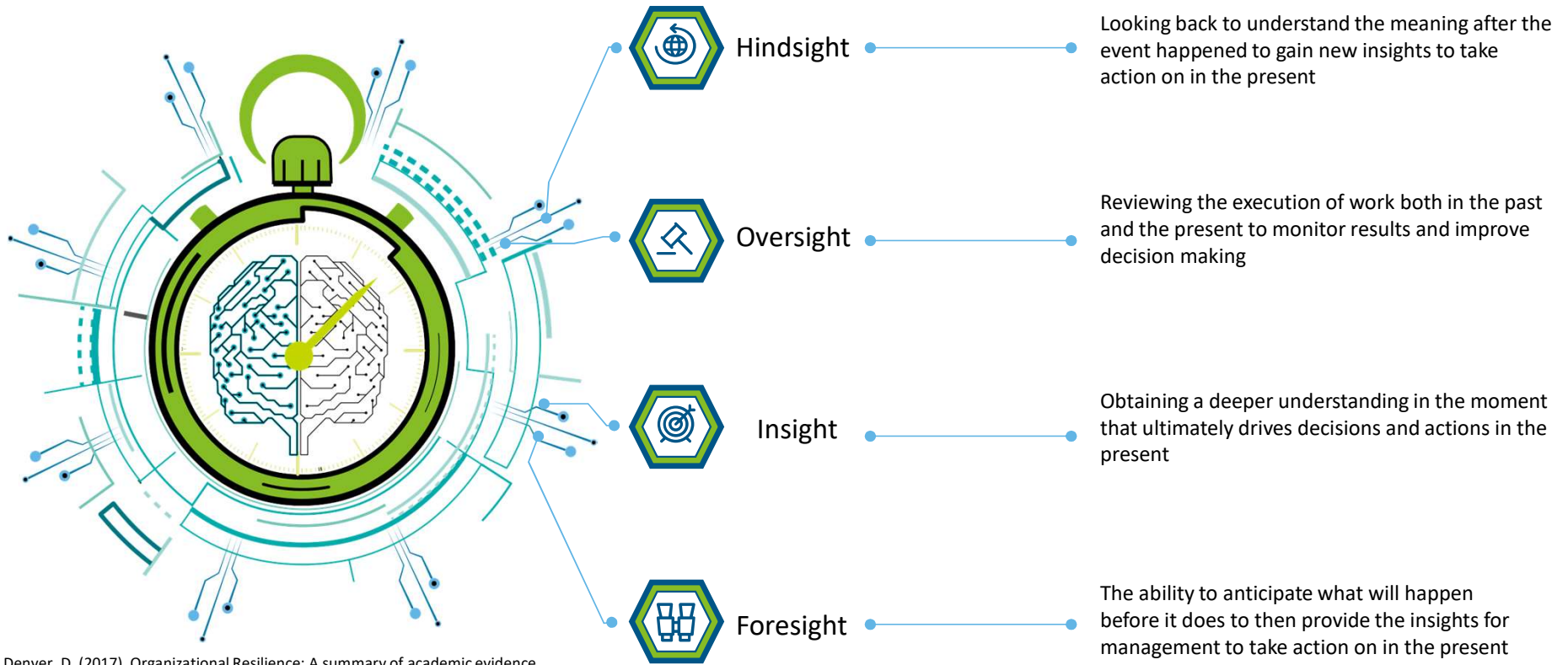


What area of concern still holds strong today during the pandemic and what has been addressed?

 Execution of controls & monitoring	 SOC report considerations	 Remote access	 Physical / manual controls
<ul style="list-style-type: none">  Reinforce the importance of “key” controls  Modify control activity to reflect updated methods of evidencing review  Confirm that appropriate transactional monitoring controls exist and are designed and operating effectively  Implement additional monitoring controls based on market conditions, as necessary 	<ul style="list-style-type: none">  SOC reporting implications <ul style="list-style-type: none"> • Modification to the description of the system and controls • Impact to the opinion • Modification to complementary user entity controls (CUECs) • Management Representation and Assertion • Bridge Letters  Proactive communication with user entities and auditors  Revisit subservice organization monitoring activity, including Complementary Subservice Organization Controls (CSOCs) 	<ul style="list-style-type: none">  Revisit user access provisioning such that granted access is appropriate and roles remain segregated.  Enhance security monitoring efforts aligned to new risks for both endpoint and network activity  Leverage monitoring efforts to gain insights on potential control frailties, people changes and impacted processes in order to risk assess and respond.  Perform threat modeling and defense rationalization. Consider threat hunting around new vectors 	<ul style="list-style-type: none">  Modify physical controls around restricted access to sensitive materials  Controls traditionally performed manually are forced to identify electronic processes  Identify alternate methods of control testing, to satisfy requirements in remote working environment
<ul style="list-style-type: none">  Increase activity  Continue to monitor frequently  Revert back to typical cadence 			

What is controls resilience?

"[A resilient organization] finds the right balance between 'defensive,' stopping bad things from happening, and 'progressive,' making good things happen. It has foresight, hindsight, insight, and oversight."⁴



⁴ Denyer, D. (2017). Organizational Resilience: A summary of academic evidence, business insights and new thinking. BSI and Cranfield School of Management.

Achieving controls resilience through digitization

Over the past five years, the way organizations operate has changed dramatically, but many controls and compliance programs have not kept pace. Digitization requires many considerations to achieve controls resilience.



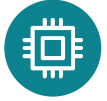
Resiliency

Management of risks proactively through adapting to emerging risks and new initiatives



Scalability

Reducing reliance on manual controls in order to scale to business needs and events



Optimization

Elevating professional productivity while focusing on exceptions and core risk management



Intelligence

Harnessing the power of analytics for insights and to “look around the corner”



Cost savings

Driving better efficiency, decreased reliance on capital investment, and rapid results

Identify relevant processes to drive value

Effective automation exists through focusing on high-value, high-risk, and time-consuming activities to reduce risk from manual processes.



Automate sound processes

01

Define business objectives

Take a top-down approach to define business objectives and identify the supporting processes and business groups.

02

Conduct cross-functional end-to-end workshops

Leverage workshops to understand connectivity amongst objective processes, risk, and controls and to detect gaps, inefficiencies, and improvement opportunities.

03

Define a process for digitization

Prioritization and intake of controls and control processes for digitization with consideration to the end-to-end conformance and compliance needs.

04

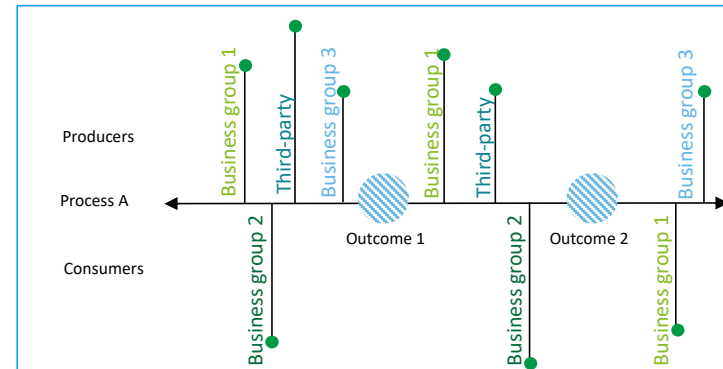
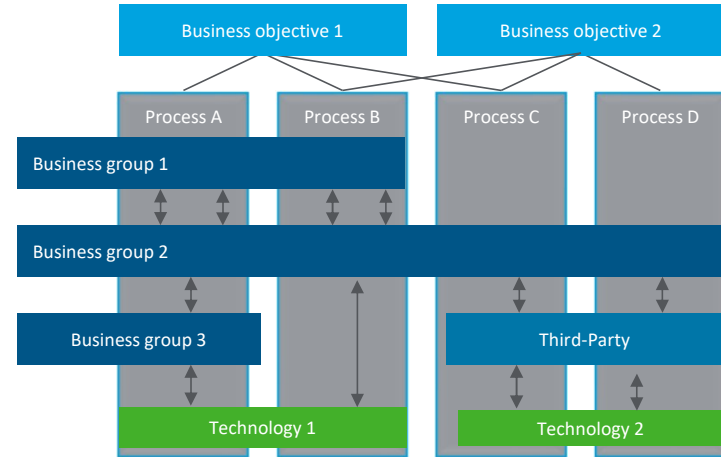
Identify gaps and improvement areas

Prioritize action items and remediation efforts and create sustainable model to continue to monitor achievement of business objectives.

05

Define ownership of future state

Provide training and clearly articulate ownership and accountability for future state.



Outcomes: milestones within an end-to-end process

Controls: activities performed by groups that achieve outcomes and mitigate risks.



This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2021 Deloitte Development LLC. All rights reserved.