CAPSULE8

The Rosetta Stone Guide to Compliance in a Cloud Native World

Cynthia Burke, Program Manager - Capsule8
May, 2020

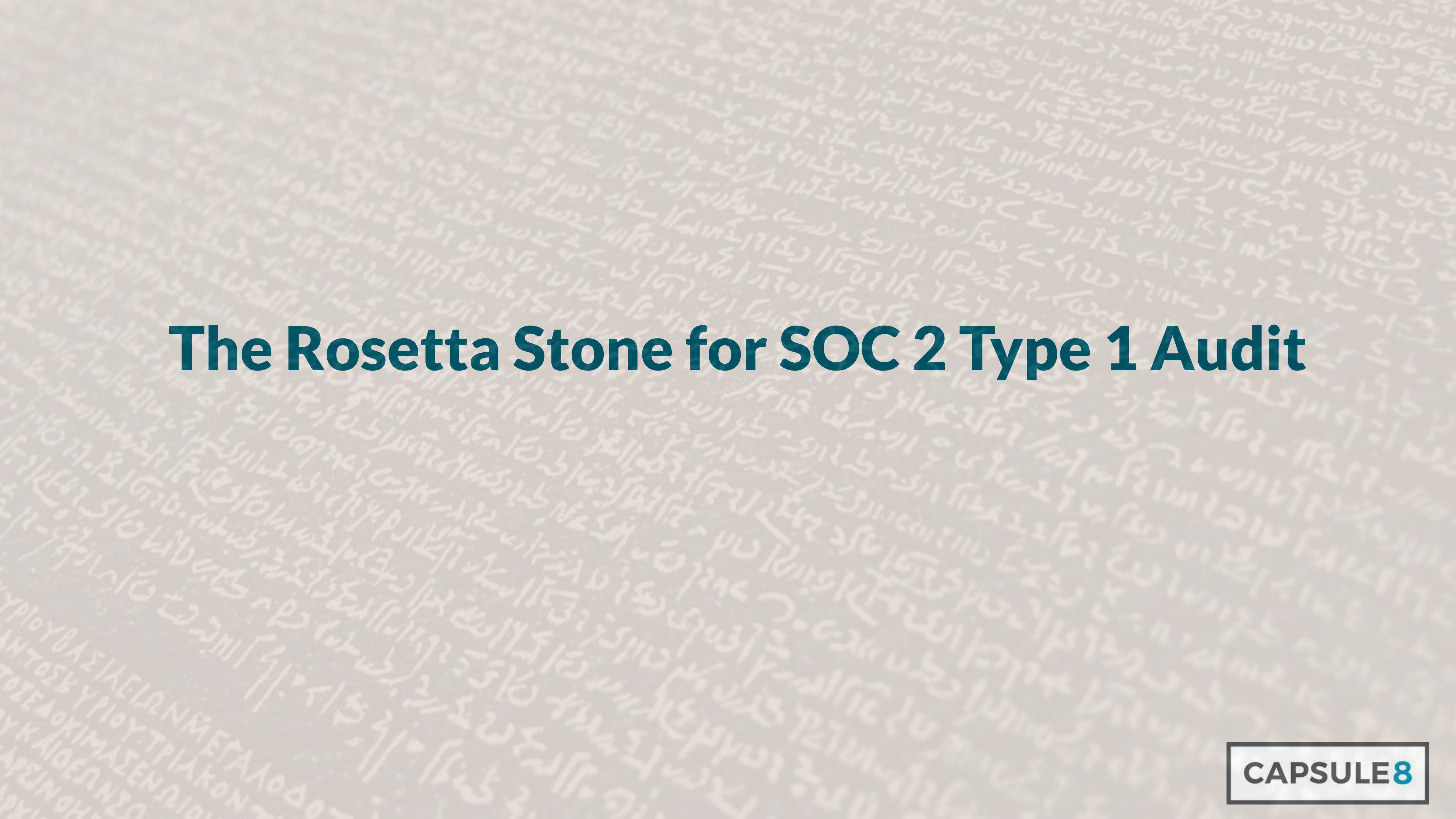
I’m Cynthia

CAPSULE8

You know compliance is important; you don’t want to make headlines. But how do you and your auditors stop speaking past each other?

Security of the cloud vs. Security in the cloud

How do those who have embraced cloud native platforms, infrastructures, and applications map controls created by the American Institute of Certified Public Accountants to assess service organizations (finally called SOC 2 in 2009) to modern infrastructures?



The Rosetta Stone for SOC 2 Type 1 Audit

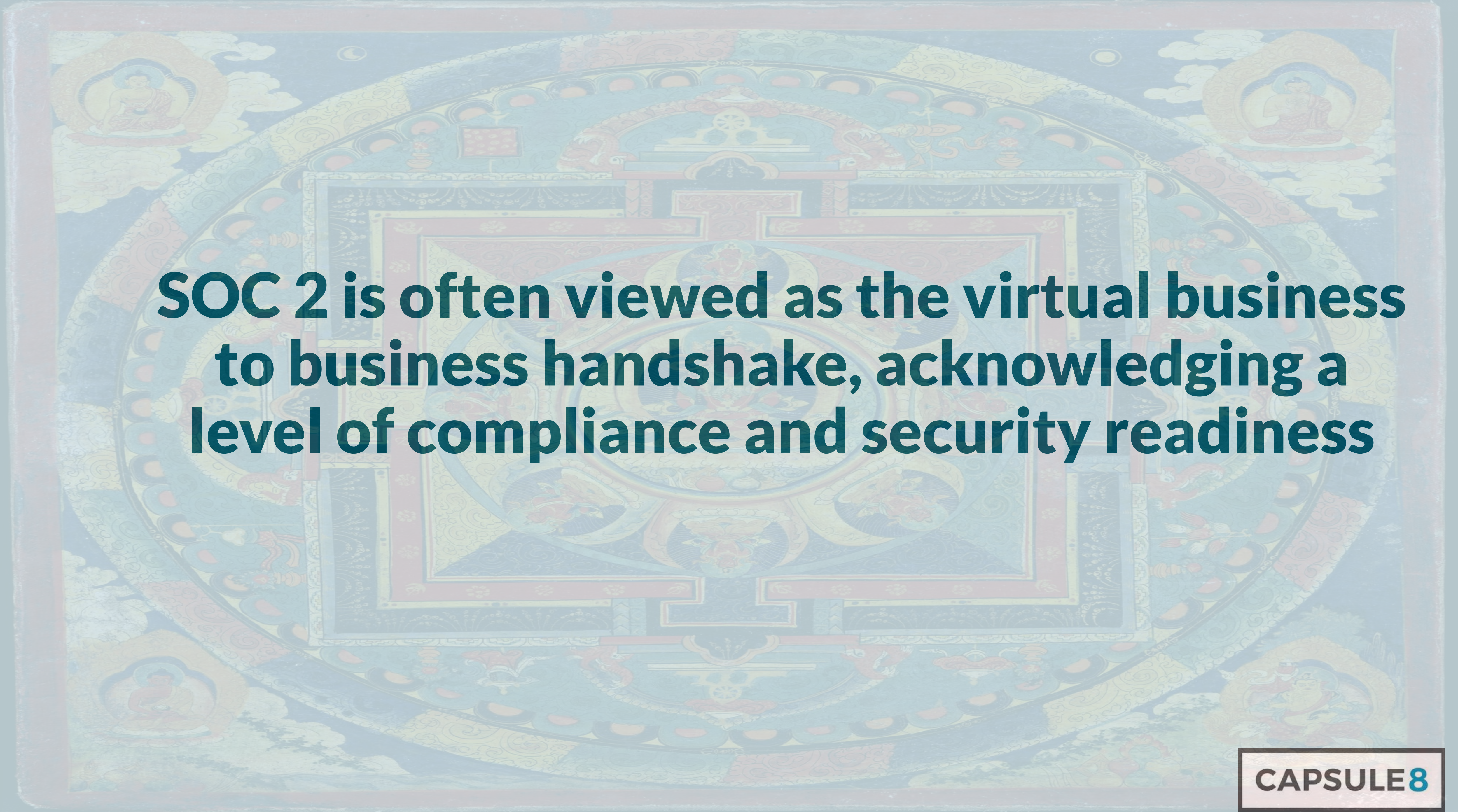
CAPSULE8

SOC 2 - Why Now?

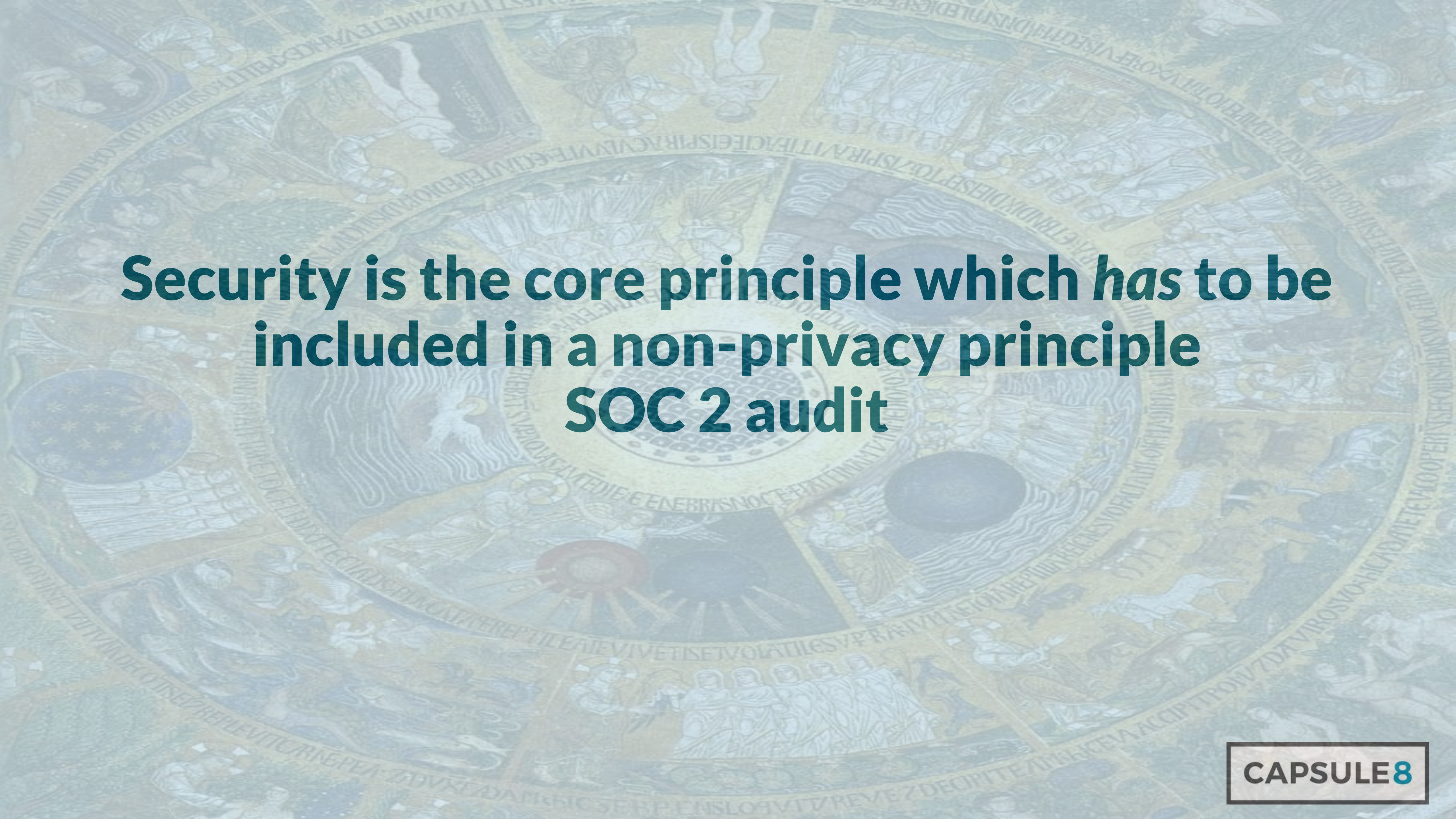
CAPSULE8

SOC 2 audits require an enormous breadth of reports; these reports can be repurposed for additional compliance endeavors

CAPSULE8



SOC 2 is often viewed as the virtual business to business handshake, acknowledging a level of compliance and security readiness



Security is the core principle which *has* to be included in a non-privacy principle SOC 2 audit

Assess Scope and Ownership of Controls and Choosing the Trust Service Criteria to Include

Responsibility Matrix for SOC 2 Controls and Audit Evidence Generation

Service Owner	SaaS	PaaS	IaaS
Data	Joint	Tenant	Tenant
Application	Joint	Joint	Tenant
Compute	Provider	Joint	Tenant
Storage	Provider	Provider	Joint
Network	Provider	Provider	Joint
Physical	Provider	Provider	Provider

Trust Service Criteria = Security, Availability, Process Integrity, Confidentiality, Privacy

CAPSULE8

MVP - SOC 2 Type 1

Who: service organizations which hold, store or process customer data

What: the *required* criteria are those pertaining to security:

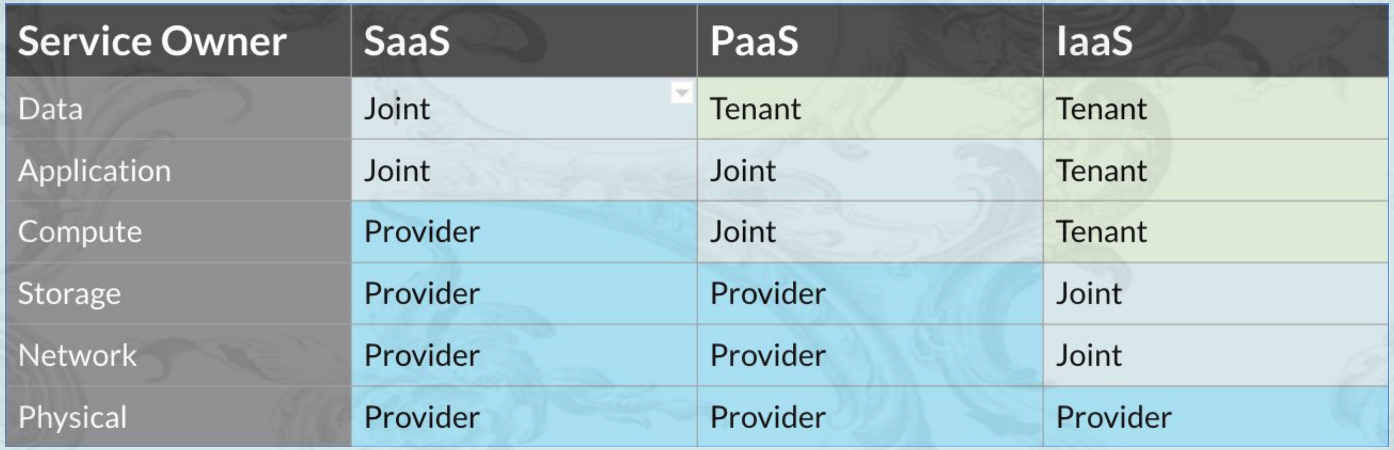
- CC 2.1 - Communication and Information
- CC 5.1 - Control Activities
- CC 6.1 - Logical and Physical Access
- CC 7.1 - System Operations
- CC 8.1 - Change Management

Where: The AICPA guidance can be found in a detailed online PDF

CAPSULE8

It’s not the destination, it’s the journey

Step 1: build your control matrix



Service Owner	SaaS	PaaS	IaaS
Data	Joint	Tenant	Tenant
Application	Joint	Joint	Tenant
Compute	Provider	Joint	Tenant
Storage	Provider	Provider	Joint
Network	Provider	Provider	Joint
Physical	Provider	Provider	Provider

Step 2: determine the trust service criteria in scope

Trust Service Criteria = Security, Availability, Process Integrity, Confidentiality, Privacy

Step 3: perform a gap analysis and remediate when necessary

(rise, lather, repeat)

Step 4: ready your communication skills

Successful audits are rooted in compelling compliance narratives

Help can be found in an appropriate frameworks, a well written summary, and clear test cases

Elements of the end-product - SOC 2 from an auditor’s perspective

- The service auditor’s report - a summary of their opinion
- Management’s assertion or summary of how controls are met
- A description of the system
- Tests of controls and corresponding results
- Any additional information provided by the service organization

Many SOC 2 controls are in no way anchored in cloud native concepts or practices.

The onus of informing the auditor is on the IT professional

Example 1:

CC 6.x Implements Boundary Protection Systems — Boundary protection systems (for example, firewalls, demilitarized zones, and intrusion detection systems) are implemented to protect external access points from attempts and unauthorized access and are monitored to detect such attempts

What are the appropriate test cases to show compliance without a software defined perimeter?

Example 2:

CC 7.x Conducts Vulnerability Scans — The entity conducts vulnerability scans designed to identify potential vulnerabilities or misconfigurations on a periodic basis and after any significant change in the environment and takes action to remediate identified deficiencies on a timely basis

How can you demonstrate periodic scans if you leverage ephemeral containers?

Sample SOC 2 audit of example 1

<table>
<tr><td colspan="4">Logical and Physical Access</td></tr>
<tr><td colspan="4">CC 6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives</td></tr>
<tr><th>Control #</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td>CC 6.8.2</td><td>IDS is accomplished by host based software deployed throughout each node in the fleet. The host based software monitors for malicious activities and triggers alerts, including a high, medium or low risk tag, to the organization's central security console. The software can monitor, log, and alert personnel of unauthorized or malicious behavior and keeps appropriate audit logs</td><td>The following MITRE ATT&CK tactics were demonstrated by the organization's staff and evaluated by the service auditor:
1. Privilege escalation including the attempt to launch a privileged container
2. Attempt to run a terminal shell in a container
3. Attempt to run netcat remote code execution in a container</td><td>No exceptions noted</td></tr>
</table>

CAPSULE8

Sample SOC 2 audit of example 2

<table>
<tr><td colspan="4"><b>System Operations</b></td></tr>
<tr><td colspan="4">CC 7.1 To meet its objectives the entity uses detection and monitoring procedures to identify 1. changes to configurations that result in the introduction of new vulnerabilities and (2) susceptibilities to new vulnerabilities</td></tr>
<tr><th>Control #</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td>CC 7.1.4</td><td>The organization base image source is from RedHat Universal Base Image. The organization leverages the yum package manager, removes unix shells, compilers and debuggers from the base image. A secretes management system is in place; secrets are never part of the base image. All containers are scanned via the CI pipeline at build and cannot be modified once deployed</td><td>A vulnerability was identified on a QA container and it was demonstrated that the container was spun down and replaced with a patched container image. The CI pipeline can be updated as needed to accommodate a change in the threat landscape</td><td>No exceptions noted</td></tr>
</table>

Safe answers to every SOC 2 control in a cloud native world:

1. How would I accomplish this in an on-premises infrastructure?

   Where's my Rosetta Stone?

2. How can I show like functionality in my cloud deployment, explain this clearly in an audit, and generate basic use cases to support it?

Trust Service Criteria Through the Lens of May 2020

CAPSULE8

Security in a workplace without boundaries

SOC 2 security criteria = *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*

Availability in an ephemeral world

SOC 2 availability criteria = *Information and systems are available for operation and use to meet the entity's objectives. Availability refers to the accessibility of information used by the entity's systems as well as the products or services provided to its customers.*

Process integrity in a highly matrixed delivery model

SOC 2 process integrity criteria = *Processing integrity refers to the completeness, validity, accuracy, timeliness, and authorization of system processing. Processing integrity addresses whether systems achieve the aim or purpose for which they exist and whether they perform their intended functions in an unimpaired manner, free from error, delay, omission, and unauthorized or inadvertent manipulation.*

Confidentiality and new challenges in physical security

SOC 2 confidentiality criteria = *Confidentiality addresses the entity’s ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity’s control in accordance with management’s objectives*

Privacy, when failure is not an option

SOC 2 privacy Criteria = *private personal information is collected, used, retained, disclosed, and disposed of to meet the entity's objectives*

Call To Action

Visit Capsule8's Cloud Native Compliance Playbook

CAPSULE8