WEBINAR:

SOC 2 COMPLIANCE & CERTIFICATION

YOUR IT COMPLIANCE PARTNER – GO BEYOND THE CHECKLIST

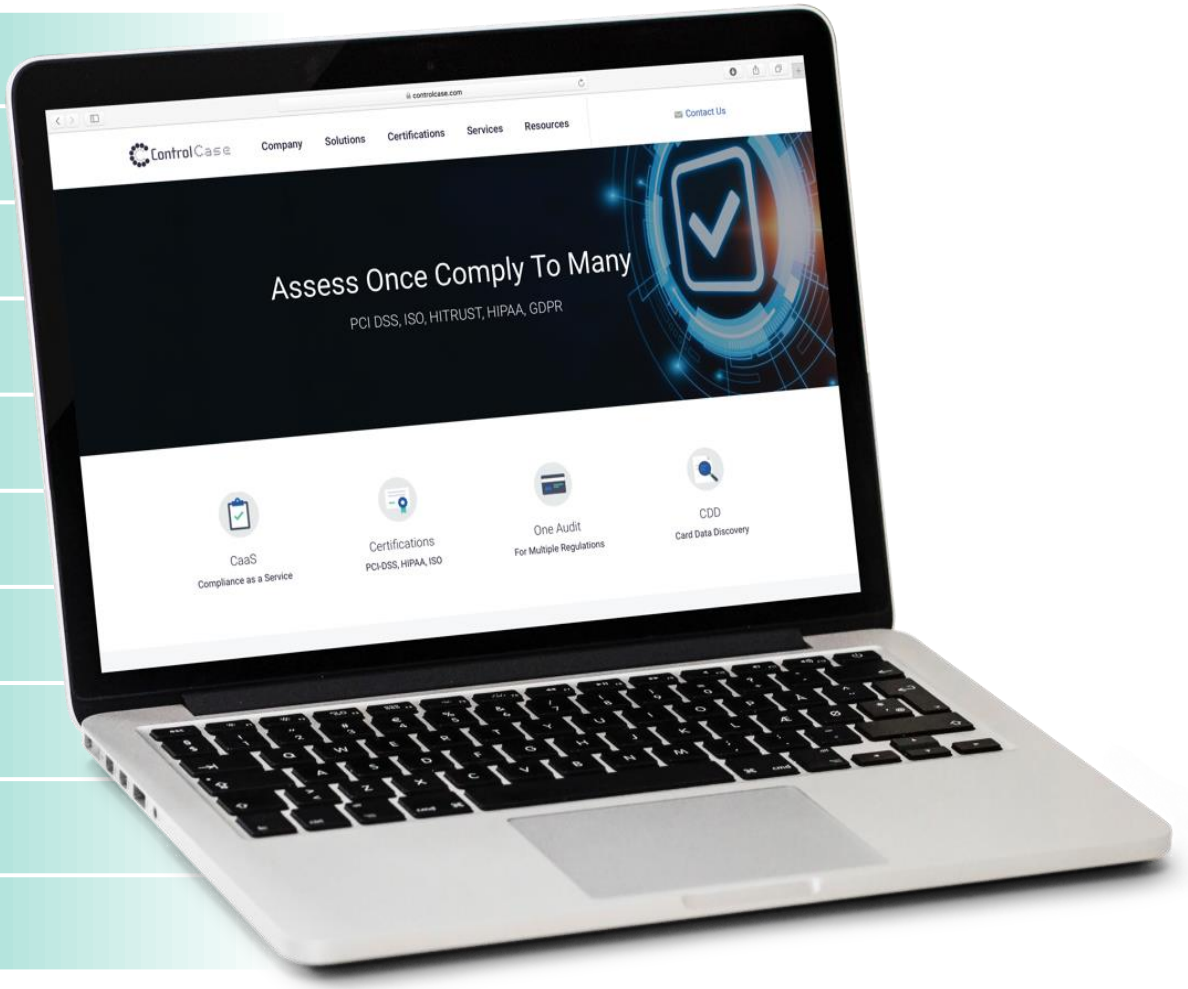
Download SOC 2 Compliance Checklist

SOC 2 Compliance Blog

Schedule SOC 2 Compliance Project Plan

Agenda

1. ControlCase Introduction
2. What does SOC stand for?
3. What is SOC 2 Compliance?
4. What is SOC 2 Certification?
5. What is a SOC 2 Report?
6. Who can perform a SOC 2 Audit?
7. How do Managed Service Providers Comply with SOC 2?
8. How to lower cost of SOC 2 Audit?
9. ControlCase Methodology for SOC 2 Compliance
10. Why ControlCase?



© 2021 ControlCase. All Rights Reserved.

1 CONTROLCASE INTRODUCTION

© 2021 ControlCase. All Rights Reserved.

ControlCase Snapshot

CERTIFICATION AND CONTINUOUS COMPLIANCE SERVICES

Go beyond the auditor's checklist to:

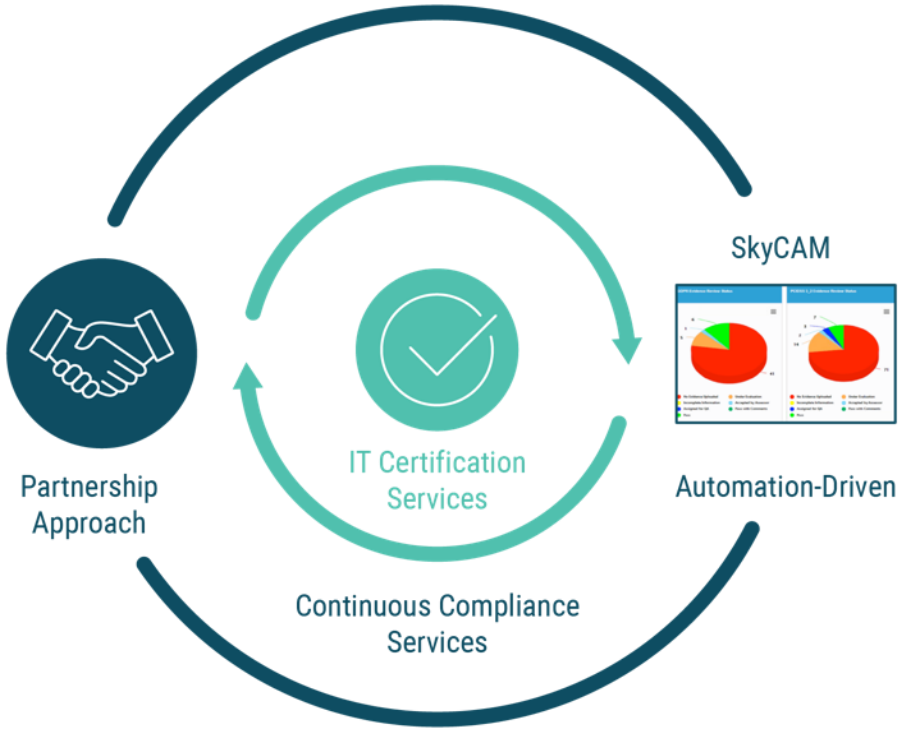
Dramatically cut the time, cost and burden from becoming certified and maintaining IT compliance.

- Demonstrate compliance more efficiently and cost effectively (cost certainty)
- Improve efficiencies
  - Do more with less resources and gain compliance peace of mind
- Free up your internal resources to focus on their priorities
- Offload much of the compliance burden to a trusted compliance partner

© 2021 ControlCase. All Rights Reserved.

Solution

Certification and Continuous Compliance Services



I've worked on both sides of auditing. ***I have not seen any other firm deliver the same product and service with the same value****. No other firm provides that continuous improvement and the level of detail and responsiveness.*

— Security and Compliance Manager, Data Center

© 2021 ControlCase. All Rights Reserved.

Certification Services

One Audit™

Assess Once. Comply to Many.


PCI DSS


ISO 27001
& 27002

SOC 1,2,3 & SOC
for Cybersecurity


HITRUST CSF


HIPAA


CCPA


GDPR

NIST 800-53

PCI PIN


PCI PA-DSS


FedRAMP


PCI 3DS

> *You have 27 seconds to make a first impression. And after our initial meeting,* ***it became clear that they were more interested in helping our business and building a relationship, not just getting the business****.*
>
> — Sr. Director, Information Risk & Compliance, Large Merchant

© 2021 ControlCase. All Rights Reserved.

2

WHAT DOES SOC STAND FOR?

© 2021 ControlCase. All Rights Reserved.

What does SOC stand for?

System and Organization Controls (SOC)

SOC represents a set of compliance standards developed by the American Institute of CPAs (AICPA) – a network of over 400,000 CPA professionals across the globe.	SOC Audits aim to examine the policies, procedures, and internal controls of an organizations.	There are 3 SOC Audits & Reports. • SOC 1 • SOC 2 • SOC 3

© 2021 ControlCase. All Rights Reserved.

What are the 3 types of SOC Reports?

SOC 1 (Financial Controls)	SOC 2 (Process/ IT Controls)	SOC 3 (Publicly Shareable)
• Reports on the processes and controls that influence the organization's internal control over financial reporting (ICFR). • This is because …the choices a company makes as a service organization may affect the financial reporting their users' organizations. • Standard assessment report required by user entities to comply with Sarbanes-Oxley Act (SOX)	• Designed for service organizations. • Reports on non-financial controls. • Focuses on five key trust services criteria (formerly called trust services principles), or TSCs. • SOC 2 outlines the standards that are necessary to keep sensitive data private and secure while it's in transit or at rest.	• SOC 3 is similar to SOC 2 in terms of the criteria. • The main difference is in the reporting - SOC 2 is tailored for sharing with specific organizations, whereas SOC 3 reports are more applicable for general audiences and therefore made publicly available.

© 2021 ControlCase. All Rights Reserved.

When are the Reports applicable?

Type 1	Type 2
• The service organization has not been in operation for a sufficient length of time to enable the service auditor to gather sufficient appropriate evidence regarding the operating effectiveness of controls, hence is “point in time”. • The service organization has recently made significant changes to their system and related controls and do not have a sufficient history with a stable system to enable a type 2 engagement to be performed.	• The service organization has had a long running stable system capable of demonstrating the effectiveness in the design of controls over a defined period of time retrospectively, normally no less than 6 months and not longer than 12 months.

© 2021 ControlCase. All Rights Reserved.

3

WHAT IS SOC 2 COMPLIANCE?

© 2021 ControlCase. All Rights Reserved.

What is SOC 2 Compliance?

		
SOC 2 focuses on non-financial reporting of internal controls and systems.	SOC 2 aims to protect the confidentiality and privacy of data that's stored in cloud environments.	SOC 2 compliance helps service providers show that the security, privacy, confidentiality and integrity of their customers' data is a priority.

© 2021 ControlCase. All Rights Reserved.

Who does SOC 2 Compliance apply to?

SOC 2 applies to any organization wanting to effectively demonstrate to associated organizations; controls associated with the selected Trust Service Criteria as part of third-party relationships. Any organization that stores its customer data in the cloud.	Third-party service providers such as cloud storage, web hosting, and software-as-a-service (SaaS) companies.

© 2021 ControlCase. All Rights Reserved.

What are the SOC 2 Trust Service Criteria?

SOC 2 defines criteria for managing customer data based on 5 “Trust Service Criteria” (TSCs):

1	2	3	4	5
SECURITY	AVAILABILITY	CONFIDENTIALITY	PROCESSING INTEGRITY	PRIVACY

© 2021 ControlCase. All Rights Reserved.

Security

Included in all SOC Audits.	Focuses on Common Criteria related to protecting data and systems.	Aims to ensure information and systems are protected against unauthorized access, disclosure and damage.

© 2021 ControlCase. All Rights Reserved.

Examples of what is included in the Security TSC

Penetration tests and vulnerability assessments	Application security measures	Firewalls	Intrusion detection systems (IDS)
Multi factor authentication tools	Access Control	Application and Network Security Measures	Computer Use Policies

© 2021 ControlCase. All Rights Reserved.

Availability

Addresses Accessibility (uptime).	Assesses the data that customers receive and how readily available it is.	Reviews accessibility for operations, monitoring, and maintenance.

© 2021 ControlCase. All Rights Reserved.

Examples of what is included in the Availability TSC

Performance and incident monitoring and response.	Disaster response and recovery. Replication and redundancy	Secure data backups.

© 2021 ControlCase. All Rights Reserved.

Confidentiality

Ensures “confidential” data remains protected and secure.	Encourages Encryption for in-transit data security.	Encourages client certificates and personal authentication certificates.

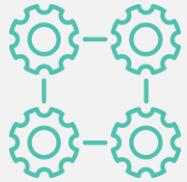
© 2021 ControlCase. All Rights Reserved.

Examples of what is addressed in the Confidentiality TSC

			
Digital access controls	Physical access controls	Network and application firewalls	Cryptographic solutions

© 2021 ControlCase. All Rights Reserved.

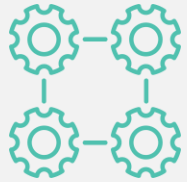
Processing Integrity



Ensures systems are processing the data as authorized.	Ensures the accuracy, completeness, validity and timeliness of the data.	Assesses that systems are achieving the goals and purposes that they were designed to achieve.

© 2021 ControlCase. All Rights Reserved.

Examples of what is included in the Processing Integrity TSC



Quality Assurance	Process Monitoring Systems

© 2021 ControlCase. All Rights Reserved.

Privacy

Reviews the onus of responsibility on the Privacy requirements of Personal Data(PII). *PII includes name, social security numbers, contact information, address .etc.*	Requires organizations to demonstrate that they protect and handle personal information securely.	Addresses how data is collected, used, disclosed, retained and disposed of.

© 2021 ControlCase. All Rights Reserved.

Examples of what is addressed in the Privacy TSC

Notice and communication of objectives	Choice and consent	Collection	Use, retention, and disposal
Access	Disclosure and notification	Quality	Monitoring and enforcement

© 2021 ControlCase. All Rights Reserved.

SOC 2 +

SOC 2 allows for Additional Subject Matter Assessments saving organizations time and cost	SOC 2 + GDPR SOC 2 + CCPA SOC 2 + GDPR and CCPA	Provides synergy of overlapping controls across multiple regulations

© 2021 ControlCase. All Rights Reserved.

4

WHAT IS SOC 2 CERTIFICATION?

© 2021 ControlCase. All Rights Reserved.

What is a SOC 2 Attestation?

SOC is not a Certification, it is an Attestation which is a type of audit report that attests to the trustworthiness of services provided by a service organization by a trusted source – a CPA, governed by the Code of Conduct of the AICPA.

© 2021 ControlCase. All Rights Reserved.

5 WHAT IS A SOC 2 REPORT?

© 2021 ControlCase. All Rights Reserved.

What is a SOC 2 Report?

There are 2 types of SOC 2 reports:

SOC 2 Type 1

Outlines management's description of a service organization's system and the suitability of the design and operating effectiveness of controls."

This report evaluates the controls at a specific point in time.

SOC 2 Type 2

Focuses not just on the description and design of the controls, but also actually evaluating operational effectiveness.

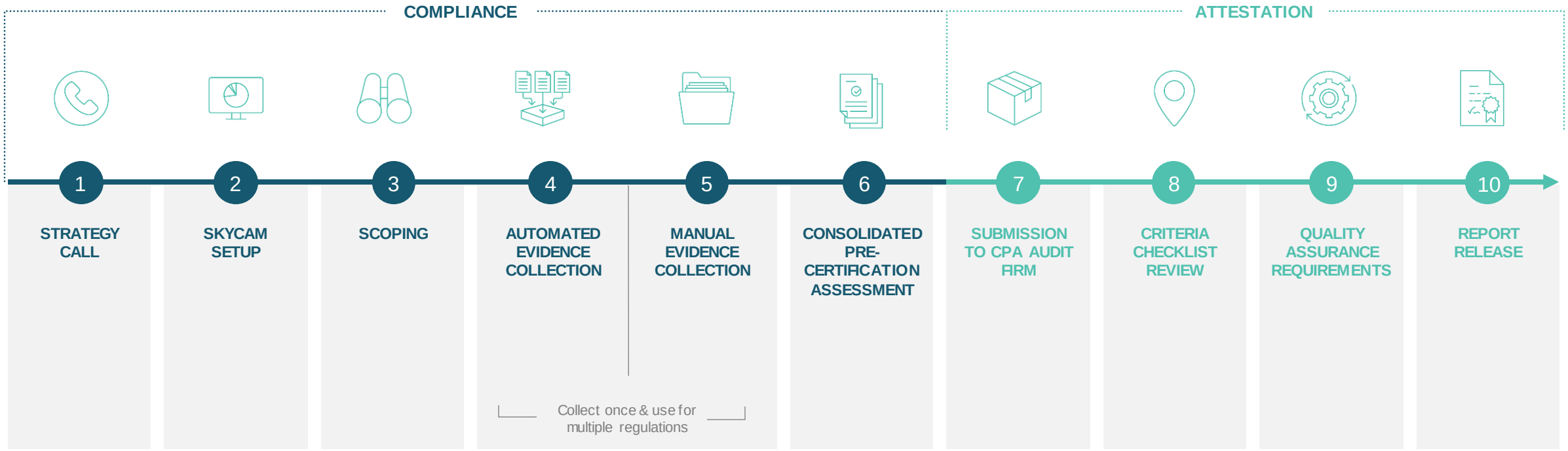
The report evaluates controls over an extended period retrospectively to ensure the effectiveness of the controls (normally no less than 6 months and no more than 12).

© 2021 ControlCase. All Rights Reserved.

WHAT IS THE PROCESS TO GET SOC 2 TYPE 2 ATTESTED?

© 2021 ControlCase. All Rights Reserved.

ControlCase SOC Attestation Methodology



© 2021 ControlCase. All Rights Reserved.

HOW DO MANAGED SERVICE PROVIDERS COMPLY WITH SOC 2?

© 2021 ControlCase. All Rights Reserved.

How do MSPs comply with SOC 2?

MSPs are generally required to comply with either SOC 1 or SOC 2 examinations depending on the services they render or scope of the services.

MSPs that handle, process, transmit or store financial data should have a SOC 1 performed.

MSPs enable their clients to inherit controls based on the relationship; for example, a Data Center provider's clients will automatically inherit controls that address physical and environmental security of the infrastructure.

MSPs that offer broader services than just financial should have a SOC 2 performed based on the TSCs required.

© 2021 ControlCase. All Rights Reserved.

HOW TO LOWER COST OF A SOC AUDIT?

© 2021 ControlCase. All Rights Reserved.

How to lower cost of a SOC 2 Audit?

Partner with existing SOC 2 Type 2 Attested MSPs.	Identify most appropriate TSCs that are relevant to your business.	Scope Reduction – architect the network to reduce scope.

© 2021 ControlCase. All Rights Reserved.

10

WHY CONTROLCASE?

© 2021 ControlCase. All Rights Reserved.

One Audit™

Assess Once. Comply to Many.

GDPR

CCPA

SOC 1,2,3 & SOC for Cybersecurity

ISO 27001 & 27002

HIPAA

FedRAMP

PCI DSS

NIST CSF

PCI PIN

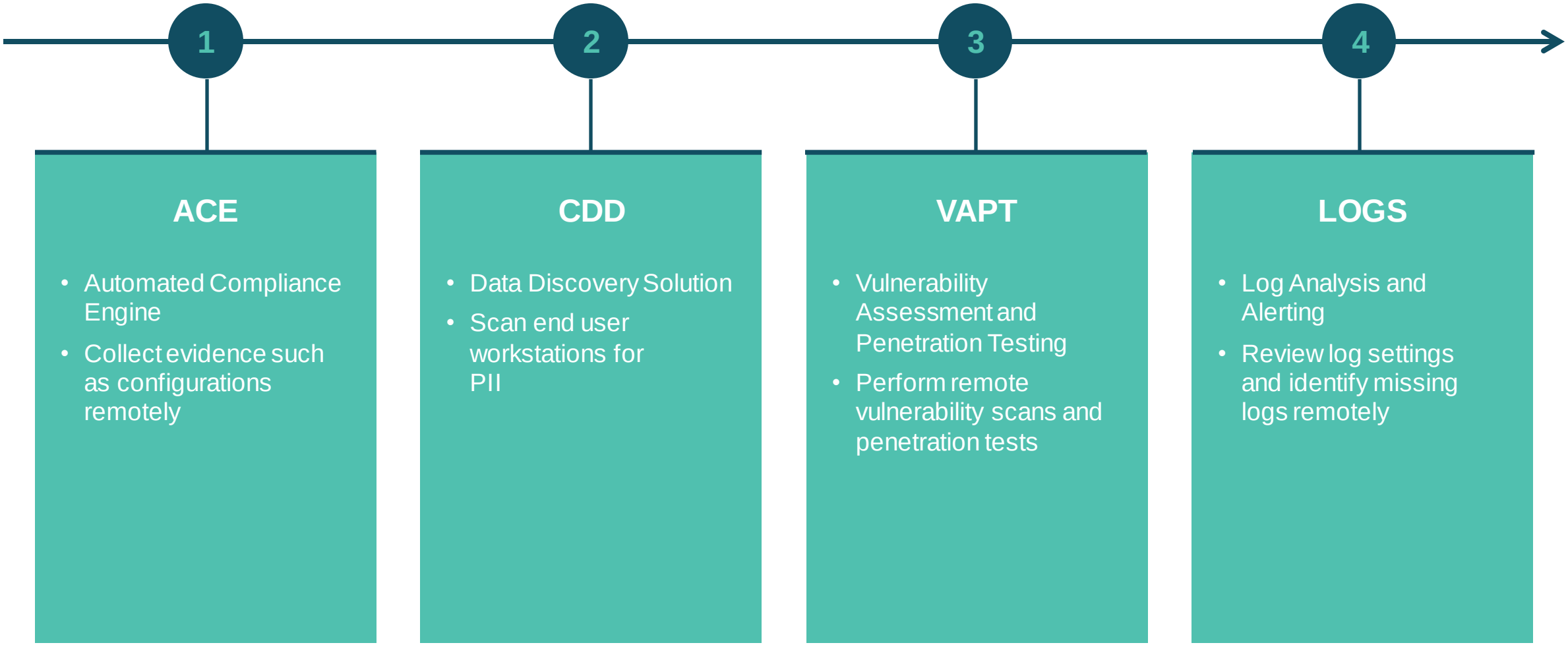
PCI PA-DSS

CSA STAR

Microsoft SSPA

© 2021 ControlCase. All Rights Reserved.

Automation



© 2021 ControlCase. All Rights Reserved.

Continuous Compliance Services

ControlCase Addresses Common non-compliant situations that may leave you vulnerable:

In-scope assets not reporting logs

In-scope assets missed from vulnerability scans

Critical, overlooked vulnerabilities due to volume

Risky firewall rule sets go undetected

Non-compliant user access scenarios not flagged

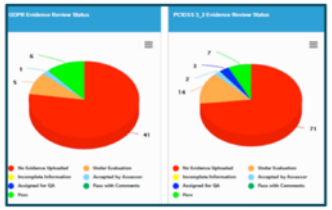
FEATURE:	**Package 1 -** With Cybersecurity Services*	**Package 2 -** Without Cybersecurity Services*
Quarterly Review of 15 to 25 Compliance Questions	✓	✓
Quarterly Review of Scope	✓	✓
Collecting & Analyzing Data through connectors from client systems	—	✓
Vulnerability Assessment	✓	—
Penetration Testing	✓	—
Sensitive Data Discovery	✓	—
Firewall Ruleset Review	✓	—
Security Awareness Training	✓	—
Logging & Automated Alerting	✓	—

* Hybrid package can be selected.

© 2021 ControlCase. All Rights Reserved.

Summary – Why ControlCase

Partnership Approach



SkyCAM IT Compliance Portal Automation-Driven

Continuous Compliance Services

> ***They provide excellent service, expertise and technology****. And,* ***the visibility into my compliance throughout the year and during the audit process provide a lot of value to us.***
>
> — Dir. of Compliance,
> SaaS company

© 2021 ControlCase. All Rights Reserved.

FREE 1 Hour Working Session - SOC Project Plan Development

SOC Project Plan Development

ControlCase will assist you in building your SOC project plan. The plan will cover:

- Address organizational buy-in
- Assist in identification of Key Personnel and their Roles.
- Parameterize Scope
- Define Observation Period
- Policy and Procedure Checklist
- Selection of applicable Trust Service Criteria

Email Amy Poblete to schedule your free working session - apoblete@controlcase.com

Email Amy Poblete Now to Secure your spot!

© 2021 ControlCase. All Rights Reserved.

THANK YOU FOR THE OPPORTUNITY TO CONTRIBUTE TO YOUR IT COMPLIANCE PROGRAM.

Download SOC 2 Compliance Checklist

SOC 2 Compliance Blog

Schedule SOC 2 Compliance Project Plan

www.controlcase.com

contact@controlcase.com