ControlCase
Compliance as a Service

Compliance as a Service (CaaS) Processes & SLAs

- Ashish Kirtikar

Agenda

- What is CaaS
- CaaS Team Structure
- CaaS Process Phases & SLAs
- CaaS Byproducts

ControlCase
Compliance as a Service

What is CaaS?

ControlCase
Compliance as a Service

What is Compliance as a Service (CaaS)?

- Establishes responsibility of monitoring and alerting on IT compliance throughout the year by means of,
  - Timely escalation letters
  - ConnectWise email based testing/interaction/alerting
  - QSA/CSM/Security Tester/Asset Manager interaction
- CaaS is ControlCase' s Business as Usual (BAU) product for IT Compliance and IT Certifications
- Annual certification to one or multiple IT regulations or standards for public consumption

ControlCase
Compliance as a Service

Value of Compliance as a Service?

- Alert on relevant items ONLY (i.e. our value is in providing compliance information not just raw scan results)
- How do we alert on relevant items within SLA's
  - › We know your compliance scope
  - › We know what will result in lapse of certification
  - › We map the risks of vulnerabilities, sensitive data and log alerts to compliance
  - › We map all logs to the relevant compliance requirements such as daily reports
- ControlCase will take ownership of this and deliver within established SLA's
- Communication through ConnectWise email and CSM's

ControlCase
Compliance as a Service

Who does what

Customer Environment

Customer Success Manager

Security Assessor

Testing Team

Asset Management Team

Certification Assessor

Compliance Portal KBOX

ConnectWise support portal

Your 1st level of interaction

Independent QSA/QA Team

Log Management Team

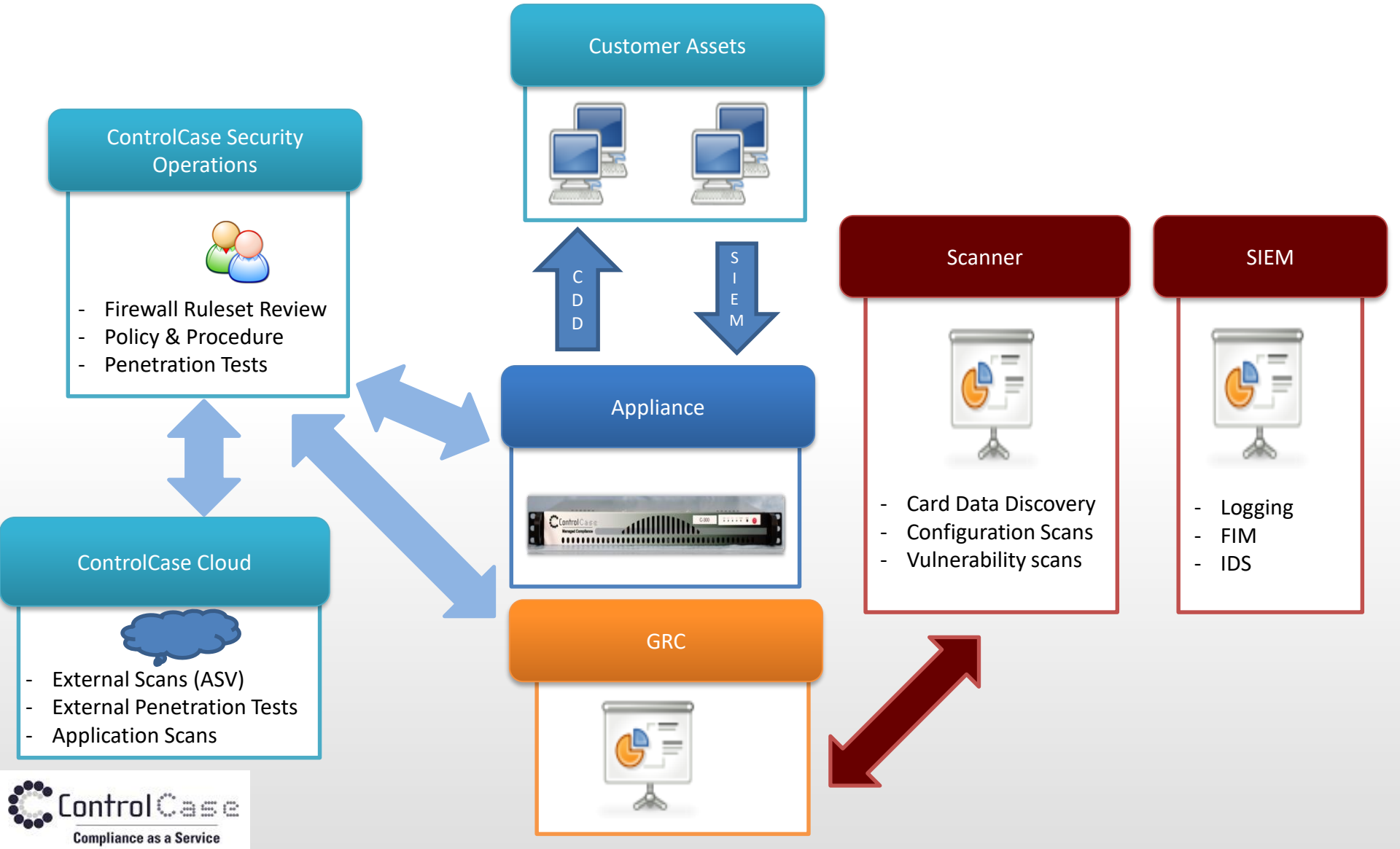
Support Team

Scheduler

Your 2nd level of interaction

ControlCase
Compliance as a Service

CaaS Data Flow



CaaS Processes & SLAs

Process Phases

- The CaaS offering will be delivered in the following phases:

Phases	Description
Phase I	Pre-scoping
Phase II	Post scoping *(sub-phases will run in parallel)*
II-a	Post Scoping Pass Testing
II-b	Post scoping log management
II-c	Post scoping samples to complete remainder questions
Phase III	Release process after Phase II has passed
Phase IV	Quarterly BAU post certification

ControlCase
Compliance as a Service

Phase I: Pre-Scoping Pass

- Implementation of appliance
- Customer to upload all scoping questions
- ControlCase will review scoping questions (once all are uploaded) with an SLA of 5 business days.
- ControlCase will provide feedback on portal on scoping questions
- Steps 1 to 4 to be repeated iteratively until scoping passes
- ControlCase will not progress to Phase II until Phase I is completed and scoping passes
- During phase I, you may request QSA time by sending a request with 72-hour notice.

ControlCase
Compliance as a Service

Phase II-a: Post Scoping Pass Testing

- Scoping will be frozen. Any changes to scoping will result in Phase I being repeated.

- All external and internal tests will be scheduled by ControlCase according to PCI DSS requirements. ControlCase will provide available time and date slots one week in advance of testing. These tests will happen in parallel and will be referred to as “Round 1” consolidated testing.

ControlCase
Compliance as a Service

Phase II-a: Post Scoping Pass Testing

- ControlCase will analyze the “Round 1” response for PCI DSS suitability and repeat additional rounds (i.e. steps 2 and 3) until test results are sufficient to pass applicable controls in PCI DSS requirements 1, 3, 6 and 11

- Please note that any additional testing rounds will be performed contingent on remediation of issues identified in “Round 1”.

ControlCase
Compliance as a Service

Phase II-b: Post scoping log management

- Scoping will be frozen. Any changes to scoping will result in Phase I being repeated
- ControlCase will inform customers settings which need to be implemented on respective assets to get correct logs.
  - *If required for non-standard system components, ControlCase can provide template in which the log format is expected for the co-relation engine.*
- Once step #2 is done, ControlCase will ensure all logs are being parsed to meet PCI DSS requirement 10
- ControlCase will not perform any log management activity that does not specifically support the daily reporting requirements of PCI DSS requirement 10.

ControlCase
Compliance as a Service

Phase II-c: Post scoping samples

- Scoping will be frozen. Any change to scoping will result in Phase I being repeated.
- ControlCase Assessors will provide samples to customer
- Customer to upload evidence for all remainder questions with respect to the samples provided.
- As questions are getting uploaded, ControlCase will review evidence and provide comments with an SLA of 10 business days.
- In case of a contractual remediation visit ControlCase team will visit onsite and guide closing any gaps identified.

ControlCase
Compliance as a Service

Phase II-c: Post scoping samples

- ControlCase will provide milestone based timelines which is necessary to meet certification dates.
- ControlCase will visit onsite for final audit.
- As applicable questions pass from phase II-a and II-b they will be updated by ControlCase in the questionnaire.

ControlCase
Compliance as a Service

Phase III – Release Process

- This phase will be invoked only upon passing Phases II-a, II-b and II-c
- ControlCase will release ROC
- ControlCase will release Attestation on Compliance (AOC)
- ControlCase will release Certificate of Compliance (COC)
- ControlCase will schedule lessons learnt call

ControlCase
Compliance as a Service

Phase IV – Q1, Q2 BaU post certification

- ControlCase Asset Management Team will perform quarterly scoping evaluation
- This scope will be used as baseline for all the tests and dependent activities.
- ControlCase will perform security tests as needed to comply with the quarterly passing of evidence for testing requirements 1, 3, 6 and 11, within SLAs
- ControlCase will let customer know the changes required as needed to comply with quarterly passing of evidence for logging requirements 10

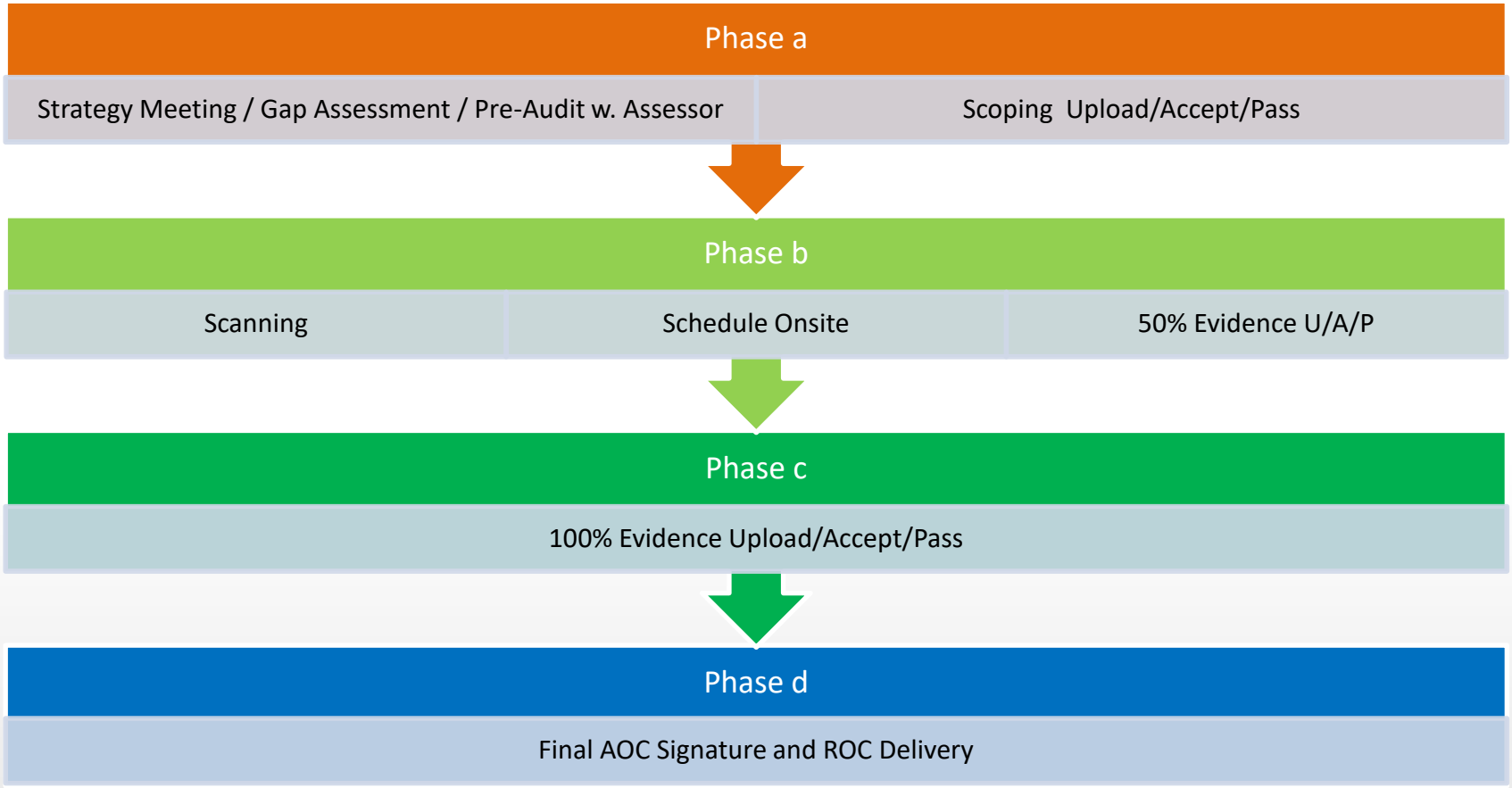
ControlCase
Compliance as a Service

Phase IV – Q3, Q4 BaU post certification

- ControlCase will provide samples to customer
- ControlCase will provide a milestone based timelines which is necessary to meet certification dates.
- Customer to upload evidences for all the remainder questions with respect to samples provided.
- As questions are getting uploaded ControlCase will review evidence and provide comments with an SLA of 10 business days.
- ControlCase will release ROC, AOC & COC and will arrange a lessons learnt call.

ControlCase
Compliance as a Service

Milestones



ControlCase
Compliance as a Service

CaaS Byproducts

Possible to provide as byproduct of CaaS

- Types of deliverables we can provide as they are typically early stage deliverables or by products of the compliance (however no established SLA's for these products)
  - Raw security test results
  - Alerts to IPS/IDS for security use case
  - Daily security log analysis reports
  - Raw logs
- Customers would need to request this through ConnectWise or CSM's (i.e. not a default deliverable)

ControlCase
Compliance as a Service

Cannot deliver as not a byproduct of CaaS

- Types of deliverable we CANNOT provide as it is not a by product of the compliance use case
  - Incident management support
  - Forensic analysis

ControlCase
Compliance as a Service

Thanks

ControlCase
Compliance as a Service