ControlCase
Compliance as a Service

Quality Assurance Overview

Presenter - Satya Rane, ControlCase

Agenda

- Introduction
- How ControlCase QA Works?
- How do we satisfy PCI SSC QA req?
- Quality Assurance Workflow
- Audit by PCI SSC
- How it helps customers?

Responsibility w.r.t Quality Assurance

- PCI SSC
  - Maintains an Assessor Quality Management (AQM) program.
- QSA Companies
  - Stating whether or not the assessed entity has achieved compliance with PCI DSS. PCI SSC does not approve ROCs from a technical perspective, but performs QA reviews on ROCs to ensure that the documentation of testing procedures performed is sufficient to support the results of the PCI DSS Assessment.
- Customers / Clients
  - Providing sufficient documentation to the QSA to support the PCI DSS Assessment.

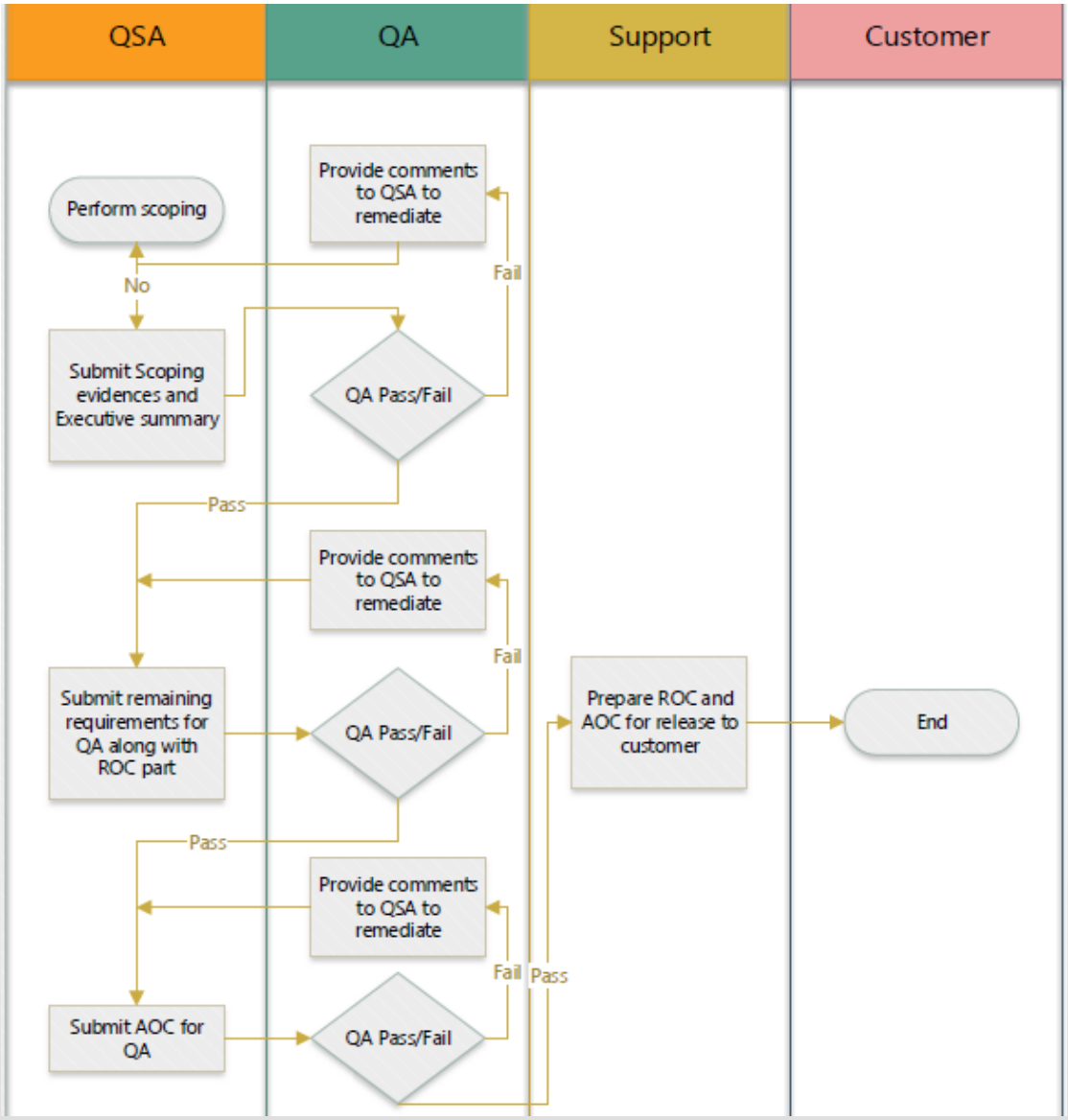
QA and Specific PCI SSC Requirements

- PCI SSC QSA qualification requirement mandates QSA Company to:
  - Have Internal Quality Assurance (QA) Program documented in Quality Assurance Manual
  - Implement Approval and sign-off processes for ROCs and PCI DSS Assessments
  - Require independent quality review of QSA Company and QSA Employee work product
  - Requirements for handling and retention of workpapers and other PCI DSS Assessment Results and Related Materials

How do we satisfy PCI SSC QA req?

- ControlCase has **independent** department for QA
- Qualified personnel (independent of the assessing and/or authoring QSA Employee) conduct a quality assurance review of assessment procedures performed, supporting documentation workpapers
- All work products including ROC, AOC, Test Reports etc. goes through independent QA. This **ensures separation of duty** and **prevent conflict of interest**
- Evidence are automatically backed up and archived on ControlCase IT GRC Platform to retain it for 3 years

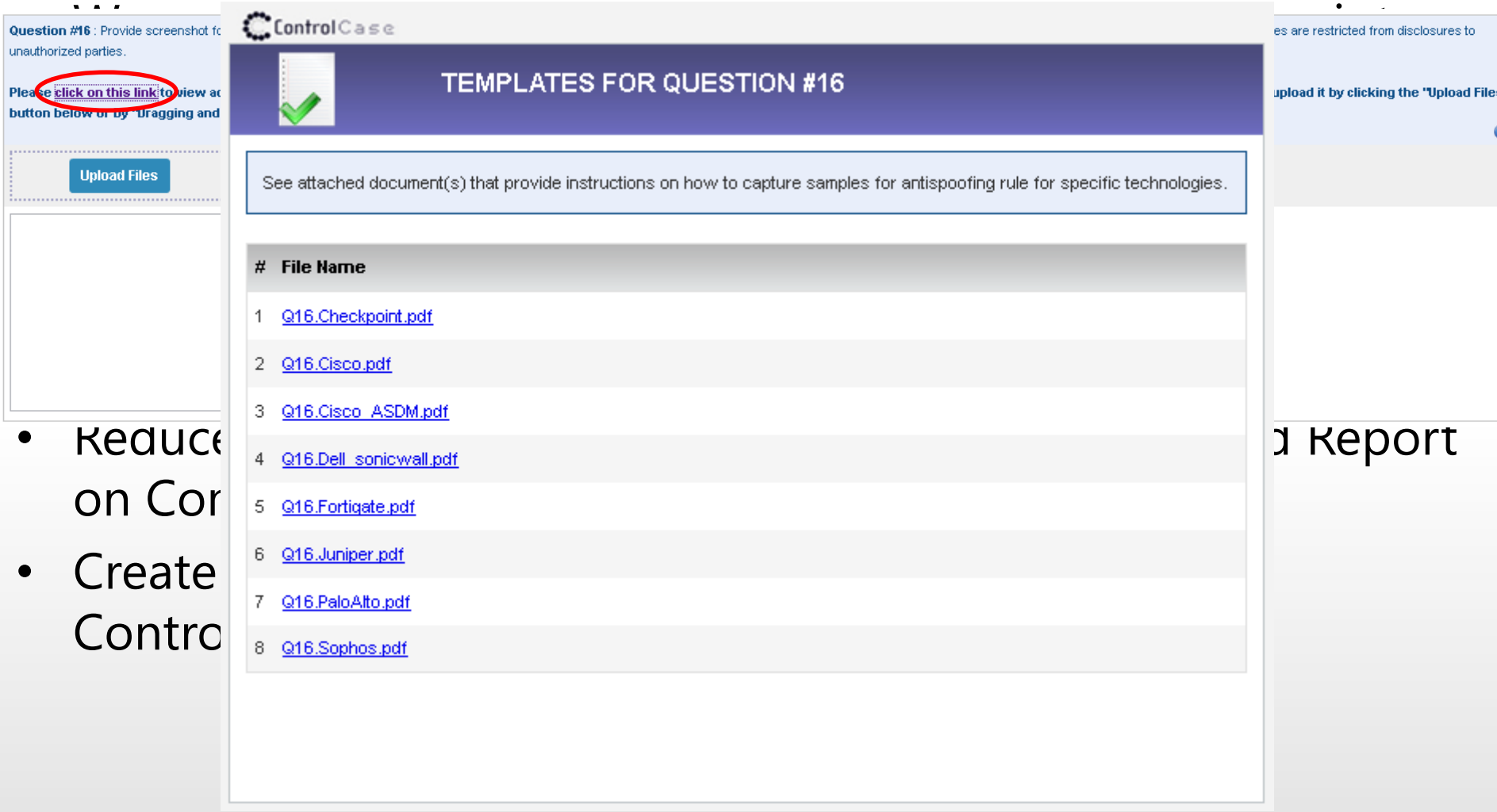
Quality Assurance Workflow



Audit by PCI SSC

- ControlCase is audited by PCI SSC periodically
- Latest review was done in 2017
- PCI SSC has three (3) possible Quality Ratings:
  - **SATISFACTORY**
  - **NEEDS IMPROVEMENT**
  - **UNSATISFACTORY**
- ControlCase achieved highest rating of "**SATISFACTORY**"

How it helps customers?



- Reduce
- on Cor
- Create
- Contro

d Report

Stringent Quality Assurance – Why?

PCI DSS standard is evolving

In-depth review by PCI SSC

No forward looking statements or project plans

Compensating Controls – Above and Beyond existing requirements

Top 5 key findings

1. Changes in scope
2. Inadequate details of third party products in use
3. Compliance checks for vendors and due-diligence
4. Logging and monitoring
5. Inconsistency and incompleteness of Scans and Tests results

Thank you

Satya Rane

Senior Vice President - ControlCase

PCI QSA, PA QSA, P2PE QSA, ASV, CISSP, CEH

✉ srane@controlcase.com

www.controlcase.com