



Certification vision, content and streamlining of PCI certification process



Agenda

- ❖ ControlCase Certification Vision
- ❖ Evidence Collection Approach
- ❖ Evidence Collection Templates
- ❖ Evidence Expiration Process
- ❖ Panel Discussion

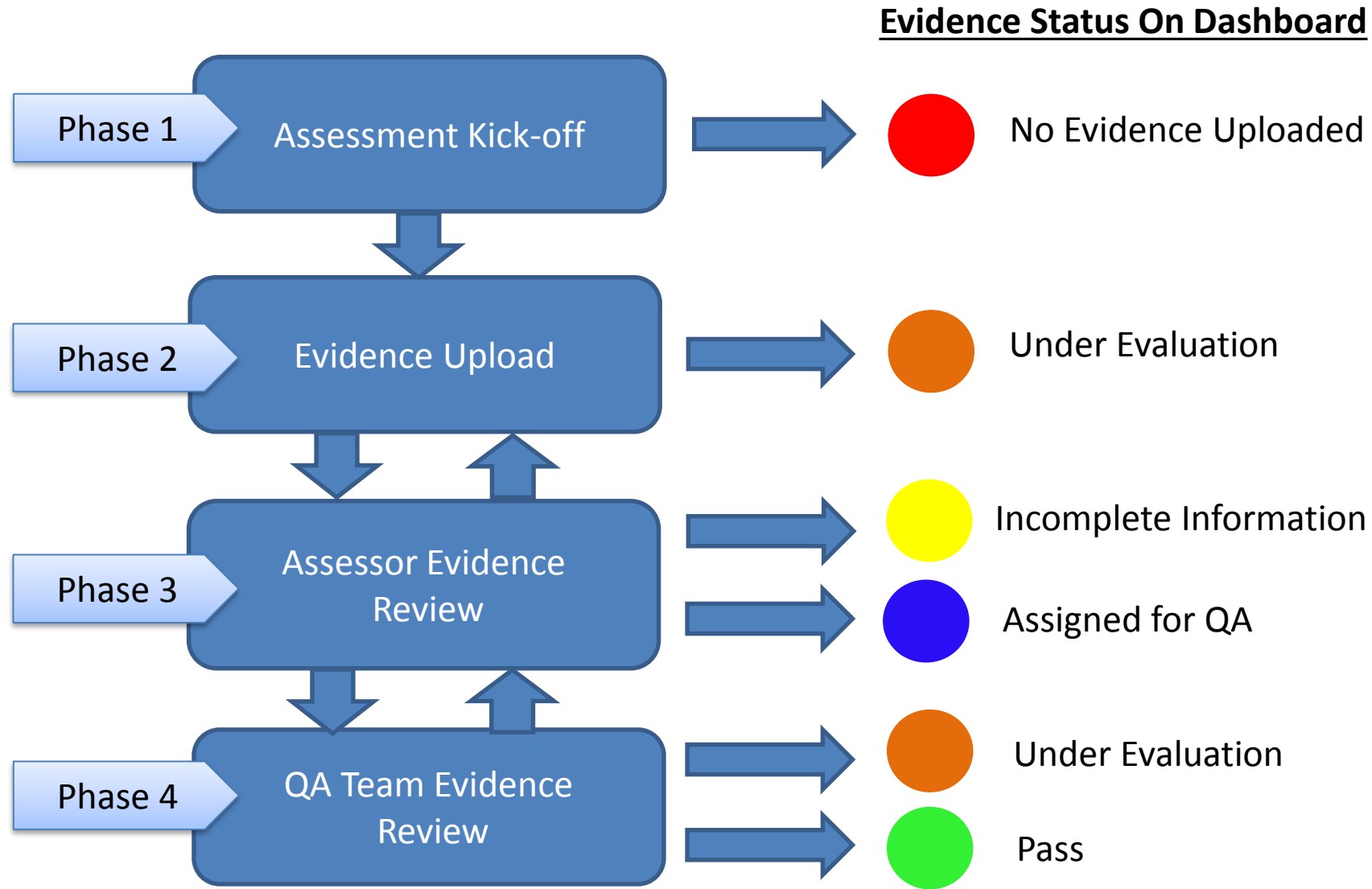
ControlCase Certification Vision

- To ensure PCI certifications are:
 - ❖ Consistent
 - ❖ Repeatable
 - ❖ Accurate
- Automate PCI certification through add-on CaaS.



Evidence Collection Approach

Evidence collection life-cycle



Evidence collection

ControlCase evidence collection process is divided into two parts:

- **Scoping questions:**

- Cover the PCI assessment scoping points including in-scope locations, asset inventory (internal and external facing systems), network diagrams and Data Flow Diagrams
- Scoping questions review helps to confirm the PCI scope and sample set for evidence collection before moving on to controls specific evidence collection
- Avoids unnecessary evidence collection for improperly selected samples at later stage
- Scoping question Quality Assurance (QA) is required to pass before moving on to post scoping questions evidence collection
- PCI ROC Executive Summary review is performed along with scoping question evidence review

Evidence collection

Post-scoping questions

- Covers all the 12 PCI requirement-specific evidences for sample set defined during scoping questions review
- Evidence status is tracked per categories - 'No Evidence Uploaded', 'Under Evaluation', 'Incomplete Information', 'Assigned to QA' & 'Pass'
- Upon passing scoping questions, requirement-specific evidences and ROC goes through QA simultaneously
- Both requirement-specific evidences and ROC are required to pass the QA in order to pass the evidence collection phase

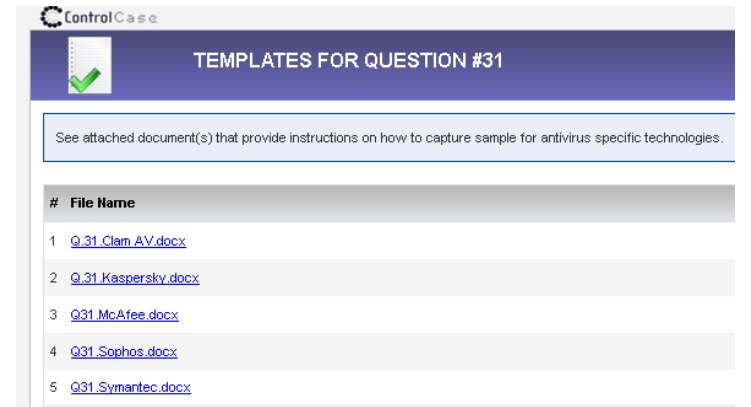


Evidence Collection Templates

Evidence Templates

Simplified Evidence Collection with Evidence Templates

- IT GRC portal with questionnaire and comprehensive set of evidence templates against each question.
- No need to guess about correct screen/evidence to be captured
- Provides good technical guidance for most of the questions

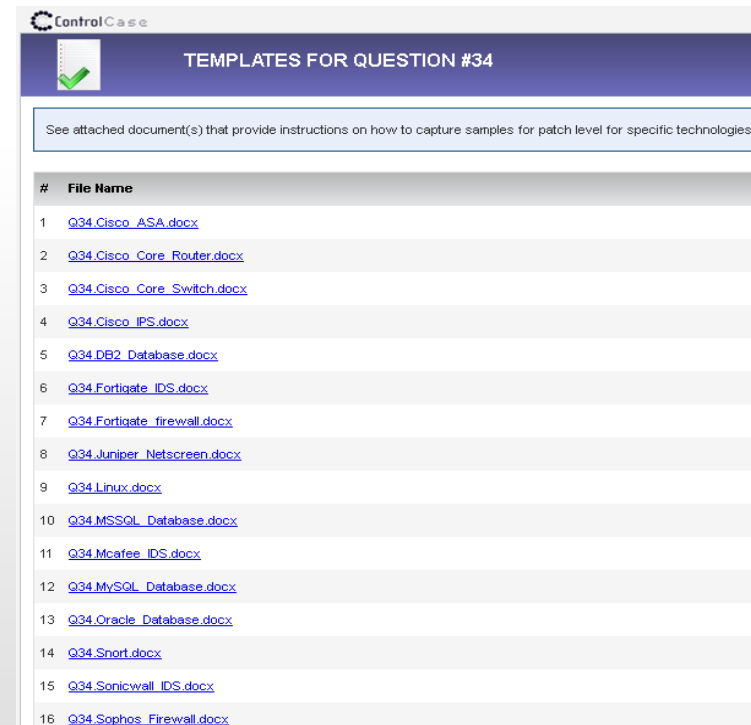


ControlCase

TEMPLATES FOR QUESTION #31

See attached document(s) that provide instructions on how to capture sample for antivirus specific technologies.

#	File Name
1	Q_31_Clam_AV.docx
2	Q_31_Kaspersky.docx
3	Q31_McAfee.docx
4	Q31_Sophos.docx
5	Q31_Symantec.docx



ControlCase

TEMPLATES FOR QUESTION #34

See attached document(s) that provide instructions on how to capture samples for patch level for specific technologies.

#	File Name
1	Q34_Cisco_ASA.docx
2	Q34_Cisco_Core_Router.docx
3	Q34_Cisco_Core_Switch.docx
4	Q34_Cisco_IPS.docx
5	Q34_DB2_Database.docx
6	Q34_Fortigate_IDS.docx
7	Q34_Fortigate_firewall.docx
8	Q34_Juniper_Netscreen.docx
9	Q34_Linux.docx
10	Q34_MSSQL_Database.docx
11	Q34_Mcafee_IDS.docx
12	Q34_MySQL_Database.docx
13	Q34_Oracle_Database.docx
14	Q34_Snort.docx
15	Q34_Sonicwall_IDS.docx
16	Q34_Sophos_Firewall.docx

Evidence Templates (examples)

Juniper:

The screenshot shows the Juniper configuration interface for a NetScreen-ISG 1000. The left sidebar contains a menu with 'Home' highlighted by a red arrow. The main content area displays system status and configuration details:

- Home
- Configuration
- Network
- Security

System Status: Up time: 153 days 18:36:49, System time: 2014-08-10 12:16:01

Hardware Version:	3010(0)
Firmware Version:	6.3.0r13-cu2.0 (Firewall+VPN)
Serial Number:	[REDACTED]
Host Name:	[REDACTED]

Do not hide/crop the menus you used to reach the screens you are going to show in screenshots.

For oracle DB

The screenshot shows the Oracle SQL Developer interface. A query window displays the following SQL statement:

```
select * from v$version
```

The Data Grid below shows the results of the query:

BANNER
Oracle9i Enterprise Edition Release 9.2.0.8.0 - 64bit Production
PL/SQL Release 9.2.0.8.0 - Production
CORE 9.2.0.8.0 Production
TNS for HP/UX: Version 9.2.0.8.0 - Production
NLSRTL Version 9.2.0.8.0 - Production

Do not hide/crop the menus you used to reach the screens you are going to show in screenshots.



Evidence Expiration

Evidence Expiration

Evidence Expiration:

- Is to support Business-As-Usual process
- To ensure continuous monitoring of security controls and periodic reviews
- Provides Compliance Dashboard to customers showing which evidences are still fresh or current and which are about to expire based on defined frequency
- Allows customers to view current evidence status and evidences due at any point of time

Evidence Expiration

Evidence Expiration process:

The Evidence Expiring applies only for the question(s) with "Pass" status as part of previous completed certification.

- Expiring evidence changes the relevant question status from "Pass" to "Incomplete Information"
- Expiring evidence question shows up in "Customer Action Required" section under Compliance Dashboard
- Only Expiring evidence shows up in "Upload Evidence Link"

Customer Action Required

ControlCase **MENU**

DASHBOARD Get quick overview of the current status using graphs; view currently assigned Remediation Tickets and Assessments.

Welcome to Controlcase GRC

PCI DSS Compliance Dashboard

Compliance Dashboard | Project / Task / Milestone | Support Ticket | **Customer Action Required 25**

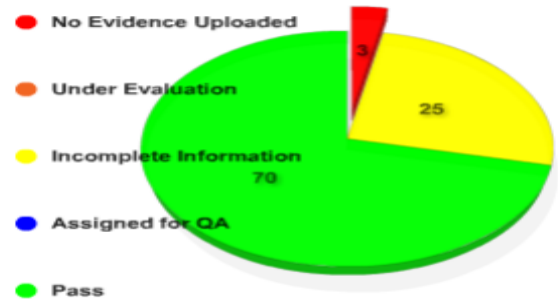
Your process start date is 2016-03-31 and process end date is 2017-03-31

Your Last ROC Compliance Date is 2016-04-05

Your QSA is cthakur

PCI DSS Compliance Activity Status

Review [redacted] _PCIDSS_3_2_Evidence Review



Evidence(s) Due

PCI DSS Compliance Dashboard

Compliance Dashboard | Project / Task / Milestone | Support Ticket | **Customer Action Required**

Evidence(s) Due

#	Question	Ready for Evidence Upload	ROC Date	Additional Detail
52	Question No: 53 Provide documented procedures for password change during new user creation or for a password reset for all platforms in scope. The attached template is provided as a sample.	2016-07-05 for month : 3	2016-04-05	It seems evidences provided for this question are incomplete or about to expire soon, please consider uploading the evidences again by clicking on "Upload Evidence" link from Important link section.
53	Question No: 54 Provide the following related to remote access, - Procedure that outlines the process of granting remote access as well as the description of the two-factor authentication technology used- List of internal and external users with remote accessThe attached template is provided as a sample.	2016-07-05 for month : 3	2016-04-05	It seems evidences provided for this question are incomplete or about to expire soon, please consider uploading the evidences again by clicking on "Upload Evidence" link from Important link section.
54	Question No: 55 This is applicable only to service providers with remote access to multiple customers. Provide user list for up to (but not exceeding) 3 customers to prove unique credentials are being used per customer. The attached template is provided as a sample.	2016-07-05 for month : 3	2016-04-05	It seems evidences provided for this question are incomplete or about to expire soon, please consider uploading the evidences again by clicking on "Upload Evidence" link from Important link section.
55	Question No: 56 If other authentication mechanisms are used apart from normal passwords (for example, physical or logical security tokens, smart cards, certificates, etc.) then provide the list of users and that the authentication method assigned to an individual account.The attached template is provided as a sample.	2016-07-05 for month : 3	2016-04-05	It seems evidences provided for this question are incomplete or about to expire soon, please consider uploading the evidences again by clicking on "Upload Evidence" link from Important link section.

PCI DSS Compliance Dashboard

Compliance Dashboard | Project / Task / Milestone | Support Ticket | **Customer Action Required**

Evidence(s) Due

#	Question	Ready for Evidence Upload	ROC Date	Additional Detail
1	Question No: 2 Provide a list of applications that are involved in storing, processing or transmitting information covered under this certification. You must use the attached template to provide us the data.	2016-12-05 for month : 8	2016-04-05	It seems evidences provided for this question are incomplete or about to expire soon, please consider uploading the evidences again by clicking on "Upload Evidence" link from Important link section.
2	Question No: 3 Provide a high level network diagram for in-scope environment (See attached templates). You may use the attached template or provide the required information in an alternative format.	2016-12-05 for month : 8	2016-04-05	It seems evidences provided for this question are incomplete or about to expire soon, please consider uploading the evidences again by clicking on "Upload Evidence" link from Important link section.
3	Question No: 4 Provide your asset list, databases, data storage locations, and other related data elements. You must use the attached template to provide us the data.	2016-09-05 for month : 5	2016-04-05	It seems evidences provided for this question are incomplete or about to expire soon, please consider uploading the evidences again by clicking on "Upload Evidence" link from Important link section.
4	Question No: 5 Provide a list of all your external IP addresses and their function. You must use the attached template to provide us the data.	2016-09-05 for month : 5	2016-04-05	It seems evidences provided for this question are incomplete or about to expire soon, please consider uploading the evidences again by clicking on "Upload Evidence" link from Important link section.
5	Question No: 6 Provide 3 sample firewall and router change forms or tickets. You may use the attached template or provide the required information in an alternative format.	2016-09-05 for month : 5	2016-04-05	It seems evidences provided for this question are incomplete or about to expire soon, please consider uploading the evidences again by clicking on "Upload Evidence" link from Important link section.
	Question No: 7			

Evidence Expiration Process

- Customer uploaded evidence(s) reflect in daily Evidence Collection criticality report. [i.e., Under Evaluation criticality report]
- Regular review is performed and status is changed to either "Pass" or "Incomplete Information".
- Evidence status which is changed to "Pass" remains the same until the next defined evidence due date for resubmission.
- All the evidences expiration configured as per quarterly, semi-annual and annual frequency.



Thank You !