ControlCase
Compliance as a Service

Welcome
ControlCase Conference

Kishor Vaswani, CEO

ControlCase Annual Conference – Miami, Florida USA 2017

Agenda

- **About ControlCase**
- **Key updates since last conference**
  - Certification methodology and support for new regulations
  - Constant Compliance offering introduced
- **ControlCase Offerings, Updates and Vision**
  - Audit & Certification
  - Constant Compliance
  - Compliance as a Service (CaaS)
  - Data Discovery
- **Questions & Answers**

ControlCase
Compliance as a Service

About ControlCase

ControlCase Corporate OverView

Products/Services include ‘Certifications’, ‘Compliance as Usual (CaU)’, ‘Compliance as a Service (CaaS)’ and ‘Data Discovery’

Support PCI DSS, PA-DSS, PCI P2PE, GDPR, SOC1, SOC2, ISO 27001, MS SSPA, HITRUST, HIPAA, NIST 800-53 and EI3PA

Over 500 clients IN 50 COUNTRIES across US, CEMEA, Europe and Asia/Pacific regions

Headquartered out of Fairfax, VA – USA

Offices & Personnel in Canada, Columbia, India, UK, Belgium, Indonesia, Philippines and Dubai

ControlCase
Compliance as a Service

ControlCase Vision, Mission and Values

Our Vision

- To make IT compliance easy

Our Mission

- To automate IT certification and audit
- To deliver peace of mind through visibility

Our Values

- Caring
- Team approach
- Problem solving
- Ethical behavior
- Value-oriented
- Empowering employees to be successful

ControlCase
Compliance as a Service

Credentials

PCI DSS

Qualified Security Assessor (QSA) Company

ISO 27001 & 27002

International Organization for Standardization

SOC 1, SOC 2 & SOC 3

Service Organization Controls (AICPA)

HITRUST CSF

Health Information Trust Alliance Common Security Framework (CSF)

HIPAA

Health Insurance Portability and Accountability Act

PCI P2PE

Point to Point Encryption

Privacy Shield

EU-U.S. and Swiss-U.S. Privacy Shield Frameworks

NIST 800-53

National Institute of Standards and Technology

EI3PA

Experian Independent Third Party Assessment

PCI PA-DSS

Payment Application Qualified Security Assessor (QSA)

Third Party Risk Assessor

Shared Assessments Program Certified product licensee for SIG and AUP

Microsoft SSPA

Supplier Security and Privacy Assurance

ControlCase
Compliance as a Service

Key Differentiators

Focused Exclusively on IT Compliance and IT Certification

Employee Experience

Investment in Technology

- GRC Platform – simplifies compliance management
- Streamlined Evidence/Document Collection
- PCI DSS compliance becomes Compliance as Usual

Customer Success Management Team

Formalized and Consistent Methodology

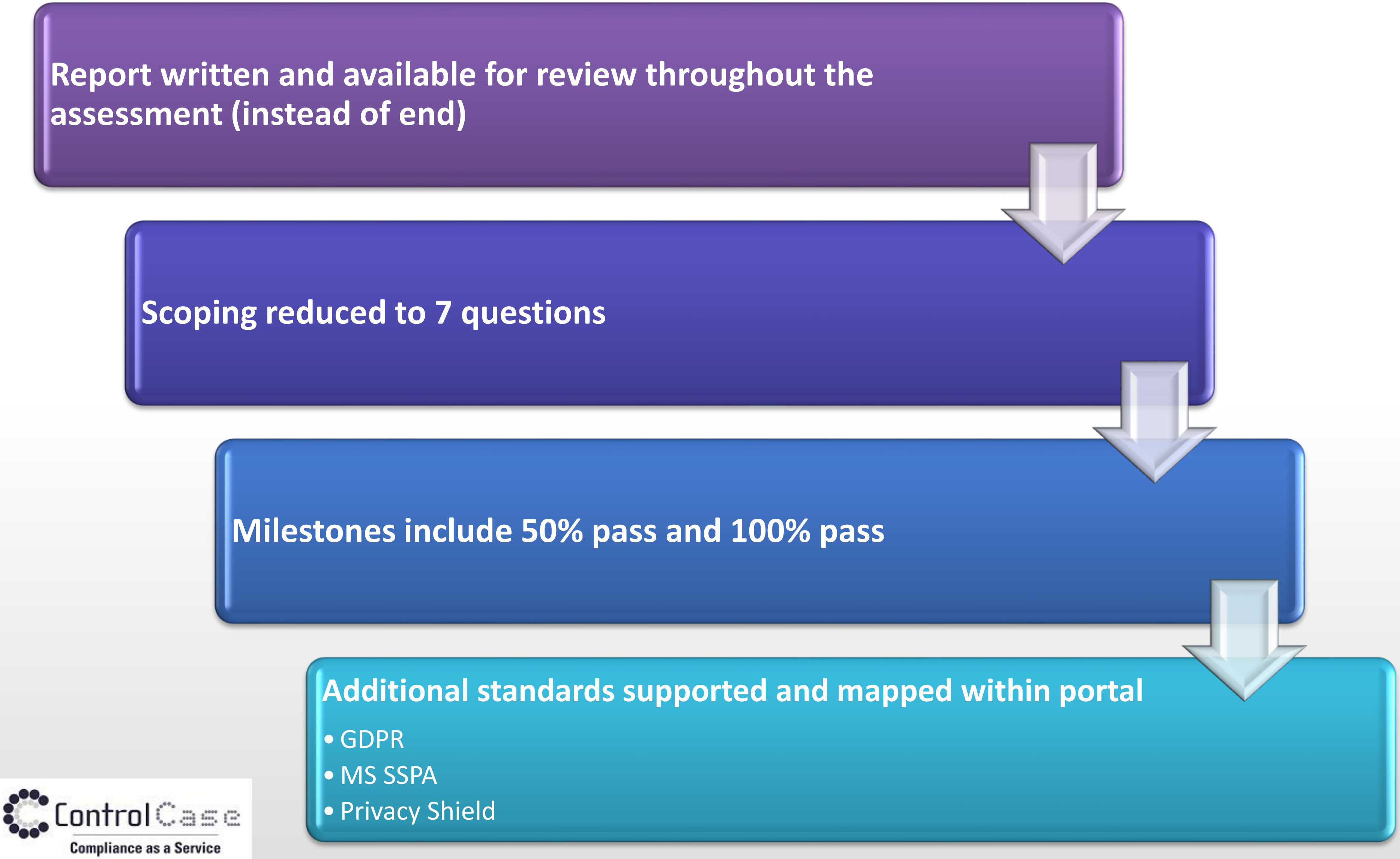
Compliance as a Service (CaaS) offering

Constant Compliance offering

ControlCase
Compliance as a Service

Key Updates

Certification Methodology Updates



Report written and available for review throughout the assessment (instead of end)

Scoping reduced to 7 questions

Milestones include 50% pass and 100% pass

Additional standards supported and mapped within portal

- GDPR
- MS SSPA
- Privacy Shield

ControlCase
Compliance as a Service

Constant Compliance offering announcement

- Establishes responsibility of monitoring and alerting on IT compliance throughout the year to ControlCase by means of,
  - Timely escalation letters
  - Alerting
  - QSA/CSM/Security Tester/Asset Manager interaction

- ControlCase’ s Business as Usual (BAU) product for IT Certification

ControlCase
Compliance as a Service

Audit and Certifications

Certifications

□ PCI DSS

□ ISO 27001

□ PCI ASV

□ PA DSS

□ EI3PA

□ SOC1

□ SOC2

□ SOC3

□ HITRUST

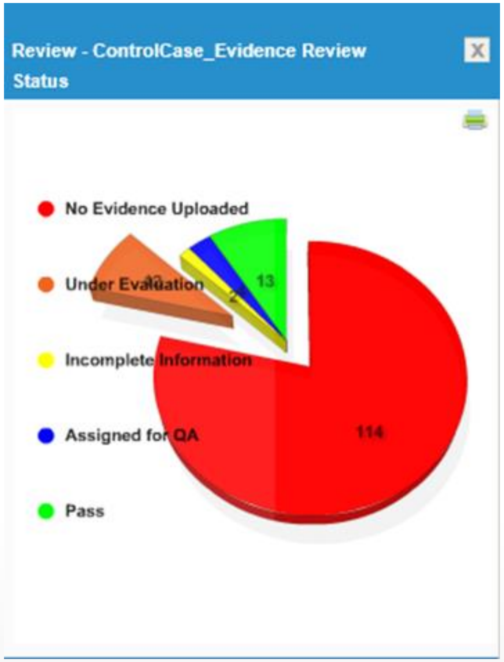
Audits

□ GDPR

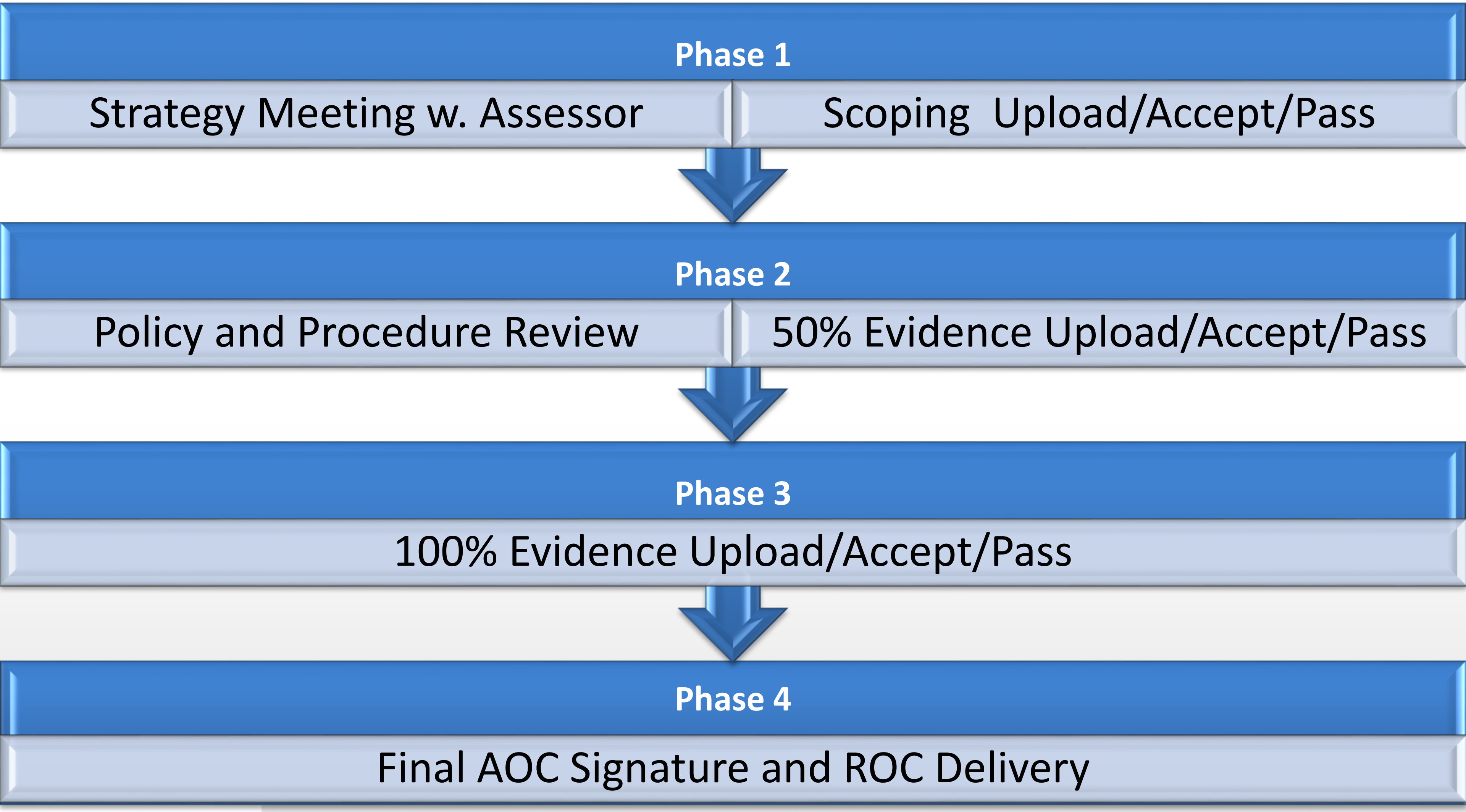
□ NIST 800-53

□ HIPAA

□ SOX



Audit Methodology



Phase 1

Strategy Meeting w. Assessor

Scoping Upload/Accept/Pass

Phase 2

Policy and Procedure Review

50% Evidence Upload/Accept/Pass

Phase 3

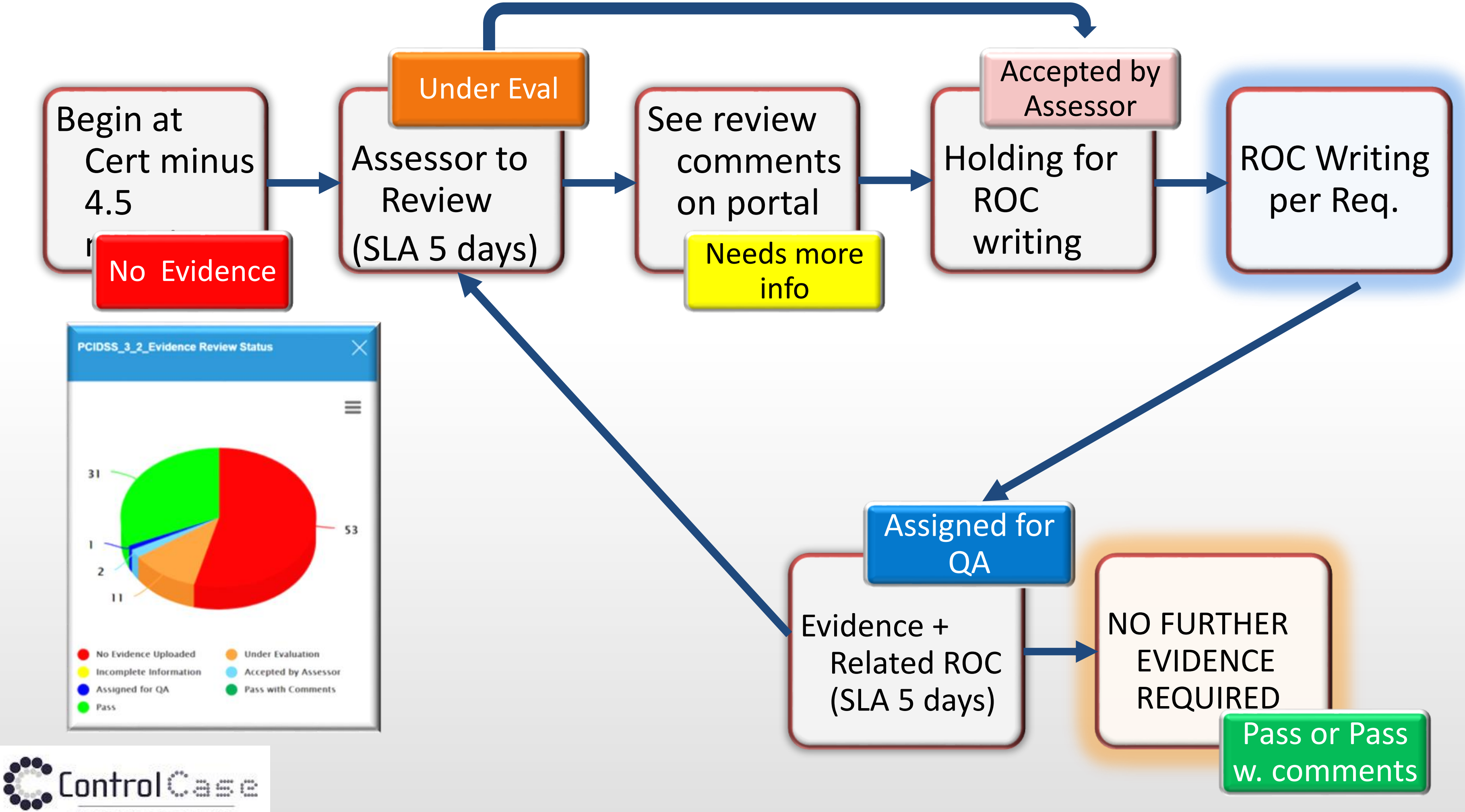
100% Evidence Upload/Accept/Pass

Phase 4

Final AOC Signature and ROC Delivery

Evidence Review: How to Pass Evidence

Go from No Evidence (Red) to Passing (Green) . . .



Constant Compliance

Component in Constant Compliance	PCI Requirement Met
Centralized compliance management portal and reminders	To support BaU requirements
Automate evidence collection against evidence collection list	To support automated evidence collection
Firewall rule-set analysis	1
Configuration scan analysis	2
Cardholder data analysis	3
Secure coding developer coverage analysis	6
Application scan results analysis	6
Log analysis	10
File integrity monitoring analysis	10
Internal vulnerability scan analysis	11
External vulnerability scan analysis	11
Internal penetration test analysis	11
External penetration test analysis	11
Application penetration test analysis	11
Policy analysis	12
Annual security awareness training coverage analysis	12
Ongoing risk assessment	12
Third party management/Vendor management analysis	12

ControlCase
Compliance as a Service

Value of Constant Compliance

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

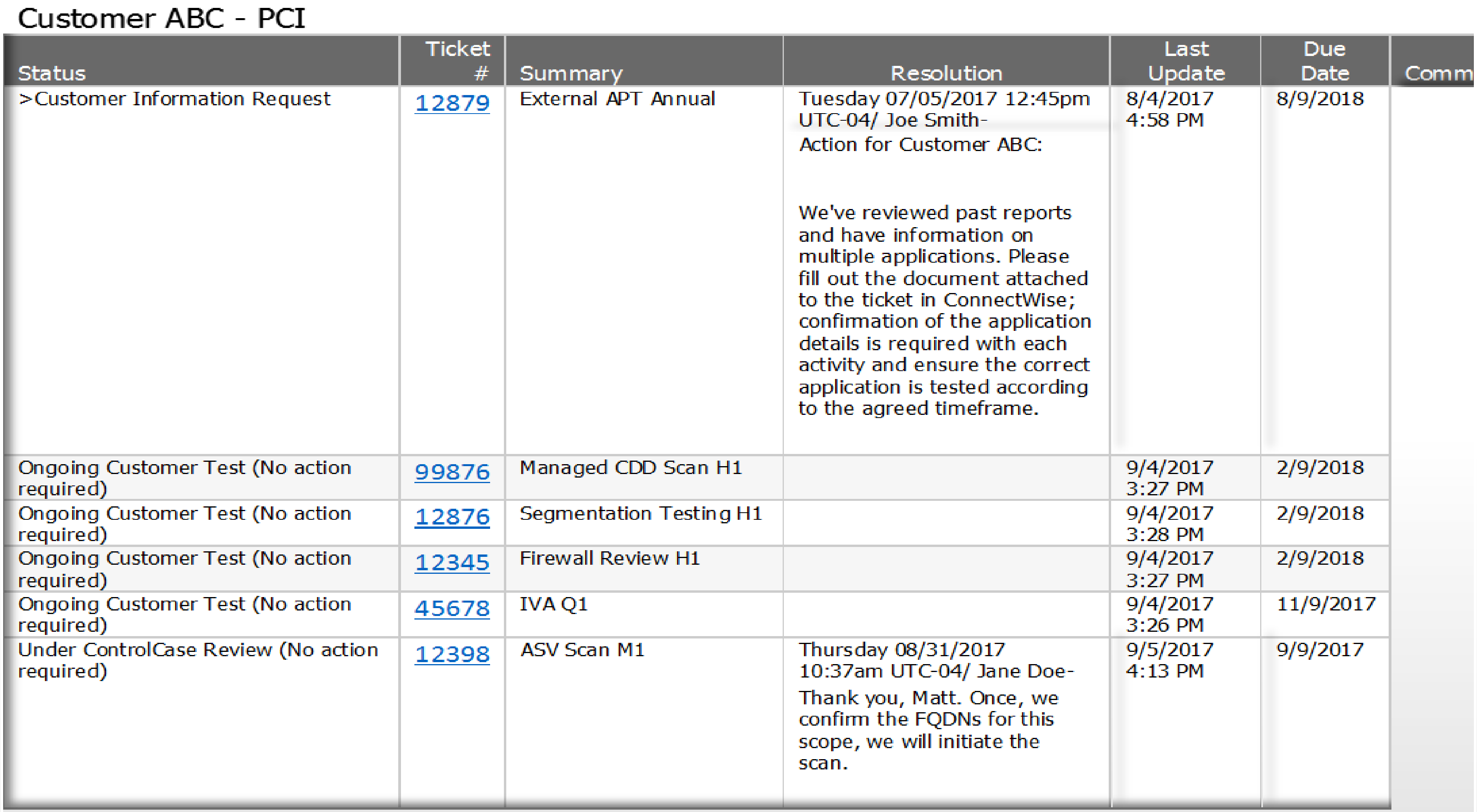
- We know your compliance scope
- We know what will result in non certification
- We map the risks of vulnerabilities, sensitive data and log alerts to compliance
- We map all logs to the relevance compliance requirements such as daily reports

ControlCase will take ownership of this and deliver within established SLA’s

Communication through ConnectWise email

ControlCase
Compliance as a Service

Deliverable – Sample Monthly/Quaterly Report



Customer ABC - PCI

Status	Ticket #	Summary	Resolution	Last Update	Due Date	Comm
>Customer Information Request	12879	External APT Annual	Tuesday 07/05/2017 12:45pm UTC-04/ Joe Smith- Action for Customer ABC: We've reviewed past reports and have information on multiple applications. Please fill out the document attached to the ticket in ConnectWise; confirmation of the application details is required with each activity and ensure the correct application is tested according to the agreed timeframe.	8/4/2017 4:58 PM	8/9/2018	
Ongoing Customer Test (No action required)	99876	Managed CDD Scan H1		9/4/2017 3:27 PM	2/9/2018	
Ongoing Customer Test (No action required)	12876	Segmentation Testing H1		9/4/2017 3:28 PM	2/9/2018	
Ongoing Customer Test (No action required)	12345	Firewall Review H1		9/4/2017 3:27 PM	2/9/2018	
Ongoing Customer Test (No action required)	45678	IVA Q1		9/4/2017 3:26 PM	11/9/2017	
Under ControlCase Review (No action required)	12398	ASV Scan M1	Thursday 08/31/2017 10:37am UTC-04/ Jane Doe- Thank you, Matt. Once, we confirm the FQDNs for this scope, we will initiate the scan.	9/5/2017 4:13 PM	9/9/2017	

Quarterly Architecture and Flows

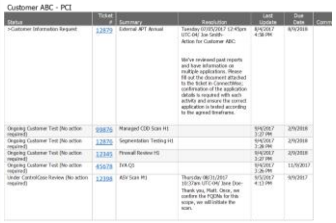
Customer Operations

- Raw vulnerability scan results
- Raw logs from SIEM
- List of assets in scope
- Any M&A activity
- Any scope change activity
- New systems/Asset list

ControlCase CaU Operations

- Asset verification
- Vulnerability mapping
- Log mapping
- Data Analytics
- Compliance intelligence
- False positive management
- QA of results
- Quarterly report generation

Monthly/Quarterly Non Compliance



Customer ABC - PCI

Status	Ticket #	Summary	Resolution	Last Update	Due Date	Comm
>Customer Information Request	12879	External APT Annual	Tuesday 07/05/2017 12:45pm UTC-04/ Joe Smith- Action for Customer ABC: We've reviewed past reports and have information on multiple applications. Please fill out the document attached to the ticket in ConnectWise; confirmation of the application details is required with each activity and ensure the correct application is tested according to the agreed timeframe.	8/4/2017 4:58 PM	8/9/2018	
Ongoing Customer Test (No action required)	99876	Managed CDD Scan H1		9/4/2017 3:27 PM	2/9/2018	
Ongoing Customer Test (No action required)	12876	Segmentation Testing H1		9/4/2017 3:28 PM	2/9/2018	
Ongoing Customer Test (No action required)	12345	Firewall Review H1		9/4/2017 3:27 PM	2/9/2018	
Ongoing Customer Test (No action required)	45678	IVA Q3		9/4/2017 3:26 PM	11/9/2017	
Under ControlCase Review (No action required)	12398	ASV Scan H1	Thursday 08/31/2017 10:37am UTC-04/ Jane Doe- Thank you, Matt. Once, we confirm the FQDNs for this scope, we will initiate the scan.	9/5/2017 4:13 PM	9/9/2017	

- Missing assets
- Assets not covered in scans
- Assets not covered in logs
- Logs not having right data
- Confirmed issues

ControlCase
Compliance as a Service

Compliance as a Service (CaaS)

Component	Requirement Met
Gap Analysis (As needed)	Certification
Remediation Support	Certification
Certification (ROC/SAQ)	Certification
Centralized compliance management portal and reminders	To support BAU requirements
Automate evidence collection against evidence collection list	To support automated evidence collection
Firewall rule-set analysis	1
Configuration scanning	2
Searching of cardholder data within environment	3
Secure coding developer training	6
Application security scanning	6
Logging platform	10
File integrity monitoring platform	10
Review of logs and alerts to meet PCI DSS requirements	10
Secure storage and archival of parsed logs	10
Internal vulnerability scanning	11
External vulnerability scanning (ASV approved scan)	11
Internal penetration testing	11
External penetration testing	11
Application penetration testing	11
Policy manager	12
Customization and updating of policies to meet PCI requirements	12
Distribution and attestation of annual security awareness training	12
Annual Risk Assessment	12
Third party management/Vendor management	12

ControlCase
Compliance as a Service

Quarter based process

- The CaaS offering following three part stage for every quarter:

Quarters	Scoping	CaaS-Tech	Risk Assessment
Quarter I	√	√	√
Quarter II	√	√	√
Quarter III	√	√	√
Quarter IV	Cert cycle (Scoping confirmed)	√	√

ControlCase

Compliance as a Service

What is Compliance as a Service (CaaS)

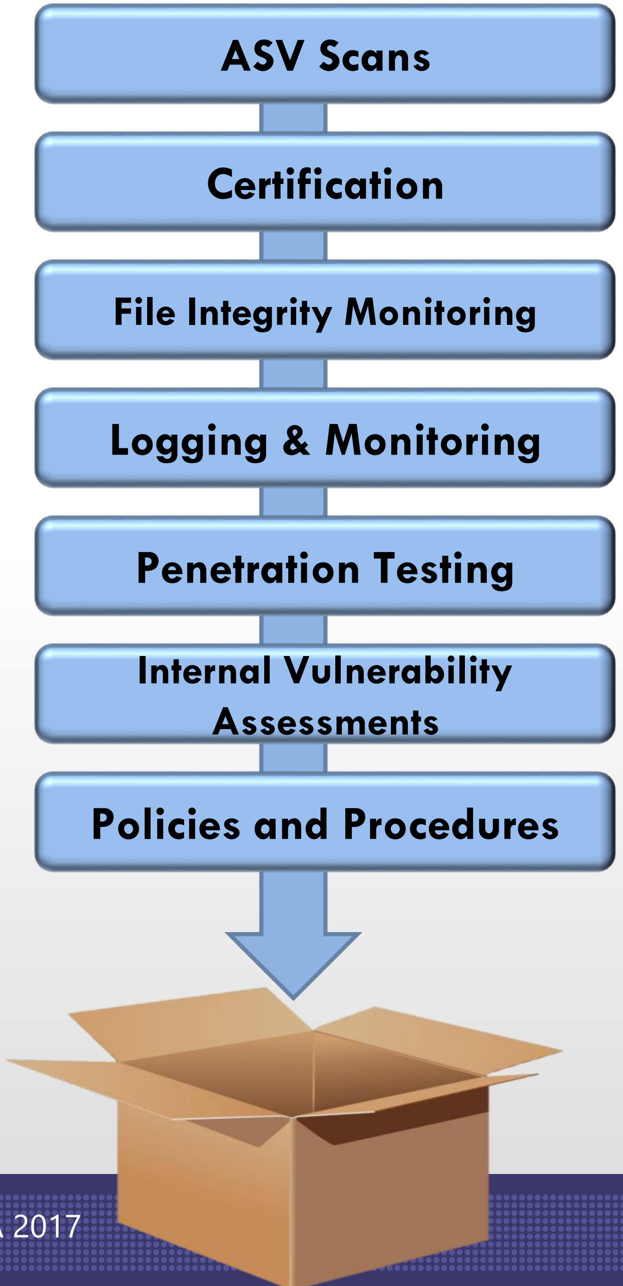
ControlCase IT GRC Software
- ControlCase Compliance Manager
-ControlCase Audit Manager
-ControlCase Vendor Manager
-ControlCase Asset and Vulnerability Manager

Data Discovery Software
- ControlCase Compliance Scanner (Card data search, Privacy data search etc)

Compliance as a Service (CaaS)

Certification Services
- PCI DSS Certification
- PA DSS Certification
- ASV Certification
- EI3PA
- ISO 27002
- CERT-IN

Managed Security Services
- External / Internal VA / PT
-Application Security Reviews
-Firewall Reviews
-Security Audits
-Assessments Customization
- 24X7 Logging and Monitoring



ASV Scans

Certification

File Integrity Monitoring

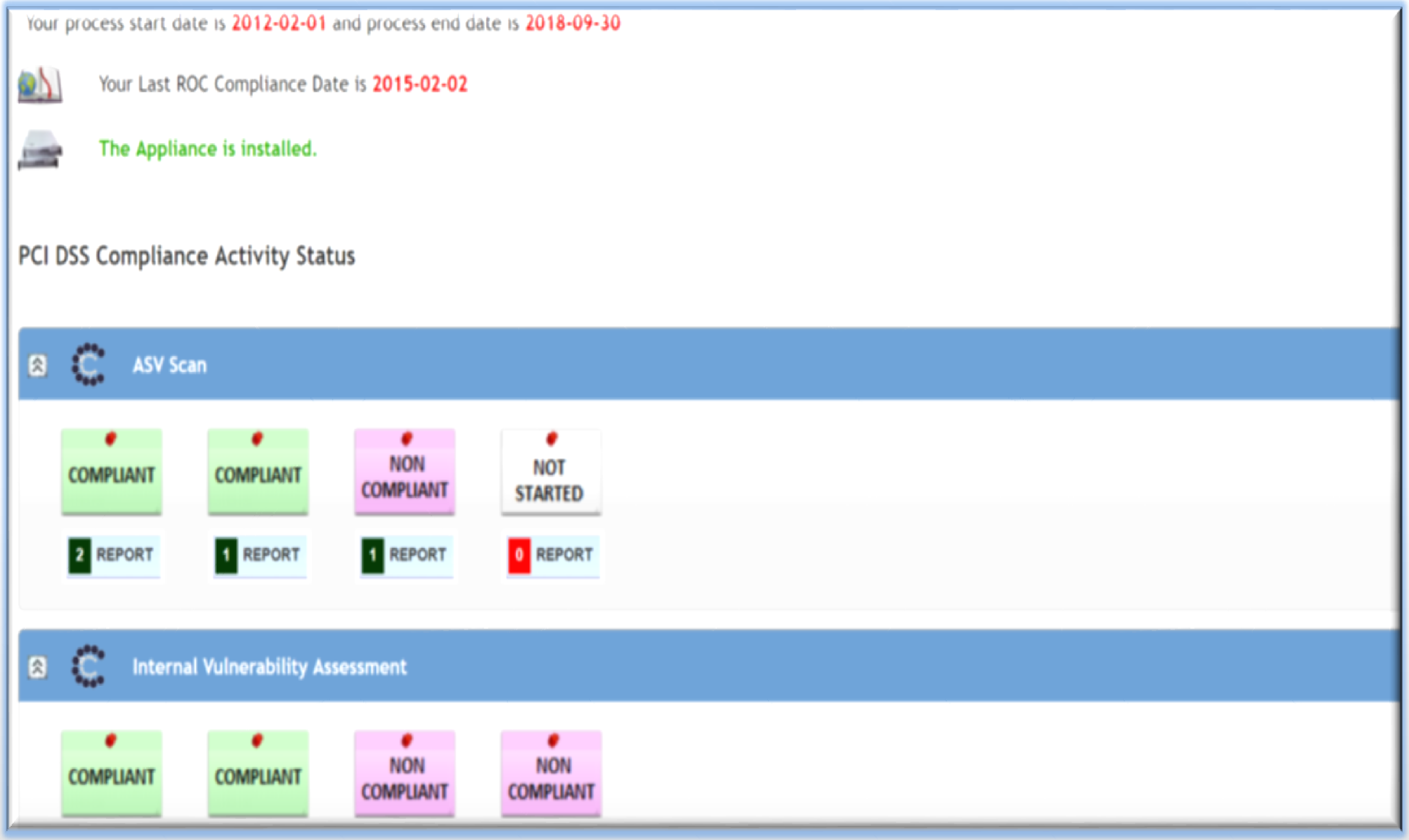
Logging & Monitoring

Penetration Testing

Internal Vulnerability Assessments

Policies and Procedures

CaaS Ongoing Tracking



Your process start date is 2012-02-01 and process end date is 2018-09-30

Your Last ROC Compliance Date is 2015-02-02

The Appliance is installed.

PCI DSS Compliance Activity Status

ASV Scan

COMPLIANT	COMPLIANT	NON COMPLIANT	NOT STARTED
2 REPORT	1 REPORT	1 REPORT	0 REPORT

Internal Vulnerability Assessment

COMPLIANT	COMPLIANT	NON COMPLIANT	NON COMPLIANT

CaaS Architecture

Current Assets

- If File Integrity Monitoring (FIM) is required agents would need to be installed on assets at store
- If data discovery needs to be done credentials for target platforms would need to be implemented
- If the appliance has been configured in a VPN mode, then logs can be directly sent to ControlCase SOC
- Store should have the capability to provide logs

Appliance

- Appliance includes GRC, Data Discovery and log/FIM collector
- The sensor/collector can collects and compresses logs coming in from the various agents
- The logs are finally transported securely to our SIEM console in our Security Operations Center (SOC)
- Virtual appliances are also available

ControlCase SOC

- The SIEM console gathers all the logs, correlates them and identifies threats and anomalies as required by the PCI DSS
- SOC personnel monitor for logs 24X7X365
- SOC personnel run security scans and monitor for vulnerabilities

ControlCase SaaS

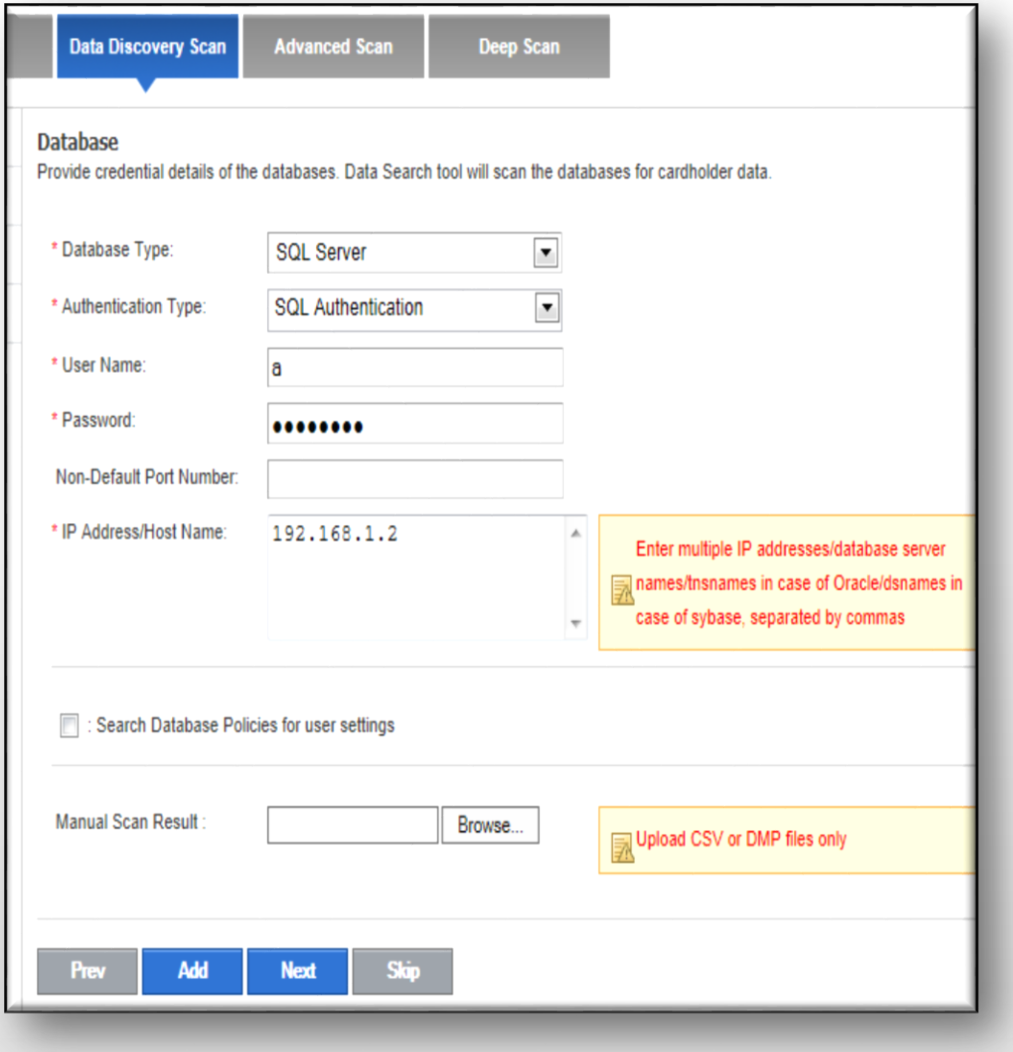
- GRC Management console includes SAQ management, dashboard of status at store, policy management, vendor management, vulnerability management and incident/ticket management
- Security Information and Event Management Console (SIEM) includes logging and FIM alerts

Data Discovery Software/Service

- □ Discover sensitive data such as SSN, GDPR Data, Card Numbers easily
- □ Available as software
- □ Available as managed service that continuously looks for unencrypted data in logs

Return On Investment

- □ Automates finding Numbers
- □ Managed Service and/or Sunknown sensitive data such as SSN and Card oftware
- □ Even if it prevents one breach, it has an ROI of 100X



Database

Provide credential details of the databases. Data Search tool will scan the databases for cardholder data.

* Database Type: SQL Server
* Authentication Type: SQL Authentication
* User Name: a
* Password: ●●●●●●●●●
Non-Default Port Number:
* IP Address/Host Name: 192.168.1.2

Enter multiple IP addresses/database server names/tnsnames in case of Oracle/dsnames in case of sybase, separated by commas

□ : Search Database Policies for user settings

Manual Scan Result :

Upload CSV or DMP files only

ControlCase
Compliance as a Service

Thank You

ControlCase
Compliance as a Service