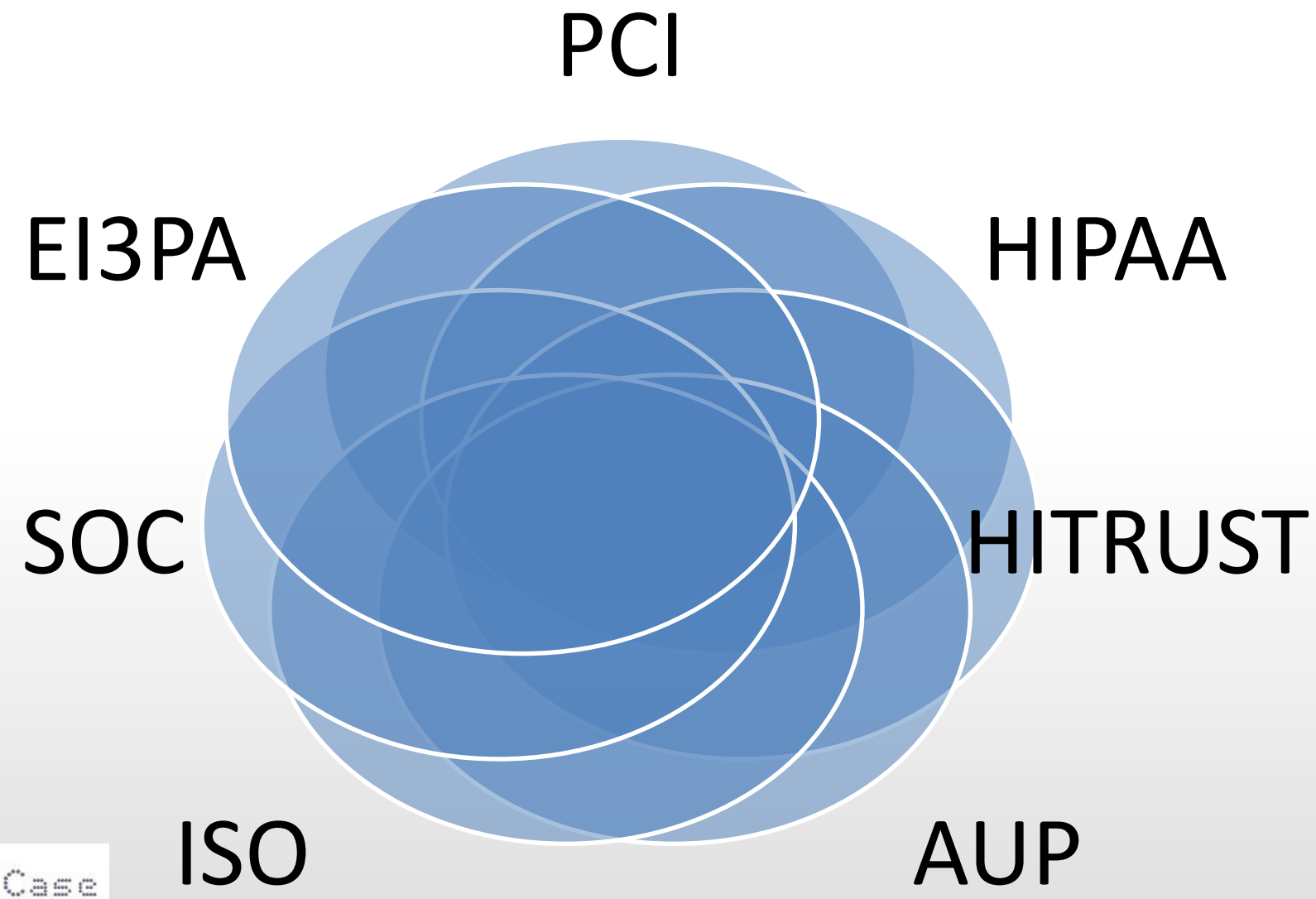
ControlCase
Compliance as a Service

Challenges and solutions toward multiple certifications

Multiple Certifications



ControlCase
Compliance as a Service

Panelist Questions

1. What are some of the biggest challenges you face with multiple certifications? Can you share specific examples of what you experienced, and the results?

ControlCase
Compliance as a Service

Panelist questions

2. What are some tactics you have used? Which worked? Which didn't? Why? Can you share specific examples of what you tried, and the results?

- What processes/procedures have proven helpful?
- What kind of tools were helpful?

ControlCase
Compliance as a Service

Panelist Questions

3. How does your organization provide support to contributing teams for ongoing compliance activities? What value does your compliance program, or compliance in general bring to contributing parties?

ControlCase
Compliance as a Service

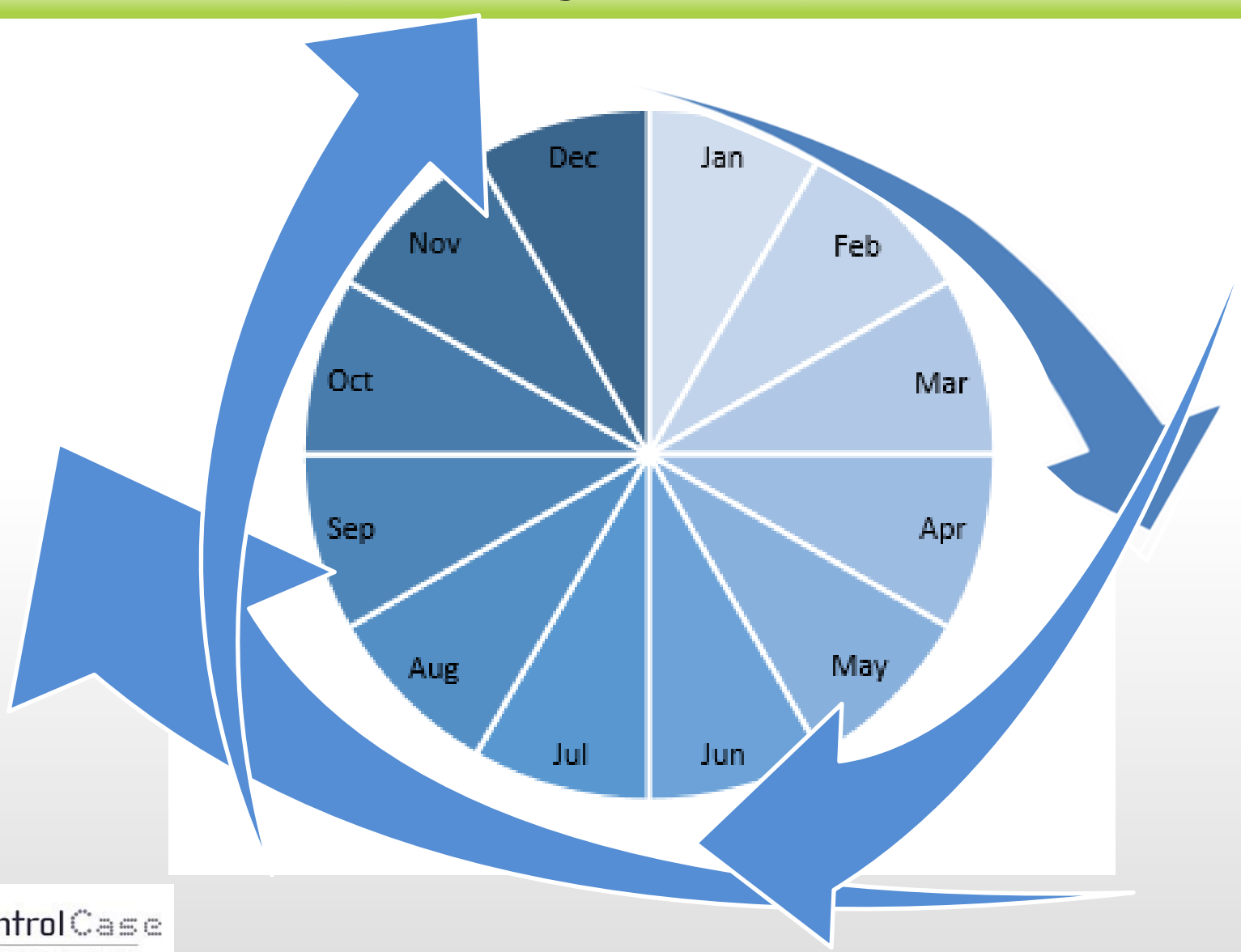
Summary of Challenges

Summary of Challenges

- Cost of Multiple Contracts
  - Cost for each audit company hired
  - Admin process replicated for each contract
- Repetitive evidence requests cause disengagement
- Multiple Areas of Scope
- Multiple Certification Dates
- Status reporting is complex
- Time . . .

ControlCase
Compliance as a Service

. . .Time: It's *Always* Audit Season



ControlCase
Compliance as a Service

ControlCase Solutions

Single Combined Certification Process

Collect evidence once . . .

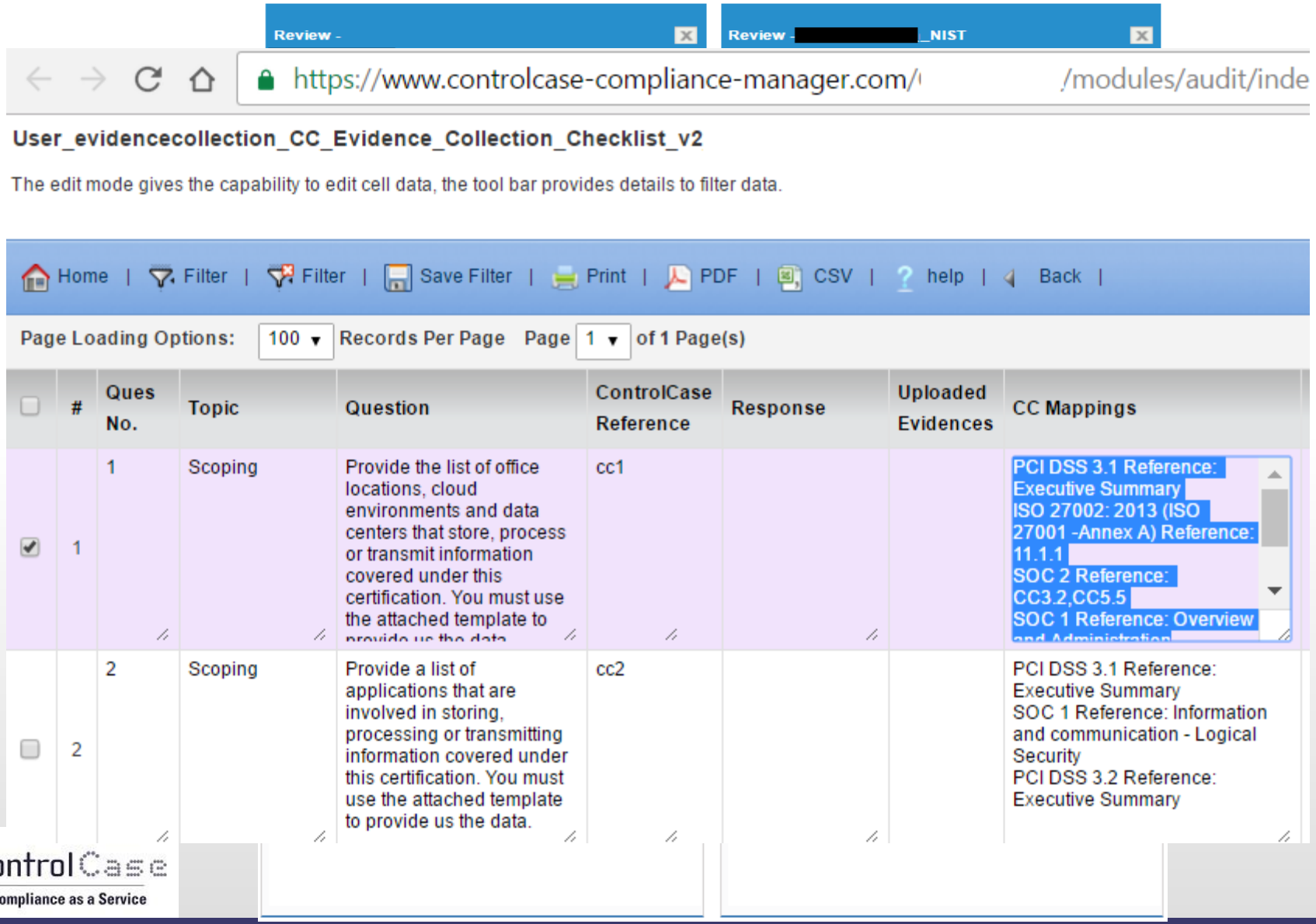
. . . see progress for multiple cert types

- **Single and Centralized Repository for all Compliance Information**
  - Store all your documents, evidences, processes related to compliance in one place and access it from anywhere any time.

- **Dashboards and flexible reporting for snapshot status views of each compliance type**
  - Dashboards with color coded charts and graphs.

ControlCase
Compliance as a Service

Compliance control mapping



	#	Ques No.	Topic	Question	ControlCase Reference	Response	Uploaded Evidences	CC Mappings
☑	1	1	Scoping	Provide the list of office locations, cloud environments and data centers that store, process or transmit information covered under this certification. You must use the attached template to provide us the data	cc1			PCI DSS 3.1 Reference: Executive Summary ISO 27002: 2013 (ISO 27001 -Annex A) Reference: 11.1.1 SOC 2 Reference: CC3.2,CC5.5 SOC 1 Reference: Overview and Administration
☐	2	2	Scoping	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.	cc2			PCI DSS 3.1 Reference: Executive Summary SOC 1 Reference: Information and communication - Logical Security PCI DSS 3.2 Reference: Executive Summary

ControlCase
Compliance as a Service

Integrated Dashboard

ControlCase
Compliance as a Service

Success Stories & Approach

Success Stories

- Marketing company has combined PCI, FISMA, HIPAA
- Healthcare company has combined MARS-E and HIPAA
- Healthcare company has combined HITRUST and HIPAA

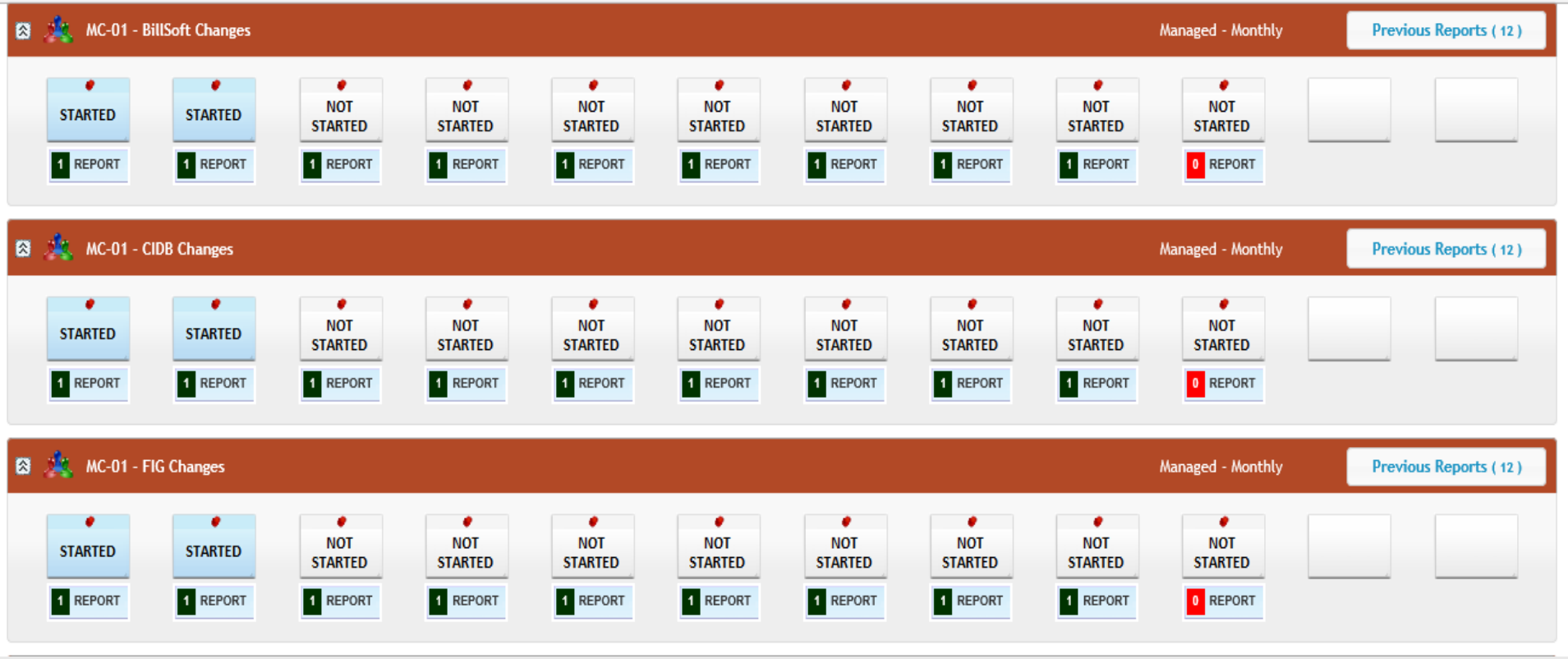
Approach to challenges

- Align Scope
- Synchronize Dates
- Reusing evidence within accepted timeframe

ControlCase
Compliance as a Service

Additional Option: Doc Repository Only

Access to outside 3rd party auditors to dashboard (Example shows SOX)



ControlCase
Compliance as a Service

Thank You !

ControlCase
Compliance as a Service