ControlCase
Compliance as a Service

Establishing the Scope for a Compliance Program

Moderator: Claire LaVelle
Panelists: Jeff Wilder and Nicholas Bettes

Definition of Scope

- The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment. The cardholder data environment (CDE) is comprised of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data. “System components” include network devices, servers, computing devices, and applications.

- *Payment Card Industry (PCI) Data Security Standard, v3.1 p10*

Scoping

- Can be done
  - By reviewing firewall rules
  - Discussing the processes of business partners (accounting, retail…)
  - Enhanced by automated tools and tests (DLP, pen test)

- Results/Goals of scoping
  - Data flows
  - Network diagrams
  - Asset list → Establish sample for evidence collection
  - Negotiating fact for boundary/scope reduction for example

ControlCase
Compliance as a Service

Questions

- 1. Why is scoping important?
- 2. Share with us the methods that you are using for scoping, the difficulties that you might be running into.
- 3. Has that been your experience that after the scope was established, assessed, and agreed upon, the scope changed? Please explain why it changed and how it could have been prevented.
- 4. How do you think an assessor should evaluate/verify your scope?

ControlCase
Compliance as a Service

Questions

- 5. Would purchasing and properly configuring a P2PE solution in your environment reduce your scope? How would you articulate the argument with the auditing company?
- 6. How do you handle the arguments of folks in your enterprise that do not agree with your scope?
- 7. Do you think PCI should strictly be about customer data? Or it should include corporate credit card data for example?

ControlCase
Compliance as a Service