PCI DSS: Business as Usual

Moderator: Neelam Patel
Panelists: Bryan Herbstritt, CTO Rapid Financial Solutions and
Sabine Lainer, Head of Security Compliance, Worldpay

Why Business as Usual is part of 3.0

Compliance is meant to be an ongoing state, as part of day to day activities, ensuring <u>sustained</u> security within the Cardholder Data Environment (CDE), & *not* just an annual push to pass an audit.

RISK: Businesses are left exposed to key vulnerabilities during the majority of the calendar year post audit

Almost no organizations achieve compliance without remediation following the assessment, which shows a low adherence to continued compliance

How does ControlCase interpret BAU?

- Interpretation has evolved over time
- Current Interpretation
  - ControlCase to "expire" evidence so customer has the option to upload new evidence
  - ControlCase to add "Automate-PCI" offering for approximately 50% of the questions
  - Customer has OPTION to keep up with the expiring evidence or do it at year end
  - Customer will get "credit" including lesser questions at end of year if they keep up with BAU

ControlCase
Compliance as a Service

Panel Discussion

Panelists:

- Bryan Herbstritt, CTO
  › Rapid Financial Solutions
- Sabine Lainer, Head of Security Compliance
  › Worldpay

Questions

1. What is your understanding and vision of business as usual, and how is your company preparing to demonstrate this requirement?

2. How does business as usual impact your business's certification?

Additional Questions

1. What are some business as usual tactics that work for your company/program and why?

2. What are the real benefits for your company once you are fully business as usual ready?

3. What is the biggest challenge to achieving business as usual? How can we overcome those?

ControlCase

Compliance as a Service