

Evidence Review Process

Panelists

Kreg Lewis

Director of Payment Systems, **Motionsoft**

Samira El Akili

Manager Security & Compliance, **AIMIA**

Ricky Hacker

Compliance Analyst **CableOne**

Moderator

Ashwani Kaul

ControlCase



Phases in a typical Compliance Process



What is the current state

Gather information

Gather evidence

Review collected evidence

Assess



Fix the gaps

Validate the gaps

Fix the gaps

Add compensating controls

Test and verify fixes

Remediate



Certification

Get the final verdict

Get certified

Start Over again!

Report

The “Assess” phase

- Gather Evidence
- Review Evidence
- Repeat

Ideas for the Panel Discussion

Current State of
this whole
process



Evolution of this
process over the
past decade



Ideas for
improvement on
the next 3 years

Panel Questions

- **Of all the phases in a certification process - how difficult or cumbersome is the evidence collection and review phase compared to other phases?**
- **What techniques or tools have worked best for you?**
- **Is there a difference between Year 1 and Subsequent years?**

Additional Questions

- How would you define a perfect process for evidence collection and review?
- Would you rather deal with a human or a computer through this whole process?
- Is there a better way to organize the documentation/evidence?