Compensating Controls

Moderator Name:

Pramod Deshmane, *ControlCase*

Panelists Names:

James DeFruscio*, Keane UP*

Kathy Lijoi*, Spoken Communication*

Compensating control

- Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating controls.

ControlCase
Compliance as a Service

Compensating Control Must

- Meet the intent and rigor of the original PCI DSS requirement.
- Provide a similar level of defense as the original PCI DSS requirement, such that the compensating control sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against.
- Be “above and beyond” other PCI DSS requirements

ControlCase
Compliance as a Service

ACCEPTABLE COMPENSATING CONTROLS – EXAMPLE 1

- **Constraint** - Organization uses a legacy payment transaction switch which does not support encryption for storage of cardholder data stored in the backend database.

- **Requirement 3.4** - Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs)

- **Identified Risk** – Cardholder data can be compromised since it is stored in clear text format.

ControlCase
Compliance as a Service

ACCEPTABLE COMPENSATING CONTROLS – EXAMPLE 1

Compensating Controls:

- Ensure the transaction switch database is segmented in a separate segment from other In-scope systems with access control filtering.
- Ensure two factor authentication for access to the database.
- Ensure monthly vulnerability assessment for the database servers.
- Ensure administrative access to the server from limited segments/systems.

ControlCase
Compliance as a Service

WHAT YOU CANNOT ASK COMPENSATING CONTROLS FOR

- Lack of Firewall
- Lack of Auditing and Logging Mechanism
- Lack of vulnerability scanning/ ASV scanning process
- Implementing database server on the internet facing web server

ControlCase
Compliance as a Service