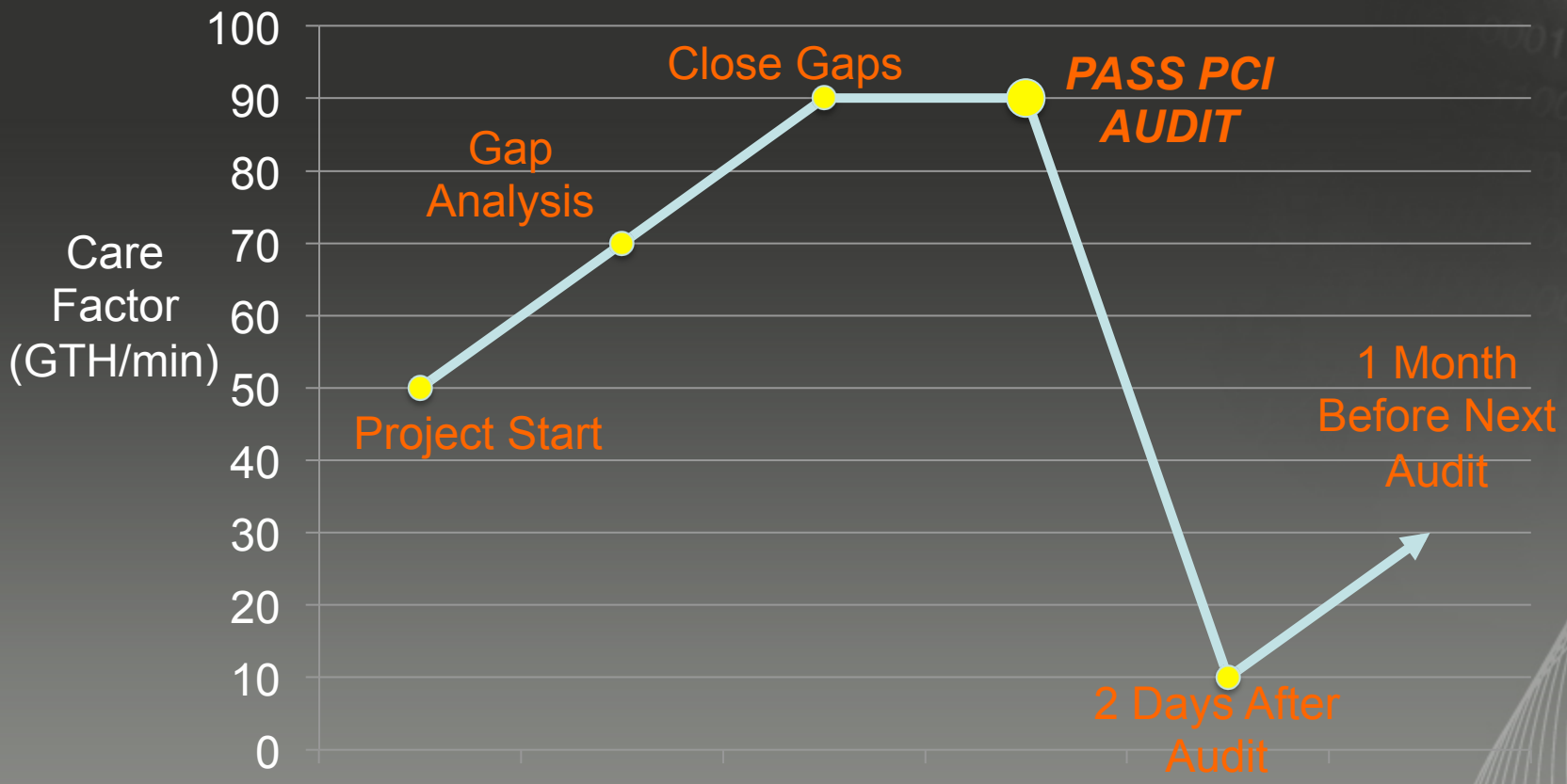
SecurusGlobal

PCI DSS

Lessons from the Field: Maintaining Compliance

Trends – PCI DSS Lifecycle



Attestation of Compliance

Part 3a. Confirmation of Compliant Status	
QSA/Merchant confirms:	
☒	The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version *2.0*, and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of the assessment in all material respects.
☒	The merchant has confirmed with the payment application vendor that their payment application does not store sensitive authentication data after authorization.
☒	**The merchant has read the PCI DSS and recognizes that they must maintain full PCI DSS compliance at all times.**
☒	No evidence of magnetic stripe (that is, track) data, CAV2, CVC2, CID, or CVV2 data, or PIN data storage after transaction authorization was found on ANY systems reviewed during this assessment.

Part 3b. QSA and Merchant Acknowledgments	
Signature of Merchant Executive Officer ↑	***Date:***
Merchant Executive Officer Name:	***Title:***

Signature of Lead QSA ↑	***Date:***
Lead QSA Name :	***Title:***

PCI Mindset

The problem:

“This is a PCI process – it only needs to happen once a year”

PCI Mindset

PCI controls need to be integrated into ‘Business as Usual’

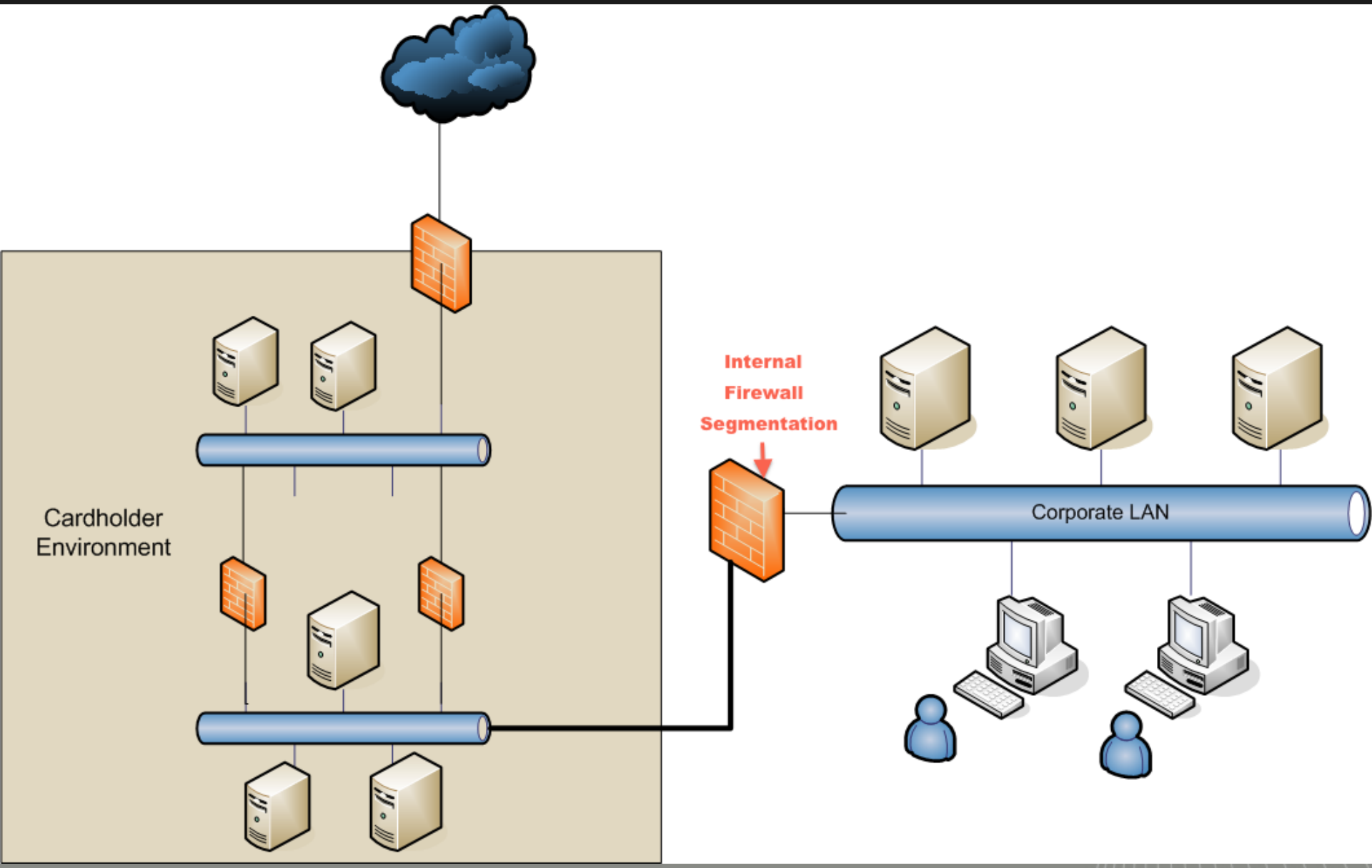

Carrefour
Euskaltel


BMC
BELL


2011
2011
BMC
LEOPARD
AUSTRALIA

Key to Maintaining Compliance

- Control changes to the cardholder environment
- Oversight of ongoing activities
- Simplify where possible


Internal
Firewall
Segmentation
Cardholder
Environment
Corporate LAN

Control the Scope of the Cardholder Environment

- Keep network and data flow diagrams up to date - know your environment
- Involvement in the change process

Maintain the Integrity of the Cardholder Environment

- System Acceptance process for additions
  - Server hardening
  - Vulnerability scan
  - Anti-virus
  - Audit log settings
  - etc

Maintain the Integrity of the Cardholder Environment

- Making significant changes?
  - Seek advice from your QSA

Maintain the Integrity of the Cardholder Environment

- Looking to use a new third party provider?
  - Seek advice from your QSA

Maintain the Integrity of the Cardholder Environment

- Periodic scan for unprotected PANs

Oversight of Ongoing Activities

- Establish an activities timetable
  - Weekly, monthly, quarterly, annual tasks
- Schedule in ticketing system in advance

Oversight of Ongoing Activities

- Spot checks

Simplify Compliance

- Simplify processes
- Automate where possible

Simplify Compliance

- IDS – tune it
- FIM – tune it
- Log monitoring – exception reports

Simplify Compliance

- Vulnerability Management
  - Add environmental criteria

Simplify Compliance

- Firewall Reviews
  - Include change number & expiry in the rule

Summary

- Control changes to the cardholder environment
- Acceptance process for new components
- Oversight of key activities
- Simplify your compliance

Questions?