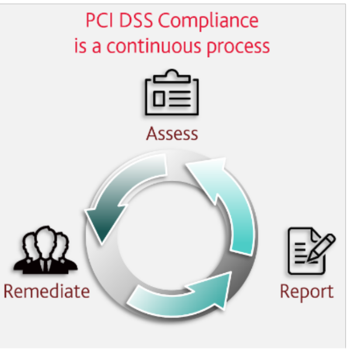
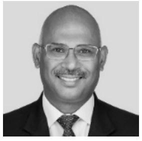
Solution spotlight

PCI DSS





Srikant Ranganathan
Senior Director
T +973 1720 6827
srikant.ranganathan@keypoint.com

Darrshan Manukulasooriya
Senior Manager
T +973 1720 6858
darrshan.m@keypoint.com

What is the PCI DSS?

The payment card industry's (PCI's) security standards council (SSC) has established a data security standard (the PCI DSS) to enhance cardholder data security and facilitate the adoption of consistent data security measures globally. The PCI DSS applies to all entities that store, process or transmit cardholder data – and any business that stores, processes or transmits any cardholder data must comply with the standard. Like many other financial services regulators, the Central Bank of Bahrain (CBB) mandates compliance with PCI DSS – and the penalties for non-compliance can be significant.

Who should follow the PCI DSS?

Types of business which should be PCI DSS-compliant include:

- Merchants – any organisation which accepts card-based payments (through devices or online)
- Banks
- Payment gateways
- Managed service providers – any organisation which manages customer infrastructure and/or applications which store, process and/or transmit card data

What are the six key PCI DSS objectives?

The current version of PCI DSS - 3.2.1 released in May 2018 - has 12 requirements based on six objectives:

- Build and maintain a secure network and systems
- Protect cardholder data
- Maintain a vulnerability management programme
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

How can PCI DSS be integrated into business as usual?

Implementing PCI DSS – and its six key objectives - into business-as-usual activities as part of an entity's overall security strategy:

- Enables the ongoing monitoring of security controls' effectiveness - such as firewalls, intrusion-detection/-prevention systems (IDS/IPS), file-integrity monitoring (FIM), anti-virus (AV) and access controls - to ensure they are operating effectively and as intended
- Helps ensure that security control failures are detected and responded to – from restoring security controls and identifying causes of failure to implementing changes to prevent recurrence and resuming monitoring of the security control - promptly
- Supports reviews of changes to security environments (such as changes in system or network configurations), including determining the potential impact to PCI DSS scope or identifying the PCI DSS requirements applicable to systems and networks affected by those changes
- Ensures changes to organisational structure lead to formal reviews of their impact on PCI DSS
- Helps confirm that PCI DSS requirements are in place and personnel are following secure processes - so that configuration standards are being applied, patches and AV are up to date and audit logs are being reviewed (and that appropriate evidence is being maintained)
- Assesses whether hardware and software technologies continue to be supported by the vendor and meet the entity's security requirements, including PCI DSS

How can Keypoint help?

Keypoint's IT consulting function has an experienced team which has implemented PCI DSS for organisations across MENA. Contact us today to set up a preliminary discussion.