Afenoid

Afenoid Enterprise Ltd

QRC

Quality • Risk • Compliance

QRC Consulting & Solutions Pvt Ltd

Meeting the Challenges of PCIDSS Compliance

By

Opeyemi Onifade, CISSP, CISA, CISM, CGEIT

Highlights

What is PCIDSS

Benefits of PCIDSS

7 Compliance Blockers

Implementation Tips

Conclusion and Questions

INTRODUCTION

IN THE VIRTUAL WORLD

Unlike merchants who operate in the physical world, <u>you do not have</u>

- **face-to-face contact,**
- **a card-in-hand, or**
- **an actual signature**
- **a physical door with a lock and key**
- **a security guard posted 24/7 for protection.**

Cyber-thieves know all of this and are always on the look-out for merchants who are thriving in business, but have let their <u>risk management guard down</u>.

Industry & Market Trends

What is Changing?

Convergence of online & offline commerce

Increased security threats

Increased levels of regulatory change

Changing technologies

Consumer expectations are rising

New emerging shopping behaviors

QRC® Quality • Risk • Compliance
QRC Consulting & Solutions Pvt Ltd

Afenoid
Afenoid Enterprise Ltd

Industry & Market Trends

Today’s card processing environment is much more sophisticated and complex than just swiping a card at the point of sale.

- Example: ecommerce, mobile payments, gateway (API’s and Hosted Pages)

Consumers are increasingly expecting an integrated buying experience that is personalized, secure, and smart.

- Example: Offers sent via smart devices based on buying habits or current locatio

Today’s customer wants to pay whenever and wherever they want and expect to be able to do so.

- Example: in-person, online, via smart device, wireless or stand alone terminal

Merchants need to be ready to provide the payment types and payment channels their
customers want to use while meeting compliance regulations and protecting against
fraud.

- Example: Alternative payment types (Pay Pal, Google Pay) , mobile commerce, EMV chip cards

WHAT IS PCIDSS?

Who is PCI-SSC, What is PCIDSS?

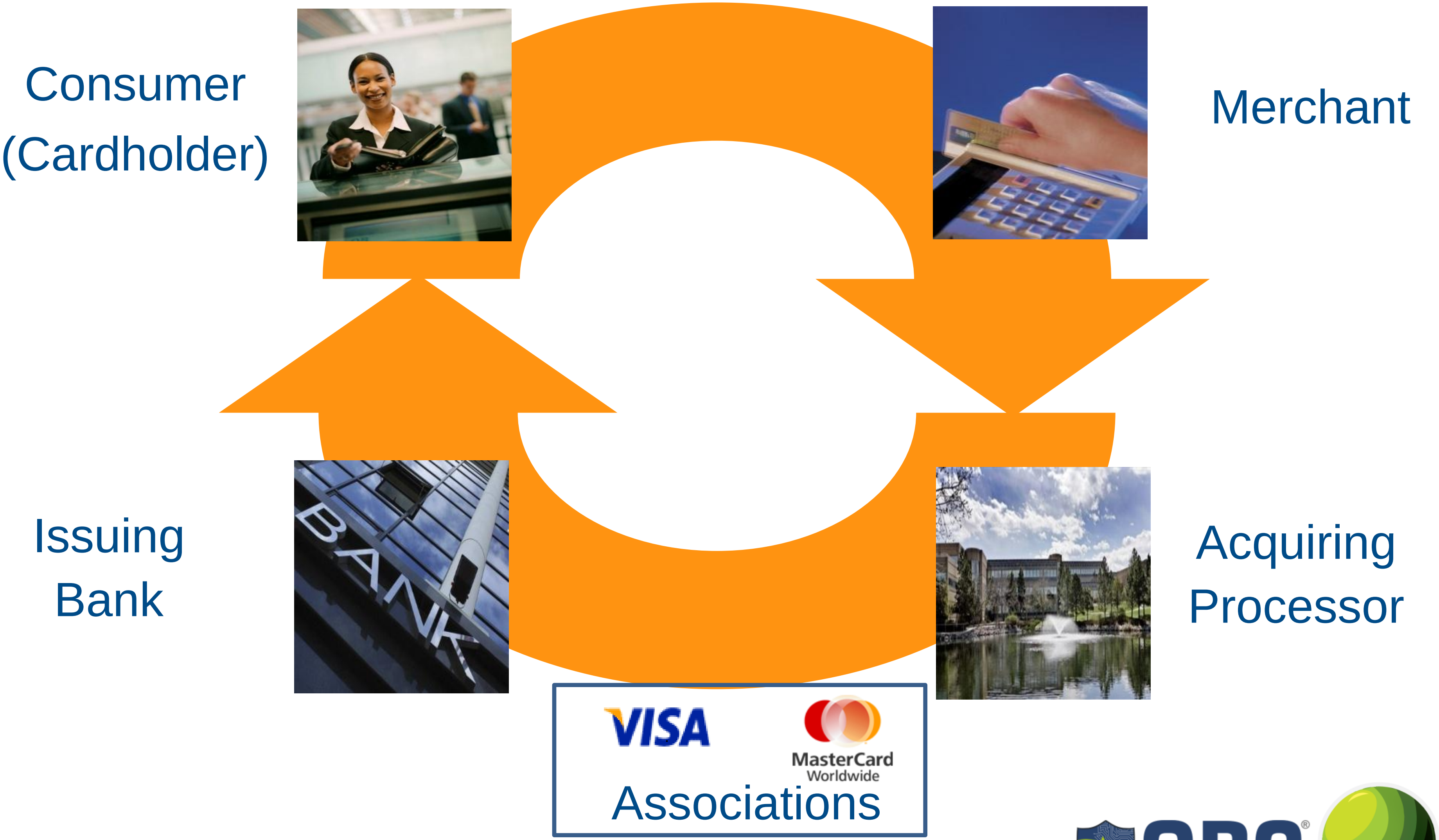
- The PCI Security Standards Council is a global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection. Payment Card Industry Data Security Standard (PCI DSS) developed and propagated by the Council which provides guidelines to secure the card payment processing happening across the global financial system.
- The standards are expected to be complied by any organisation that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) of member branded card data, be it small organization or big, be it merchants, processors, acquirers, issuers or service providers.
- The purpose of PCI DSS is to protect cardholders' financial information by setting a **minimum security standard** that all merchants must meet or exceed. The standard includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.
- Member-branded card data is any card that is part of Visa, Master Card, American Express, Discover and JCB payment schemes, including their subsidiaries and international partners.

PCI DSS

Payment Card Industry Data Security Standard

- Standard that is applied to:
  - Merchants
  - Service Providers (Third Third-party vendor, gateways)
  - Systems (Hardware, software)
- That:
  - Stores cardholder data
  - *Transmits* cardholder data
  - Processes cardholder data
- Applies to:
  - Electronic Transactions
  - Paper Transactions

PAYMENT CARD TRANSACTION: PROCESS FLOW



Consumer (Cardholder)

Merchant

Acquiring Processor

Issuing Bank

VISA

MasterCard Worldwide

Associations

Participants in the Payment Card Cycle

Customers expect to pay for goods and services just as producers expect to be paid for the goods and services they provide.

- Consumers

  Desire to purchase goods and services without making an immediate cash disbursement.

- Merchants

  Want to provide customers with the broadest range of payment options possible with the minimum investment.

  Need the payment process to be as simple and fast as possible.

- Issuing Banks

  Desire to offer a broad range of financial services to consumers.

  Want to charge an annual fee for issuing the card and interest on the payment card balance.

- Associations

  Want to offer a broad range of payment options to consumers.

  Need to cover the cost of processing and the risk associated with the transaction.

  They are required to compensate the issuing bank with the proceeds of the interchange fee.

- Acquiring Processor

  Desires to provide merchants with the maximum range of payment options with minimum investment.

  Need to make a profit on the transactions processed.

THE PCI FRAMEWORK IS DIVIDED INTO 12 SECURITY REQUIREMENTS

Build and Maintain a Secure Network

- 1. Install and maintain a firewall configuration to protect data.
- 2. Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data

- 3. Protect stored data.
- 4. Encrypt *transmission* of cardholder data and sensitive information across public networks.

Maintain a Vulnerability Management Program

- 5. Use and regularly update antivirus software.
- 6. Develop and maintain secure systems and applications

THE PCI FRAMEWORK IS DIVIDED INTO 12 SECURITY REQUIREMENTS..CONT'D

Implement Strong Access Control Measures

- 7. Restrict access to data by business need-to-know.
- 8. Assign a unique ID to each person with computer access.
- 9. Restrict physical access to cardholder data.

Regularly Monitor and Test Networks

- 10. Track and monitor all access to network resources and cardholder data.
- 11. Routinely test security systems and processes.

Maintain an Information Security Policy

- 12. Establish high-level security principles and procedures.

Afenoid
Afenoid Enterprise Ltd

QRC®
Quality • Risk • Compliance
QRC Consulting & Solutions Pvt Ltd

BENEFITS OF PCIDSS

HOW PCI DSS COMPLIANCE HELPS AN ENTITY

Reduce the risk of security breaches:

- complying with the requirements of standard helps an entity to secure the network and infrastructure from external and internal threats. Companies who are PCI compliant significantly reduce their risk of a breach, and therefore, their exposure to penalties and reduce the reputation loss.

Increase in business:

- It is merchant’s responsibility to demonstrate to their customers that they provide secure channel for transactions. The padlock and a trusted logo demonstrate that the website of the business entity applicable encryption that the site claims to be. The enhanced customer satisfaction will ultimately result in increased business.

Proactive Control:

- Enable proactive security incident management through integration with control and monitoring automation.

Protecting image and reputation:

- Complying with the requirements of standard helps an entity to reduce reputation loss because if the data has been compromised it has negative affect on merchant’s reputation.

7 COMPLIANCE BLOCKERS

COMPLIANCE BLOCKERS

1. Inappropriate Scoping

- The very initial phase of PCI DSS implementation is defining the correct scope of assessment which is also considered as the first step of implementation and usually several entities fail to define proper scope. Most of the organization restrict themselves in covering the exact infrastructure within the scope of assessment in order to limit their liability. At a minimum level an organization need to identify infrastructure that is related to the storing, processing and transmitting of cardholder data, and identify all payment channels, locations and data flows in a network diagram.

COMPLIANCE BLOCKERS

2. Undefined and Not formalized stakeholder roles and accountabilities

- Failure to define and formalize roles and responsibilities in interdependent business environments and shared infrastructure scenarios is a blocker to meeting the standard guidelines. Often it has been observed that organization forget to have an agreement with defined roles and responsibility with a service provider with whom card data is shared.

QRC® Quality • Risk • Compliance
QRC Consulting & Solutions Pvt Ltd

Afenoid
Afenoid Enterprise Ltd

COMPLIANCE BLOCKERS

3. Lack of significant controls into CDE:

- It has been observed that entities spend the majority of their efforts to ensure security of their system network devices and servers. However within their internal server where the CDE resides the environment is left moderately unprotected. Usually organizations forget to implement certain controls over internal sensitive environment such as build separate VLAN, properly segmented from Non-CDE, anti-spoofing, NAT, etc. The lack of visibility into the system components and traffic flowing in and out of the CDE makes it difficult, if not impossible, to fully protect this critical environment.

COMPLIANCE BLOCKERS

4. Inconsistent security policies and lack of awareness:

- Taking advantage of modern computing infrastructures, like public cloud infrastructure, creates additional challenges for organizations trying to achieve PCI DSS compliance because public cloud providers do not allow control of their environments. This means organizations seeking the flexibility and cost savings found in cloud offerings are forced to construct divergent security policies relevant the physical infrastructure. The lack of uniformity in security architecture and policies, create constrain to businesses when integrating newly acquired businesses or while migrating applications to public clouds. And also with the advancements in technology it takes time for people to get accustomed to the same which happens because of lack of security awareness training. However PCI DSS mandates that an entity shall provide training and awareness to their existing and new personnel at regular intervals

COMPLIANCE BLOCKERS

5. Leniency by QSAC during onsite assessment:

- Sometimes auditors or QSAC become lenient while collecting the evidences. They do not scrutinize the collected documents and evidences because by which entity fails to comply with PCI DSS.

COMPLIANCE BLOCKERS

6. Complacency assessed entity after certification:

- Once the certification is done entities develop a mind-set that they are in compliance with the standard and now they do not need to do anything till next assessment. Entities fail to maintain the implemented controls as they regularly need to monitor the activities, environmental changes, technology changes and people changes.

COMPLIANCE BLOCKERS

7. Ineffectiveness of Time-based controls

- PCI DSS in an ongoing process with weekly, quarterly and half yearly activities such as patches updating, quarterly internal VA scan, ASV, wireless scan, risk assessment, firewall rule set review etc.. An entity falls into non-compliance zone if it fails to present the above mentioned evidences during the assessment.

Afenoid

Afenoid Enterprise Ltd

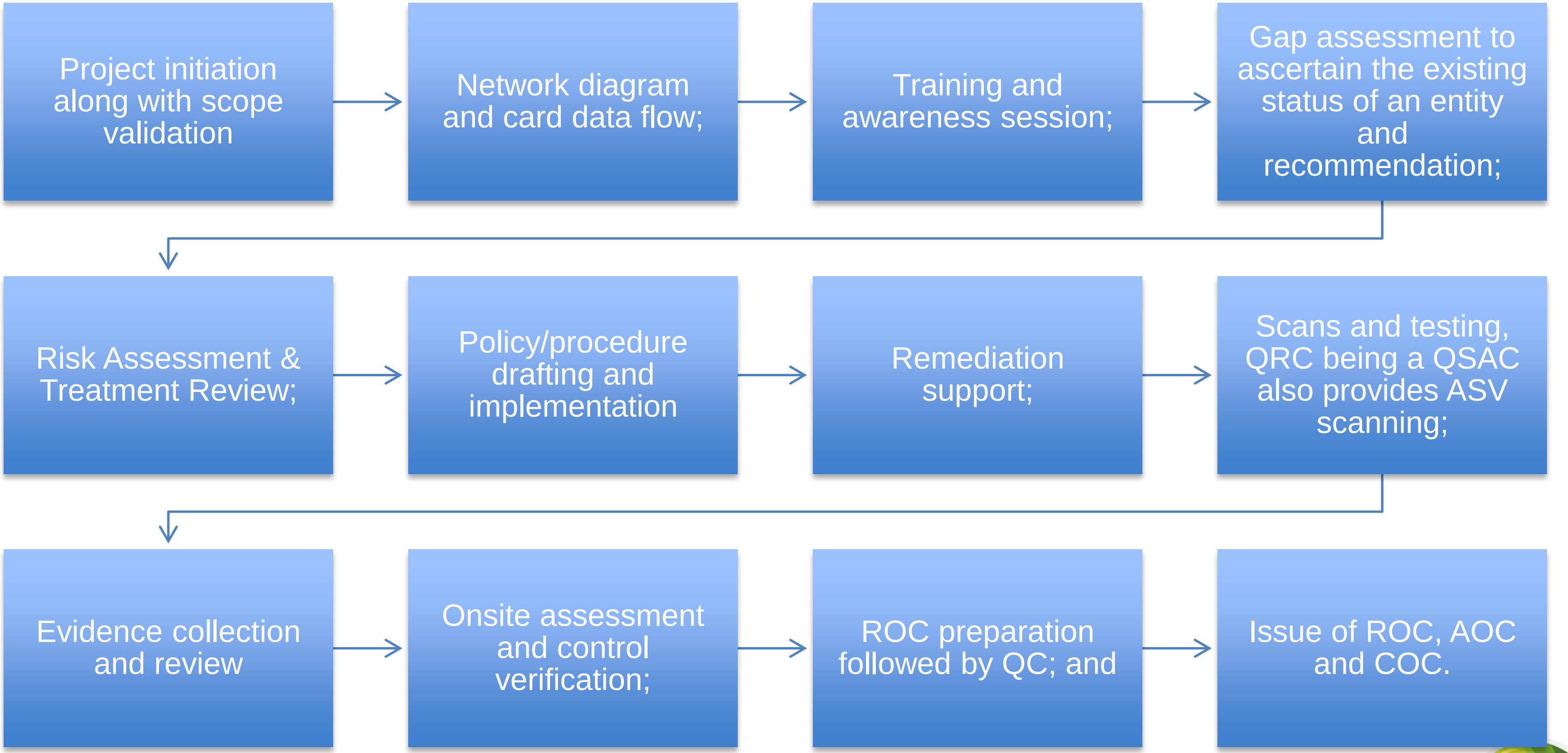
QRC

Quality • Risk • Compliance

QRC Consulting & Solutions Pvt Ltd

IMPLEMENTATION SUPPORT

IMPLEMENTATION TIPS- HOW WE HELP



Project initiation along with scope validation

Network diagram and card data flow;

Training and awareness session;

Gap assessment to ascertain the existing status of an entity and recommendation;

Risk Assessment & Treatment Review;

Policy/procedure drafting and implementation

Remediation support;

Scans and testing, QRC being a QSAC also provides ASV scanning;

Evidence collection and review

Onsite assessment and control verification;

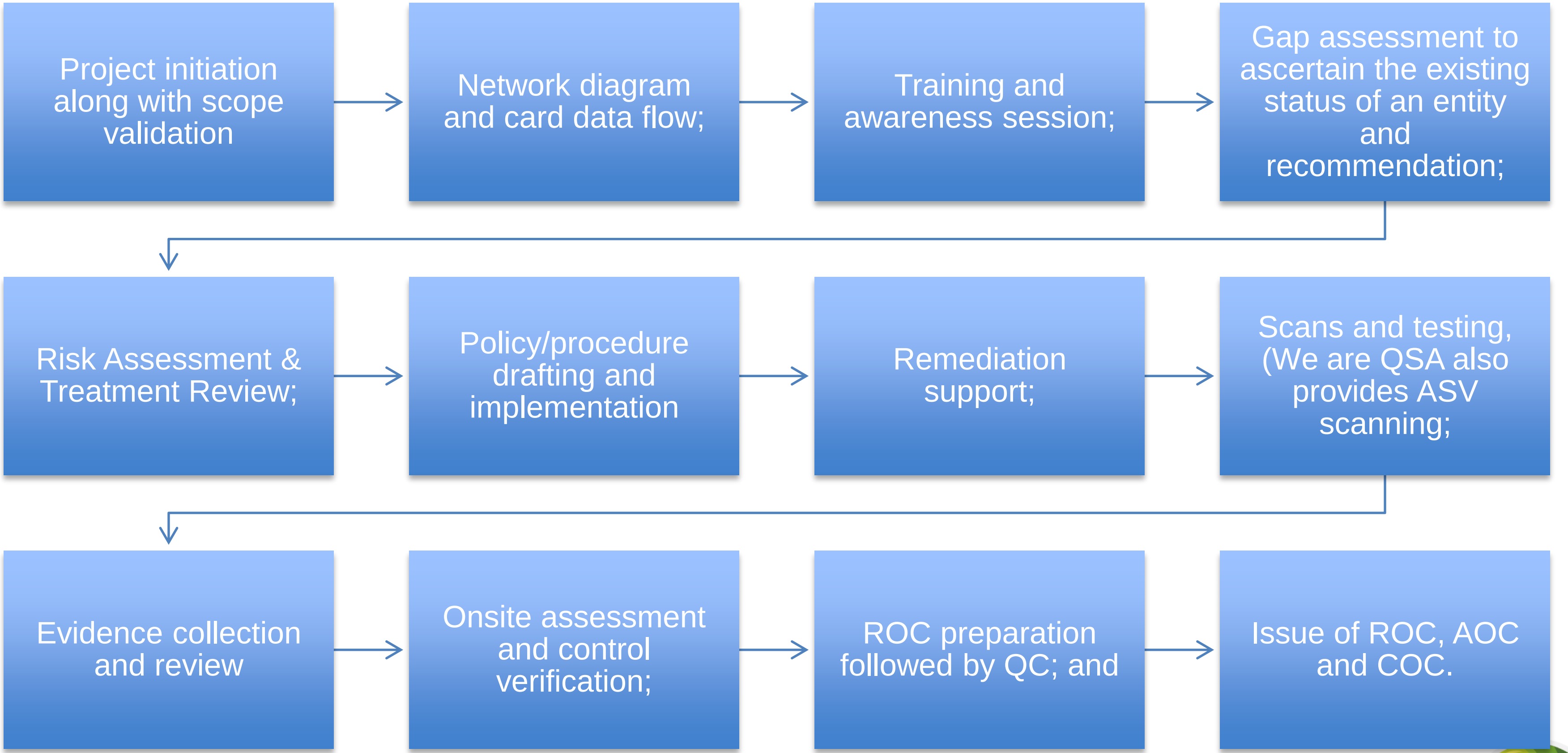
ROC preparation followed by QC; and

Issue of ROC, AOC and COC.

QRC®
Quality • Risk • Compliance
QRC Consulting & Solutions Pvt Ltd

Afenoid
Afenoid Enterprise Ltd

IMPLEMENTATION TIPS- HOW WE HELP



Project initiation along with scope validation

Network diagram and card data flow;

Training and awareness session;

Gap assessment to ascertain the existing status of an entity and recommendation;

Risk Assessment & Treatment Review;

Policy/procedure drafting and implementation

Remediation support;

Scans and testing, (We are QSA also provides ASV scanning;

Evidence collection and review

Onsite assessment and control verification;

ROC preparation followed by QC; and

Issue of ROC, AOC and COC.

QRC®
Quality • Risk • Compliance
QRC Consulting & Solutions Pvt Ltd

Afenoid
Afenoid Enterprise Ltd

KEY CHALLENGES

- Training
- Equipment
- Personnel
- Information
- Management (policy, process, instructions- SOPs etc
- Roles and Responsibilities
- Infrastructure
- Compliance Calendar and Logistics

CONCLUSION

The Data Security Risk is Significant and Therefore Requires Appropriate Controls

The threat of data compromise is global in scope (Web)

Many parties are involved in maintaining data security

The impact of data compromise is widespread financially, legally, and in goodwill exposures

Data security is a primary risk concern for Members, Merchants, Service Providers, Consumers, and Regulators

Data security has evolved from an operational problem and financial threat to a significant reputation risk

CONCLUSION

Proper security enables a company to meet its business objectives by providing a safe and secure environment that helps avoid:

- Loss of revenue
- Loss or compromise of data
- Interruption of business process
- Legal consequences due breach of contracts or regulatory violations
- Damage to customer and partner confidence
- Damage to reputation

A more secure organization also enables easier and safer connectivity with customers and business partners

Local Partner in Ghana: Innovare

Presented by Afenoid Enterprise Limited

November 2015