



PCI DSS Implementation Master

COMPLIANCE WITH PCI DSS_V4.0.1

Housekeeping

2

- ❑ Personal property
- ❑ Mobile phones
- ❑ Smoking
- ❑ Safety
- ❑ Washrooms
- ❑ Breaks and meals



1. About Us

Risk Response Africa is a technology led risk management consulting & training firm specialized in the delivery of the full spectrum of Risk & Resilience management services with emphasis on Enterprise risk & resilience management, Information Security Risk, governance and compliance, IT governance & compliance, Data Privacy & Protection and cybersecurity virtual services.

Our consulting expertise is based on deep technical knowledge & understanding of industry best practices, enabling us to deliver customized solutions that align with your specific business goals and regulatory obligations. Equally our belief that building a resilient organization starts with building a competent workforce, has led us to the design & development of bespoke training services designed to empower individuals & board members to effectively identify, assess, respond and manage risks.

Our mission is to deliver high value & quality world class services etched in international best practice. We aim to serve our clients and the overall ecosystem by shaping not only the African risk & resilience management narrative but also playing an active role in defining the future of risk & resilience management.



For over 10 years, Risk response Africa consultants have matched appropriate security and risk management solutions to business requirements, demonstrating the value of risk management and true information security ROI to relevant stakeholders and embedded resilience and security within organization's day to day operations in a consistent repeatable approach.

COUNTRIES OF WORK EXPERIENCE



Libya



Malawi



Zambia



Rwanda



Tanzania



Botswana



Uganda



Kenya

Risk Response Africa
Nairobi, Kenya

OUR SERVICES

From Strategy to project to Operations, we provide a "one stop" approach to risk management to meet the needs of our clients comprehensively. With decades of experience and a team of certified trainers and consultants, we're well positioned to help you implement the latest approaches and techniques for your business.

SERVICES PORTFOLIO

STRATEGY & ROADMAP
DEVELOPMENT

MATURITY & CAPABILITIES
ASSESSMENT

ERM

ENTERPRISE
RISK &
RESILIENCE
MANAGEMENT

CONTINUITY &
RESILIENCE

4

ESG &
SUSTAINABILITY

SECURITY
GOVERNANCE

SECURITY
GOVERNANCE

MANAGED
VSICO

IT GOVERNANCE

VIRTUAL
SERVICES

DATA PRIVACY &
PROTECTION

MANAGED
DPO

ISO27701
ALIGNED
PIMS

GDPR

ISO27018

OUR COURSES

“Learning and innovation go hand in hand. The arrogance of success is to think that what you did yesterday will be sufficient for tomorrow.”
– William Pollard

RISK
RESPONSE AFRICA
Value Impact Quality

COURSES PORTFOLIO

CYBERSECURITY
FOR MANAGERS

IT DISASTER
RECOVERY

ENTERPRISE
RISK &
RESILIENCE
MANAGEMENT

BUSINESS
CONTINUITY

5

ESG &
SUSTAINABILITY

INFORMATION
SECURITY RISK
MANAGEMENT

INFO SECURITY
GOVERNANCE

SECURITY
GOVERNANCE

PCI DSS
FOUNDATIONS

DATA PRIVACY
FOR
CONSULTANTS

DATA PRIVACY &
PROTECTION

DATA PRIVACY
FOUNDATIONS
COURSE

DATA PRIVACY
FOR
MANAGERS

Course Brief & Adopted Themes

- ❑ This course is designed to help organizations navigate the complexities of the **Payment Card Industry Data Security Standard (PCI DSS) v4.0**. The course provides a comprehensive understanding of the updated PCI DSS requirements and offers practical guidance for implementing and maintaining compliance. Participants will learn how to define their Cardholder Data Environment (CDE), conduct gap analyses, implement controls, and develop policies and procedures to ensure ongoing compliance.
- ❑ The course emphasizes **hands-on learning**, with practical tasks, case studies, and real-world examples to reinforce key concepts. It also references **open-source tools** and **PCI SSC implementation guides** to provide actionable insights and resources.



Following the Pareto principle, our training Programs intend to tackle most of the risk management challenges we face every day (80%) by delivering a selected number of skills and techniques (20%) across the course modules. This approach allows for more focused learning as a small number of focused tasks account for biggest impact on student learning. At the end of each module the student is required to undertake an assessment to assess their understanding of the information provided in that module and to see if the objectives of the module have been met.

This course follows the PACER model, a structured learning approach that stands for Procedural (step-by-step instructions for hands-on expertise), Analogous (drawing comparisons to familiar concepts for easier understanding), Concepts (core theories and principles), Evidence (real-world examples and case studies), and References (key resources and further readings). Feedback loops, peer learning, and reflective opportunities are also embedded to further enhance understanding. Key themes are color-coded for easy reference, and supplementary resources like diagrams, charts, and external data enhance the learning experience. Color-coded tags used throughout the course material include:

Best Practice

Important to note

Further reading

Useful External Data Source

Open source Tool reference

About the course Author

With over a decade of experience in both corporate and consultancy roles, Mary Mbugua is a highly accomplished expert in Risk, Governance, and Compliance. Her diverse expertise spans critical areas such as Enterprise Risk Management (ERM), data privacy, sustainability and resilience, IT risk, and governance. Throughout her career, Mary has consistently demonstrated her ability to navigate the complexities of today's regulatory landscape while delivering strategic, actionable risk management solutions that drive organizational success. Her proficiency encompasses both the technical and strategic dimensions of risk management. In addition to her comprehensive knowledge of privacy, security frameworks, and technical implementations, she has been instrumental in fostering a robust risk management culture within organizations. She is particularly adept at guiding businesses to integrate risk management best practices into their daily operations, ensuring these practices become an intrinsic part of decision-making processes at all levels.

As a Certified Data Protection Officer and a Certified Information Privacy Technologist (CIPT), Mary Mbugua has a profound understanding of global data privacy regulations and compliance practices. She provides valuable guidance to organizations on safeguarding sensitive information and ensuring adherence to international privacy standards, including GDPR, CCPA, and other emerging regulations. Mary's extensive consultancy experience spans various sectors across Africa, where she has helped organizations strengthen their risk frameworks, refine governance structures, and implement sustainable, future-proof business practices.

Beyond her consultancy and advisory roles, Mary Mbugua is a seasoned course author and trainer renowned for her ability to deliver high-quality, engaging, and practical learning experiences to a global audience. She has designed and facilitated comprehensive training programs in areas such as risk management, information security compliance, data privacy, IT Risk & governance, and sustainability. These programs empower professionals across diverse industries to master complex risk management concepts and implement effective strategies within their organizations. As a course author, Mary Mbugua designs and tailors content that is globally relevant, accessible, and tailored to meet the unique needs of an international audience. She has an exceptional ability to translate complex topics into clear, actionable insights that resonate with learners at all levels—from junior staff to senior executives. Her training methodology combines thought leadership with practical, real-world application, ensuring that participants not only understand theoretical concepts but also gain the tools and skills needed to apply them in practice.



Course Resources

- ❑ *"Payment Card Industry Data Security Standard (PCI DSS) v4.0: Helping You to Navigate a Safe Passage Through the Maze of Payment Card Data Security Controls"* by Jim Seaman.
- ❑ **The Definitive Guide to PCI DSS Version 4: Documentation, Compliance, and Management** by Arthur B. Cooper Jr., Jeff Hall, David Mundhenk, and Ben Rothke (2023)
- ❑ **PCI Compliance: Understand and Implement Effective PCI Data Security Standard Compliance (5th Edition)** by Branden Williams and James Adamson (2023)

Key Terms

The following terms and acronyms are used throughout this course:

- ❑ **CDE** – Cardholder data environment
- ❑ **CHD** – Cardholder data
- ❑ **SAD** – Sensitive authentication data
- ❑ **Account Data** – Cardholder data and/or sensitive authentication
- ❑ **PAN**- Primary Account Data
- ❑ **PCI DSS**- Payment Card Industry Data Security Standard
- ❑ **PCI SSC**- Payment Card Industry Security Standards Council

Further reading

❖ Definitions for these terms are provided in the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms:
<https://www.pcisecuritystandards.org/glossary/>

Key Definitions

10

- ❑ **Card Networks** – A credit card network determines where a particular brand of credit card is accepted and sets the interchange fees for each transaction. There are four major credit card networks: Visa, MasterCard, American Express, and Discover. Credit card networks are also often called “card associations” and “card schemes.”
- ❑ **Acquirers** – Banks or financial institutions that process card payments on behalf of merchants.
- ❑ **Issuers** – Banks or entities that provide payment cards to consumers and issue their customers with credit/debit cards. The issuer grants the cardholder the right to use the card, determines the cardholder’s line of credit, and approves or declines the transaction. Most credit and debit cards are issued by banks that partner with either Visa or MasterCard, but American Express and Discover act as both credit card networks and credit card issuers. The issuer is also often called an “issuing bank” or a “cardholder’s bank.”
- ❑ **Switching & Routing** – The process of directing transactions to the correct network for authorization and settlement.
- ❑ **Card Transaction Initiation** – The cardholder presents a payment card at the merchant’s terminal.
- ❑ **Authorization Request** – The merchant sends the transaction request to the acquiring bank.
- ❑ **Transaction Routing** – The acquirer forwards the request to the respective card network (Visa, MasterCard, etc.).
- ❑ **Issuer Bank Approval** – The issuing bank verifies cardholder details, balance, and risk factors before responding with approval or decline.
- ❑ **Transaction Response** – The approval/decline message is sent back to the merchant.
- ❑ **Clearing & Settlement** – Approved transactions are batched and settled between acquirers, issuers, and merchants.
- ❑ **Cardholder-** The cardholder is the customer or client who makes payments or purchases with a credit or debit card

❖ Definitions for these terms are provided in the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms:

<https://www.pcisecuritystandards.org/glossary/>

Further reading

Learning Objectives

Objectives

By the end of this course, participants will:

1. Understand the key changes and requirements of PCI DSS v4.0.
2. Define and scope their Cardholder Data Environment (CDE).
3. Implement technical and operational controls to meet PCI DSS requirements.
4. Develop and document policies and procedures for compliance.
5. Train employees and establish a culture of security awareness.
6. Perform regular testing, monitoring, and internal audits.
7. Manage third-party risks and ensure continuous improvement.

Key Takeaways

- ❑ **Practical Skills:** Participants will gain hands-on experience with tools and techniques for implementing PCI DSS controls.
- ❑ **Actionable Insights:** Real-world case studies and examples will help participants apply concepts to their own organizations.
- ❑ **Comprehensive Resources:** References to PCI SSC implementation guides and open-source tools will provide ongoing support for compliance efforts.
- ❑ **Confidence:** Participants will leave the course equipped to navigate the complexities of PCI DSS v4.0 and maintain compliance effectively.

Course Outline

12

DAY 1

- ❑ MODULE 1
 - ❑ 1.1 PCI DSS ORIGINS
 - ❑ 1.2 PAYMENT ECOSYSTEM
 - ❑ 1.3 APPLICABILITY & ENFORCEMENT
 - ❑ 1.4 COMPLIANCE ASSESSMENTS
- ❑ MODULE 2
 - ❑ 2.1 PCI DSS STANDARD STRUCTURE
 - ❑ 2.2 IMPLEMENTATION APPROACHES
 - ❑ 2.3 IMPLEMENTATION TEAM COMPOSITION
 - ❑ 2.4 IMPLEMENTATION VALIDATION

DAY 2

- ❑ MODULE 3
 - ❑ 3.1 SCOPING FOR PCI DSS
 - ❑ 3.2 CARD DATA FLOW MAPPING
 - ❑ 3.3 CDE DEFINITION
 - ❑ 3.4 ITERATIVE SCOPING
- ❑ MODULE 4
 - ❑ 4.1 CONTROLS SELECTION
 - ❑ 4.2 DOCUMENTED CONTROLS

DAY 5

- ❑ EXAM DAY

DAY 3

- ❑ MODULE 4
 - ❑ 4.1 CONTROLS SELECTION
 - ❑ 4.2 DOCUMENTED CONTROLS
 - ❑ 4.3 TECHNICAL CONTROLS
 - ❑ 4.4 TECHNICAL CONTROLS
- ❑ MODULE 5
 - ❑ 5.1 COMPLIANCE PROGRAM PLANNING
 - ❑ 5.2 TIMEFRAMES & LIFECYCLES

DAY 4

- ❑ MODULE 5
 - ❑ 5.3 CONTROLS IMPLEMENTATION PLANNING
 - ❑ 5.4 CONTINUOUS COMPLIANCE
- ❑ MODULE 6
 - ❑ 6.1 DEMONSTRATING ROI
 - ❑ 6.2 SECURITY PERFORMANCE EVALUATION & MONITORING
 - ❑ 6.3 SAMPLE METRICS & ROI CALCULATIONS
 - ❑ 6.4 SECURITY & ROI REPORTING