BLACKBIRD FOR TRAINING

Visa Payments Cybersecurity Certification

Lagos (Nigeria)

30 November - 4 December 2026

Visa Payments Cybersecurity Certification

Code: IT32 From: 30 November - 4 December 2026 City: Lagos (Nigeria) Fees: 4900 Pound

Introduction

As digital payment systems continue to evolve and online transactions become integral to modern economies, cybersecurity has emerged as a crucial pillar of trust and business continuity. The Visa Payments Cybersecurity Certification equips professionals with the expertise required to protect digital payment environments from advanced cyber threats.

This certification program is designed for managers, team leaders, and cybersecurity professionals seeking to deepen their knowledge of payment security standards, risk management, and data protection strategies. Participants will gain hands-on experience in implementing effective defense mechanisms, ensuring compliance with international standards, and building robust payment infrastructures that resist modern cyber threats.

Course Objectives

- Understand global standards for payment data protection.
- Explore Visa’s cybersecurity framework and operational structure.
- Apply advanced strategies to prevent cyberattacks.
- Assess and mitigate risks in digital payment ecosystems.
- Develop response and recovery plans for security incidents.
- Strengthen governance and compliance mechanisms.
- Implement fraud detection and prevention controls.
- Enhance cross-departmental communication for security coordination.

Course Outlines

Day 1: Fundamentals of Payment Security

- Overview of cybersecurity principles.
- Structure and operation of Visa payment systems.
- Life cycle of a digital transaction.
- Identifying potential vulnerabilities.
- Case studies of major cyberattacks on payment systems.
- Practical exercises on risk assessment.

Day 2: Risk Management and Compliance

- Introduction to enterprise risk management frameworks.
- Techniques for risk evaluation and mitigation.
- Administrative and technical control measures.
- Understanding PCI DSS compliance requirements.
- Preparing analytical risk reports.
- Group activity on designing risk mitigation plans.

Day 3: Technical Protection of Payment Infrastructure

- Securing payment servers and networks.
- Managing encryption keys and authentication systems.
- Monitoring abnormal activity and analyzing logs.
- Tools for early threat detection.
- AI-based solutions for fraud detection.
- Simulation of a cyberattack scenario.

Day 4: Incident Response and Business Continuity

- Incident response principles and frameworks.
- Steps for immediate containment and recovery.
- Digital evidence collection and documentation.
- Business continuity and disaster recovery planning.
- Coordinating response teams under pressure.
- Workshop on institutional response plan development.

Day 5: Compliance and Final Assessment

- Review of Visa certification requirements.
- Internal audit and reporting procedures.
- Self-assessment and readiness testing.
- Certification and validation process.
- Discussion of real-world case studies.
- Final evaluation and knowledge test.

Why Attend This Course? Wins & Losses!

- Gain advanced expertise in payment cybersecurity.
- Increase career growth and professional credibility.
- Learn global standards and best practices.
- Strengthen analytical and risk management skills.
- Foster a proactive cybersecurity culture.
- Master compliance and audit frameworks.
- Improve interdepartmental collaboration.
- Build customer and stakeholder trust.

Conclusion

The Visa Payments Cybersecurity Certification is more than a technical qualification it's a strategic investment in the future of secure financial operations. By combining theoretical insights with real-world applications, the program empowers professionals to anticipate, prevent, and respond effectively to cybersecurity threats targeting payment systems.

Organizations that adopt this training not only safeguard their digital assets but also reinforce their reputation for reliability and data integrity in an increasingly interconnected world.

Blackbird Training Clients

MANNAI Trading Company WLL,
Qatar

Alumina Corporation
Guinea

Booking.com
Netherlands

Oxfam GB International Organization,
Yemen

Capital Markets Authority,
Kuwait

Waltersmith Petroman Oil Limited
Nigeria

Qatar National Bank (QNB),
Qatar

Qatar Foundation,
Qatar

AFRICAN UNION ADVISORY BOARD ON CORRUPTION,
Tanzania

KFAS
Kuwait

Reserve Bank of Malawi,
Malawi

Central Bank of Nigeria
Nigeria

Ministry of Interior,
KSA

Mabruk Oil Company
Libya

Saudi Electricity Company,
KSA

BADAN PENGELOLA KEUANGAN Haji,
Indonesia

NATO
Italy

ENI CORPORATE UNIVERSITY,
Italy

Gulf Bank
Kuwait

General Organization for Social Insurance
KSA

Defence Space Administraion
Nigeria

National Industries Group (Holding),
Kuwait

Hamad Medical Corporation,
Qatar

USAID
Pakistan

STC Solutions,
KSA

North Oil company,

EKO Electricity

Oman Broadband

UN.

Authority for

Head Office: +44 7480 775 526
Email: Sales@blackbird-training.com
Website: www.blackbird-training.com

Blackbird Training Categories

Management & Admin

- Entertainment & Leisure
- Professional Skills
- Finance, Accounting, Budgeting
- Media & Public Relations
- Project Management
- Human Resources
- Audit & Quality Assurance
- Marketing, Sales, Customer Service
- Secretary & Admin
- Supply Chain & Logistics
- Management & Leadership
- Agile and Elevation

Technical Courses

- Artificial Intelligence (AI)
- Sustainability, ESG & Corporate Responsibility
- Advanced Courses
- Hospital Management
- Public Sector
- Special Workshops
- Oil & Gas Engineering
- Telecom Engineering
- IT & IT Engineering
- Health & Safety
- Law and Contract Management
- Customs & Safety
- Aviation
- C-Suite Training

Head Office: +44 7480 775 526
Email: Sales@blackbird-training.com
Website: www.blackbird-training.com