VISA University

# Visa Intermediate Payments Cybersecurity (VIS-CS100) Examination Guide

## Table of Contents

## About the Exam

You are encouraged to use this document to help prepare for the Visa Intermediate Payments Cybersecurity (VIS-CS100) Exam. Passing the exam is a requirement for becoming a Visa Payments Cybersecurity Certified Associate.

The Visa Intermediate Payments Cybersecurity Exam (VIS-CS100) is intended for individuals who have one to two years of payments cybersecurity experience in roles within information security, software development, IT/product security assurance, incident response, risk management, compliance, fraud management, application support, threat intelligence, identify and access management or equivalent training.

Passing this exam shows you have the knowledge and skills necessary to effectively demonstrate an overall understanding of payments cybersecurity. To pass the exam, you should have a solid understanding of the payments system, security concepts, the payments threat landscape, risk management, applied security and payments industry and regulatory concepts.

## Recommended Visa University Courses and Training

- Visa Intermediate Payments Cybersecurity

## Exam Details

**Number of questions: 60**

**Types of questions: Multiple choice and multiple response**

**Length of test: 90 minutes**

**Passing score: 750 (out of a possible 1000)**

### Unscored Content

Your examination may include unscored items that are placed on the test to gather statistical information. These items are not identified on the form and do not affect your score.

### Exam Results

The Visa Intermediate Payments Cybersecurity Exam (VIS-CS100) is a pass or fail exam. The exam is scored against a minimum standard established by professionals who are guided by certification industry best practices and guidelines.

Your results for the exam are reported as a score from 100-1000, with a minimum passing score of 750. Your score shows how you performed on the exam as a whole and whether you passed. Scaled scoring models are used to equate scores across multiple exam forms that may have slightly different difficulty levels.

**Back to top**

VISA University

## Content Outline

This exam guide includes weightings, test domains and objectives only. It is not a comprehensive listing of all the content on this exam. This table lists the main content domains and their weightings.

| Domain | Percentage of Examination |
|---|---|
| Domain 1.0: Payments System Overview | 12% |
| Domain 2.0: Security Concepts | 33% |
| Domain 3.0: Payments Threat Landscape | 13% |
| Domain 4.0: Payments Industry and Regulatory Concepts | 10% |
| Domain 5.0: Risk Management | 9% |
| Domain 6.0: Applied Security | 23% |
| **TOTAL** | **100%** |

## Exam Objectives

### 1.0: Payments System Overview

1.1 Identify different payment types

1.2 Identify the players in the payments ecosystem and their roles

### 2.0: Security Concepts

2.1 Identify the Confidentiality, Integrity, Availability (CIA) Triad concept and other fundamental security concepts

2.2 Identify the purpose of security standards, policies, baseline security configurations and guidelines

2.3 Describe security control domains (e.g., security awareness and user responsibilities, asset management, identity and access management, data security and cryptography, physical and environmental controls, secure operations, network security, secure system and application development, supply chain risk management, incident response and operational resilience)

### 3.0: Payments Threat Landscape

3.1 Identify the payments threat landscape

3.2 Describe the cybersecurity mitigations for current threats

### 4.0: Payments Industry and Regulatory Concepts

4.1 Identify payment standards or regulatory requirements applicable to the payments industry

4.2 Identify the purpose of the payment card industry (PCI) Security Standards Council

Back to top

5.0: Risk Management

5.1 Identify the importance of risk appetite or appropriate risk management strategies (e.g., risk identify, analysis, monitoring, and treatment)

5.2 Describe the details of risk rating based on common vulnerability scoring system (CVSS)

6.0: Applied Security

5.1 Describe different data protection strategies and how each can be applied to payments

5.2 Describe enterprise security operations (e.g., security logging and monitoring and end point security)

5.3 Describe the product security lifecycle

5.4 Identify the importance of patching and vulnerability management processes

Back to top

VISA University

## Gap Analysis Worksheet

**Purpose:**
The purpose of this gap analysis worksheet is to help you assess your own readiness to sit for the Visa Intermediate Payments Cybersecurity Exam (VIS-CS100). By thinking about and evaluating your knowledge, skills and abilities for each objective (i.e., 1.0, 2.0, etc.) and sub-objective (i.e., 1.1, 1.2, 2.1, etc.) you can identify areas where you feel confident and competent versus areas where you may feel less prepared. This can help you better decide where to spend your valuable time studying for the exam. Although you should spend time understanding and studying every objective and sub-objective, the gap analysis can help you understand how to focus more time where your knowledge is weak and less time where you are strong. It can also help you to identify areas where Visa University's Intermediate Payments Cybersecurity course can help to strengthen your knowledge.

**Instructions:**
Three blank columns have been provided so you can conduct a periodic gap analysis throughout your preparation. At a minimum it is recommended that you do one pre-study gap analysis before you start, one roughly during the middle of your preparation (to help gauge your progress and refocus your efforts) and again once you are ready to sit for the exam.

The process is as follows:

1. Evaluate each sub-objective (i.e., 1.1, 1.2, 2.1, etc.) one by one. Ask yourself questions like this: "Do I understand this topic and if so, how well? Do I have experience with this topic? If someone were to ask me about this topic, could I explain it well?" Based up on your answers, rate yourself on a scale of 1 through 5: 1 being very weak/needing significant study and 5 being very strong/needing minimal study.

2. Based upon your results, plan your study time accordingly, focusing more time and effort on weaker areas.

3. As detailed above, it is recommended you repeat the process three times throughout your preparation.

We hope this tool helps to make your study time more effective and assists you in passing the exam.

**Back to top**

| Exam Objective | Self-Analysis 1 | Self-Analysis 2 | Self-Analysis 3 |
|---|---|---|---|
| **1.0: Payments System Overview** | | | |
| 1.1 Identify different payment types | | | |
| 1.2 Identify the players in the payments ecosystem and their roles | | | |
| **2.0: Security Concepts** | | | |
| 2.1 Identify the Confidentiality, Integrity, Availability (CIA) Triad concept or other fundamental security concepts | | | |
| 2.2 Identify the purpose of security standards, policies, baseline security configurations and guidelines | | | |
| 2.3 Describe security control domains | | | |
| **3.0: Payments Threat Landscape** | | | |
| 3.1 Identify the payments threat landscape | | | |
| 3.2 Describe the cybersecurity mitigations for current threats | | | |
| **4.0: Payments Industry and Regulatory Concepts** | | | |
| 4.1 Identify payment standards or regulatory requirements applicable to the payments industry | | | |
| 4.2 Identify the purpose of the payment card industry (PCI) Security Standards Council | | | |
| **5.0: Risk Management** | | | |
| 5.1 Identify the importance of risk appetite or appropriate risk management strategies (e.g., risk identify, analysis, monitoring, and treatment) | | | |
| 5.2 Describe the details of risk rating based on common vulnerability scoring system (CVSS) | | | |

Back to top

| | | | |
|---|---|---|---|
| **6.0: Applied Security** | | | |
| 6.1 Describe different data protection strategies and how each can be applied to payments | | | |
| 6.2 Describe enterprise security operations (e.g., security logging and monitoring and end point security) | | | |
| 6.3 Describe the product security lifecycle | | | |
| 6.4 Identify the importance of patching and vulnerability management processes | | | |

Back to top

## Practice Questions

This Visa Intermediate Payments Cybersecurity Exam (VIS-CS100) guide contains a set of 10 practice questions. There is an answer key provided at the end of the guide. First, read and understand the question thoroughly, then attempt to answer each question on your own. After you have finished, consult the answer key to check your work and understand any errors. These practice questions can be a valuable tool for enhancing your understanding of the material, as they provide an opportunity to gauge your readiness for the actual exam.

**Question 1**

You are a customer who wants to buy a product but do not have enough funds to make the payment. In this situation, which payment method are you likely to use to make the purchase?

- **A.** Debit card
- **B.** Prepaid card
- **C.** Credit card
- **D.** Cryptocurrency

**Question 2**

What is the role of a payment network?

- **A.** A payment network provides payment cards to consumers.
- **B.** A payment network manages the rules and brand and performs transaction switching and settlement.
- **C.** A payment facilitator network is responsible for acquiring merchants to accept payment.
- **D.** The payment network provides back-office payment processing to issuers and/or acquirers.

**Question 3**

Given the statement below:
*The person authorizing a paycheck should not also be the person who prepares the check.*

Which fundamental security concept does this scenario emphasize?

- **A.** Least privilege principle
- **B.** Accountability
- **C.** Non-repudiation
- **D.** Separation of duties

Back to top

**Question 4**

What are three important cryptographic lifecycle management steps? (Choose three.)

**A.** Validation

**B.** Destruction

**C.** Encryption

**D.** Generation

**E.** Distribution

**Question 5**

Which two algorithms are supported by PCI standards? (Choose two.)

**A.** Advanced Encryption Standard (AES)

**B.** COMP128

**C.** Data Encryption Standard (DES)

**D.** Triple Data Encryption Standard (TDES)

**Question 6**

Which type of fraud does EMV 3-D Secure safeguard against?

**A.** Card-present fraud

**B.** Card-not-present fraud

**C.** Counterfeit

**D.** Chargeback

**Question 7**

The vulnerability CVE-2012-1516 has the following metrics and values:

- Access Vector: Network
- Access Complexity: Low
- Authentication: Single
- Confidentiality Impact: Complete
- Integrity Impact: Complete
- Availability Impact: Complete

Which Common Vulnerability Scoring System (CVSS) v2.0 base score is correct in this scenario?

**A.** 0

**B.** 3.5

**C.** 9.0

**D.** 10.5

Back to top

**Question 8**

What are two accepted data at rest protection mechanisms to protect a primary account number (PAN)? (Choose two.)

**A.** Implement keyed cryptographic hashes of the entire PAN.

**B.** Implement a simple hash of the entire PAN.

**C.** Encrypt the Bank identification number (BIN) and the last four digits of the PAN and leave the rest of digits in plaintext

**D.** Leave the BIN and the last four digits of the PAN in plaintext and encrypt the rest of the digits.

**Question 9**

IAM requires that users are authenticated and receive access authorization _____.

**A.** in a short time

**B.** in advance

**C.** if the users have been previously authorized

**D.** only if their authorization has been recently reviewed

**Question 10**

Which statement is correct about an enterprise-wide software patching management strategy?

**A.** An enterprise-wide software patching management strategy is required to handle the number and frequency of patches released on a daily basis.

**B.** An enterprise-wide software patching management strategy is the recommended approach to mitigate unpatched software.

**C.** An enterprise-wide software patching management strategy significantly lowers costs.

**D.** An enterprise-wide software patching management strategy ensures compliance with all regulations.

Back to top

Answer Key

| Question | Answer | Objective |
|---|---|---|
| Question 1 | **C** | 1.1: Identify different payment types |
| Question 2 | **B** | 1.2: Identify the players in the payments ecosystem and their roles |
| Question 3 | **D** | 2.1: Identify the Confidentiality, Integrity, Availability (CIA) Triad concept or other fundamental security concepts |
| Question 4 | **B, D, E** | 2.3: Describe security control domains |
| Question 5 | **A, D** | 4.1: Identify payment standards or regulatory requirements applicable to the payments industry |
| Question 6 | **B** | 5.1: Identify the importance of risk appetite or appropriate risk management strategies (e.g., risk identify, analysis, monitoring and treatment) |
| Question 7 | **C** | 5.2: Describe the details of risk rating based on common vulnerability scoring system |
| Question 8 | **A, D** | 6.1: Describe different data protection strategies and how each can be applied to payments |
| Question 9 | **D** | 6.2: Describe enterprise security operations (e.g., security logging and monitoring and end point security) |
| Question 10 | **B** | 6.4: Identify the importance of patching and vulnerability management processes |

Back to top