



IBM Security Verify PCI DSS Guidance

[IBM Security Verify Compliance Guide](#)

Disclosure

This document is provided for informational purposes only. It represents IBM Security Verify product offerings and practices as of October 2021.

IBM is committed to providing our existing and potential clients with the knowledge to enable them to make decisions regarding their own client base needs.

This document is not legally binding and does not create any warranties, representations, contractual commitments, conditions, or assurances.

Table of Contents

Disclosure 2

1 Introduction 4

2 PCI DSS and IBM Security Verify 5

2.1 Introduction to PCI DSS 5

2.2 Introduction to IBM Security Verify 5

2.3 IBM PCI DSS shared responsibility matrix 6

3 Architecture 10

3.1 Account Setup and Managing User Identity, Access, and Authentication 10

4 Securing the Client’s Services for PCIDSS 13

5 Conclusion 14

6 Disclaimers 15

1 Introduction

This guide documents IBM Security Verify™ guidance for Payment Card Industry Data Security Standard (PCI DSS) compliant environments and usage by clients.



IBM Security Verify clients cannot rely solely on this guide and must independently analyze their particular environments and use cases to verify that their own control environment meets the requirements defined by the PCI Security Standards Council (SSC).

No information in this guide can, or is intended to, supplant any guidance that is given to the IBM Security client by a Qualified Security Assessor (QSA), the PCI SSC, or the entity's acquirer. An entity's acquirer is [defined by the PCI SSC](#) as an "Entity, typically a financial institution, that processes payment card transactions for merchants and is defined as an acquirer."

This guide outlines how an IBM Security Verify client can build PCI DSS-enabled environments and applications. Review the latest guidance, news, and version of the PCI DSS to determine whether any of the PCI DSS requirements apply to your application or environment. Find the latest PCI content at <https://www.pcisecuritystandards.org/>.

The intended audience for this guide are IBM Security Verify clients who need to make their IBM Security Verify environment and related applications PCI DSS-compliant. Readers need to be familiar with the latest PCI DSS requirements and have some background in IBM Security Verify Infrastructure as an identity-as-a-service (IDaaS) offering.

2 PCI DSS and IBM Security Verify

This section introduces the PCI DSS and its 12 requirements. The description of the IBM Security Verify offering and service responsibility matrix are provided to be used as a starting point for the discussion of responsibilities for a client's unique architecture and services.

2.1 Introduction to PCI DSS

The PCI DSS was developed to encourage and enhance cardholder data security and facilitate the global adoption of consistent data security measures. PCI DSS provides a baseline of technical and operational requirements that are designed to protect account data (including card number, expiration date, and verification data). PCI DSS requirements and Security Assessment Procedures require 12 PCI DSS requirements to be met to confirm a system as compliant.

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks.
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs. 6. Develop and maintain secure systems and applications.
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know. 8. Identify and authenticate access to system components. 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. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel.

Figure 1: PCI Data Security Standard – High-Level Overview, from [PCI DSS Requirements and Security Assessment Procedures Version 3.2.1, May 2018](#)

2.2 Introduction to IBM Security Verify

IBM Security Verify, an identity-as-a-service (IDaaS) offering, helps information technology (IT), security, and business leaders manage their identity access management (IAM) programs. IBM Security Verify supports users' requirements for access to applications, business leaders' needs to increase productivity, developers' needs to roll out new services quickly, and IT requirements to respond to business changes more rapidly. IBM Security Verify is a comprehensive platform of IAM capabilities for single sign-on (SSO), multi-factor authentication (MFA), and identity governance, suitable for business-to-employee (B2E), business-to-business (B2B), and business-to-consumer (B2C) use cases.

As a Level 1 Service Provider, IBM Security Verify provides only identity and access management as a service to its client and **does not** directly process, transmit, or store cardholder data.

2.2.1 Physical Security

The in-scope IBM Security Verify environment is hosted in the IBM Cloud® Infrastructure Services Data centers which are located in the US and Europe. IBM Cloud Infrastructure Services is an independent division within IBM and is a PCI DSS v3.2.1 validated Service Provider with Attestation of Compliance

(AOC) dated 31 October 2019.

A key component of a PCI DSS solution is the security of the physical infrastructure and facilities that house the system. For cloud computing, this security extends to the infrastructure and facilities of the cloud service provider. Appropriate physical security controls are in place for IBM Cloud as a cloud service provider. Every aspect of an IBM Cloud Infrastructure Services data center—from location and accessibility to power density and redundancy—is designed to ensure its security, resiliency, and efficiency.

Because physical security in IBM Cloud depends on the underlying infrastructure, clients need to understand how IBM implements physical and environmental security at all IBM Cloud Infrastructure Services data centers. Physical security for data centers is the protection of personnel, hardware, software, networks, and data from physical actions and events that might cause serious loss or damage to an enterprise, agency, or institution. Actions might arise due to human intervention or natural disasters.

IBM Cloud adopts several measures for increased physical security:

- Physical security of the data center perimeter.
- Entry and exit access controls and logging.
- Secure offices, rooms, and facilities.
- Protection against external and environmental threats.
- Redundancy of power and network equipment.
- Secure disposal of equipment during de-provisioning.
- Corporate HR business policy and security for onboarding, training, and offboarding.

Refer to [IBM Cloud Architecture Center > Security architecture > Physical asset security](#) for an overview of the physical security built into IBM Cloud data centers.

2.2.2 Information Security Policy

When a secure cloud solution based on PCI DSS requirements is created, clients must adopt a strong security policy and governances to mitigate risk and meet accepted standards for security and PCI DSS compliance.

To ensure successful cloud adoption, both clients and IBM Security Verify need to establish and follow their respective cloud security policies. These security policies are often aligned to the cloud consumption and delivery model infrastructure as an identity-as-a-service (IDaaS) offering. IBM builds security into its cloud solutions. IBM Security Verify meets strict industry security guidelines and policies as detailed at [IBM Cloud Architecture Center > Security architecture > Policy, governance, risk, and compliance](#).

2.3 IBM PCI DSS shared responsibility matrix



Only a client's assessor (QSA) and acquirer or other responsible PCI DSS authority can determine the appropriate division of responsibilities for a specific operating model on IBM Security Verify. The information and matrix that is provided in this guide are designed to assist the client and their assessor (QSA) in developing and testing appropriate operational processes for their compliance posture.

IBM Security Verify is responsible only for the compliance of the offerings that are designated as PCI DSS ready and delivered. Any processes that are created on or in addition to the IBM Security Verify standard offering by the client or any third party are outside the scope of IBM Security Verify's responsibility.

Some security and PCI DSS compliance recommendations involve IBM products or offerings that do not currently have a PCI DSS Attestation of Compliance (AOC). In these instances, it is the responsibility of the client to document and operate the service or product in a PCI DSS-compliant manner. For a detailed Service Responsibility Matrix, contact your IBM representative.

Shared Responsibility Matrix: IBM Security Verify and Client			
Requirement #	IBM	Client	Notes
1 Install and maintain a firewall configuration to protect cardholder data	X	X	Client is responsible for maintaining and configuring all items that they have access to change. IBM Security Verify is responsible for maintaining public facing network security devices that are used to deliver cloud services. IBM Security Verify does not directly process, transmit, or store cardholder data.
2 Do not use vendor-supplied defaults for system passwords and other security parameters	X	X	When the client provisions a service, the client is responsible for managing their provisioned instances. IBM Security Verify is responsible for managing the configuration of devices that are used to provide the cloud services.
3 Protect stored cardholder data		X	Client is responsible for protecting stored cardholder data. IBM Security Verify does not directly process, transmit, or store cardholder data.
4 Encrypt transmission of cardholder data across open, public networks		X	Client is responsible for securing their data, including cardholder data, and for confirming that data that is transmitted over the public network is encrypted. IBM Security Verify does not directly process, transmit, or store cardholder data. All IBM Security Verify data-in-transit and data at rest is encrypted.
5 Protect all systems against malware and regularly update anti-virus software or programs	X	X	Client is responsible for ensuring that anti-virus software with the latest protections are deployed and maintained on their applications. IBM Security Verify is responsible for managing the use of AV software on devices that are used to provide the cloud services. When the client provisions a service, the client is responsible for managing their provisioned instances.
6 Develop and maintain secure systems and applications	X	X	Client is responsible for secure development when they are using IBM Security Verify offerings. IBM Security Verify develops secure services that use the IBM secure engineering process. See the IBM Secure Engineering Framework Redbook.
7 Restrict access to cardholder data by business need to know	X	X	Client is responsible for provisioning and managing access to their data in IBM Security Verify. IBM Security Verify restricts access to the infrastructure and platform resources that are used to deliver cloud services. IBM Security Verify does not directly process, transmit, or store cardholder data.
8 Identify and authenticate access to system components	X	X	Client is responsible for provisioning and verifying all access to their resources on IBM Security Verify. IBM Security Verify authenticates all access to management planes and components that IBM is responsible for operating.
9 Restrict physical access to cardholder data		X	Client is responsible for maintaining control of any data that is stored outside of the IBM Security Verify environment. IBM Security Verify does not directly process, transmit, or store cardholder data.
10 Track and monitor all access to network resources and cardholder data	X	X	Client is responsible for tracking the use of their applications and access to data in their environment. It is the client's responsibility to maintain and review all access privileges that are provided to their tenant. IBM Security Verify monitors access of its administrators to the infrastructure and platform resources that are used to deliver cloud services. IBM Security Verify does not directly process, transmit, or store cardholder data.

Shared Responsibility Matrix: IBM Security Verify and Client			
Requirement #	IBM	Client	Notes
11 Regularly test security systems and processes	X	X	Client is responsible for testing their implementation within the bounds of the IBM Security Verify Terms of Service or Services Agreement. IBM Security Verify regularly tests security systems and processes as a part of the secure engineering and operations process.
12 Maintain a policy that addresses information security for all personnel	X	X	The client is responsible for their own information security policy. IBM Security Verify maintains a robust information security policy.

3 Architecture

In this section, the IBM Security Verify architecture for PCI DSS-compliant usage is described.

3.1 Account Setup and Managing User Identity, Access, and Authentication

Creating a new IBM Security Verify account is critical to isolate the payment-processing environment that includes IDaaS architecture. To simplify access restriction and compliance auditing, clients need to create a production-quality payment-processing and Cardholder Data Environment (CDE) that is fully isolated from non-CDEs and any development or QA environments.

3.1.1 Managing User Identity and Access

Setting up proper user roles and permissions is key to limit who can access resources and to minimize the damage that a user can do when legitimate permissions are misused. Users experienced with IBM Security Verify and Access Management (IAM) configuration can accomplish equivalent isolation. IBM Security Verify IAM provides secure authentication and delivers digital trust to all resources in the account. Clients can specify who (whether a user or a service) can access which Cloud resource using IBM Security Verify.

The IBM Cloud, IBM Security Verify, and client IAM responsibilities and roles are described in the following section.

IBM Cloud responsibilities

Responsible for protection the infrastructure that runs all the services that are offered in the Cloud. For more information, see section [2.2.1 Physical Security](#).

IBM Security Verify responsibilities

– **IBM Security Verify Operations:**

- Manages the overall configuration of the Service Verify offering that is used by multiple tenants (one tenant per customer).
- Onboards a tenant with pre-defined configurations.
- Facilitate DevOps for upgrades and compliance checks.
- Build and deploy new environments to support our SaaS products.
- Troubleshoot and resolve defects, understand capacity and address performance requirements.
- Monitor network traffic for security events and perform triage analysis to identify security incidents.
- Support and troubleshoot our security cloud and ‘as a service’ environments.
- Configure patch, troubleshoot, and secure, Linux® systems and applications.
- System backups.

Client responsibilities

– **Client IT administrator:**

- Installs, configures, and maintains identity and access tools.
- Manages and configures infrastructure for application integration.
- Monitors all activity reports across IAM framework for unusual activity.
- Responds to security violations specific to identity.
- Creates and manages access policies.
- Evaluates new identity solutions.
- Monitors account lifecycles.
- Sets up and manages Verify settings across the platform.

– **Client service owner:**

- Improve customer and employee end-user experience for owned products and applications.
 - Increase employee productivity.
 - Optimize business processes.
 - Ensure that new applications and solutions comply with security controls and are not vulnerable to exploitation.
 - Set-up and manage Verify settings across the platform.
 - Monitor reports for unusual activity on applications.
 - Ensure that applications are ready for both employee and consumer use.
 - Ensure that employees have appropriate access to applications.
- **Client application developer:**
- Improve customer and employee end-user experience for owned products and applications.
 - Increase employee productivity.
 - Optimize business processes.
 - Ensure that new applications and solutions comply with security controls and are not vulnerable to exploitation.
 - Set-up and manage Verify settings across the platform.
 - Monitor reports for unusual activity on applications.
 - Ensure that applications are ready for both employee and consumer use.
 - Ensure that employees have appropriate access to applications.
- **Client architect:**
- Plan, design, and oversee the development of enterprise programs and IT systems.
 - Define, monitor, and enforce security and user policies and protocols.
 - Evaluate the security and compliance of IT systems, services, and applications.
 - Identify and analyze system and application level vulnerabilities.
 - Create and refine alerts for security tools and processes.
 - Oversee response to high severity incidents.
 - Evaluate and contribute to final decision making for the purchase of new security products.
- **Client customer or employee:**
- Protect company and personal hardware, software, and operating systems from security threats and unauthorized access while productivity is maintained.
 - Monitor what personal data is being collected from them by either their employee or the company where they are providing their data.

3.1.2 Managing Authentication

For application user authentication, clients can secure resources and add authentication by using IBM Security Verify. The client can use IAM service access roles to enable their users, such as configuring identity providers, managing users, customizing the authentication UI, and more.

For more information, see the [IBM Security Verify documentation](#).

4 Securing the Client's Services for PCI DSS

To obtain a copy of IBM Security Verify certification documentation, send an [email](#) with the following required information:

- Client's full business name and full business address.
- Full name of individual client contact (include Mr., Ms., and so on) and job title.
- Statement indicating whether the client is an existing or prospective offering client.
- Statement confirming that an IBM Agreement for Exchange of Confidential Information (AECI) is in place with the existing or prospective offering client.



IBM Security Verify clients cannot rely solely on this guide and must independently analyze their particular environments and use cases in order to verify that their own control environment meets the requirements set forth by the PCI Security Standards Council

5 Conclusion

IBM Security Verify offers many key capabilities to support a client's PCI DSS-compliant environment. This guide addresses those related issues.



Cloud security is a shared responsibility between the cloud service provider and its clients. IBM Security Verify clients cannot rely solely on this guide but must independently analyze their particular environments and use cases in order to verify that the client control environment meets the requirements set forth by the PCI SCC.

6 Disclaimers

© Copyright IBM Corporation 2021

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America October 2021

IBM, the IBM logo, ibm.com, and IBM Security Verify are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates. THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Clients are responsible for ensuring their own compliance with various applicable laws and regulations. Clients are solely responsible for obtaining professional legal advice as to the identification and interpretation of any relevant laws and regulations that may affect the clients’ business and any actions the clients may need to take to comply with such laws and regulations. IBM does not provide legal, accounting or auditing advice. IBM also does not represent or warrant that its services or products will ensure that clients are compliant with any applicable laws or regulations.