



IBM Cloud™ PCI DSS Guidance

IBM Cloud Compliance Guide

Disclosure

This document is provided for informational purposes only. It represents IBM Cloud product offerings and practices as of March 2020.

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

This document does not create any warranties, representations, contractual commitments, conditions or assurances.

Table of Contents

1	Introduction	4
2	PCI DSS and IBM Cloud	5
2.1	Introduction to PCI DSS	5
2.2	Introduction to IBM Cloud Platform	6
2.2.1	Physical Security	6
2.2.2	Information Security Policy	6
2.3	IBM Cloud Platform Services and PCI DSS	7
2.4	IBM PCI DSS shared responsibility matrix	7
3	Architecture	10
3.1	Account Setup and Managing User Identity, Access, and Authentication	10
3.1.1	Managing User Identity and Access	10
3.1.2	Managing Authentication	11
3.2	IBM Cloud IaaS Architecture Examples for PCI DSS	11
3.2.1	IBM Cloud VSIs and Bare Metal Servers	11
3.2.2	Using Firewalls and Load Balancers with VSIs and Bare Metal	13
3.2.3	Using Storage with VSIs and Bare Metal Server	13
3.3	IBM Cloud PaaS Architecture Examples for PCI DSS	14
3.3.1	Explaining PaaS Architecture components	16
3.3.2	Setting up the PaaS environment	18
3.3.3	IBM Cloud Kubernetes Service (IKS) Configuration	19
3.3.4	Summary: Secure Flow for an IKS Application	21
4	Securing the Client's Services for PCI DSS	23
4.1	IBM Cloud Infrastructure Services and PCI DSS	23
4.1.1	IBM Cloud Virtual Servers	23
4.1.2	IBM Cloud Bare Metal	24
4.1.3	Storage (Block Storage, Cloud Object Storage, and File Storage)	25
4.1.4	IBM Cloud Direct Link	26
4.1.5	Hardware Security Module	27
4.1.6	IBM Cloud Load Balancer Options	28
4.2	IBM Cloud PaaS Offerings and PCI DSS	29
4.2.1	IBM Cloud App ID	29
4.2.2	IBM Cloud Certificate Manager	30
4.2.3	IBM Cloud Container Registry	31
4.2.4	IBM Event Streams for IBM Cloud Enterprise	31
4.2.5	IBM Cloud Foundry Enterprise Environment	32
4.2.6	IBM Cloud Identity and Access Management (IAM)	32
4.2.7	IBM Cloud Internet Services	34
4.2.8	IBM Key Protect for IBM Cloud	35
4.2.9	IBM Cloud Kubernetes Service	37
4.2.10	LogDNA services: IBM Log Analysis and IBM Cloud Activity Tracker	41
4.2.11	IBM Cloud Security Advisor	41
4.2.12	IBM QRadar on Cloud	42
5	Conclusion	43
6	Index: IBM Cloud Infrastructure and PaaS Offerings	44
7	Disclaimers	46

1 Introduction

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



IBM Cloud 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 (SSC).

No information in this guide can, or is intended to, supplant any guidance given to the cloud 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 Cloud client can build PCI DSS-compliant environments and applications. It provides a high-level overview of PCI DSS requirements as well as example architectures to help clients deploy and operate a payment processing system to properly handle credit card data (including card number, expiration date, and verification data) in a secure, compliant environment. It's also important to review continually updated guidance and news—as well as the latest version of the PCI DSS—published by the PCI SSC to determine if any of the PCI DSS requirements apply to your application or environment. Find the latest news and standards at: <https://www.pcisecuritystandards.org/>.

The intended audience for this guide is IBM Cloud clients who need to make their IBM Cloud environment and related applications PCI DSS-compliant. Readers should be familiar with the latest PCI DSS requirements, as well as have some background in IBM Cloud Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) architecture.

2 PCI DSS and IBM Cloud

This section introduces the PCI DSS and its 12 requirements. In addition, the IBM Cloud Platform (IaaS and PaaS) and a range of services are presented. A service responsibility matrix is described, 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 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	<ol style="list-style-type: none">1. Install and maintain a firewall configuration to protect cardholder data2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	<ol style="list-style-type: none">3. Protect stored cardholder data4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none">5. Protect all systems against malware and regularly update anti-virus software or programs6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none">7. Restrict access to cardholder data by business need to know8. Identify and authenticate access to system components9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ol style="list-style-type: none">10. Track and monitor all access to network resources and cardholder data11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none">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](#)

Overall, the client is responsible for compliance at the application level. To meet the associated security requirements, a client would need to select appropriate infrastructure and PaaS components from the IBM Cloud Catalog.

2.2 Introduction to IBM Cloud Platform

IBM Cloud is a platform that helps developers build and run modern applications and services. IBM Cloud Platform combines Platform as a Service (PaaS) with Infrastructure as a Service (IaaS) to provide an integrated experience. The platform provides developers with instant access to the compute and services needed to launch quickly, iterate continuously, and scale with success.

Used either individually or in conjunction with one another, various IBM Cloud services provide clients with an extensive array of infrastructure and PaaS capabilities to help ensure the security, accessibility, and usability of clients' business-critical web applications.

2.2.1 Physical Security

A key component to restrict physical access to cardholder data of a PCI DSS solution is the security of the physical infrastructure and facilities that house the system. In the case of cloud computing, this 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 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 is dependent on the underlying infrastructure, clients need to understand how IBM implements physical and environmental security at all IBM Cloud data centers. Physical security for data centers is the protection of personnel, hardware, software, networks, and data from physical actions and events that could cause serious loss or damage to an enterprise, agency, or institution. Actions could 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

Please 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 creating a secure cloud solution for PCI DSS requirements, clients must adopt 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 as a cloud service provider 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 a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). IBM builds security into its cloud solutions. IBM Cloud meets strict industry security guidelines and policies as detailed at [IBM Cloud Architecture Center > Security architecture > Policy, governance, risk, and compliance](#).

2.3 IBM Cloud Platform Services and PCI DSS

A view of PCI DSS-ready IBM Cloud Platform services, and options to request a PCI DSS Attestation of Compliance (AOC), can be found at <https://www.ibm.com/cloud/compliance/industry>. Additional IBM services may be PCI DSS-ready but are not yet listed on the IBM.com page.

IBM Cloud is continuously deploying new and innovative services into the IBM Cloud Catalog. Based upon market demand, the capabilities of these services continue to be enhanced. Not all offerings included in the catalog may currently be PCI DSS-ready (i.e., have a PCI DSS Attestation of Compliance (AOC) available). The client should discuss compliance requirements for their specific architecture with their QSA.

IBM Cloud leverages strategic services from third party IBM Business Partners. IBM terms do not govern or warrant the compliance claims by any third party offering.

2.4 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 Cloud. The information and matrix 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 Cloud is responsible only for the compliance of the IBM Cloud IaaS and PaaS offerings designated as PCI DSS ready and delivered from the IBM Cloud Catalog. Any processes created on or above the IBM Cloud standard offering by the client or any third party are outside the scope of IBM Cloud's responsibility.

For IBM Cloud infrastructure offerings (bare metal, VMware, OpenShift, etc.), the client is responsible for PCI DSS control implementation on the stack above the cloud services provisioned directly from IBM Cloud.

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, please contact your IBM representative.

Shared Responsibility Matrix: IBM Cloud 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 Cloud is responsible for maintaining public facing network security devices used to deliver cloud services.
2 Do not use vendor-supplied defaults for system passwords and other security parameters	X	X	IBM Cloud is responsible for managing the configuration of devices used to provide the cloud services. Once the client provisions a service, the client is responsible for managing their provisioned instances.
3 Protect stored cardholder data		X	Client is responsible for protecting stored cardholder data. IBM Cloud IaaS provides data-at-rest encryption as an option available for clients.
4 Encrypt transmission of cardholder data across open, public networks		X	Client is responsible for securing their data, including cardholder data, and for ensuring that data transmitted over the public network is encrypted. IBM manages the network controls necessary to deliver the cloud services.
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 Cloud is responsible for managing the use of AV software on devices used to provide the cloud services. Once 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 that utilizes IBM Cloud offerings. IBM Cloud develops secure services using IBM's 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 cloud. IBM Cloud restricts access to the infrastructure and platform resources used to deliver cloud services.
8 Identify and authenticate access to system components	X	X	Client is responsible for provisioning and verifying all access to their resources on IBM Cloud. IBM Cloud authenticates all access to management planes and components that IBM is responsible for operating.

Shared Responsibility Matrix: IBM Cloud and Client

Requirement #	IBM	Client	Notes
9 Restrict physical access to cardholder data	X	X	Client is responsible for maintaining control of any data stored outside of the IBM Cloud IaaS environment. IBM Cloud IaaS maintains control of all physical media onsite and follows secure drive sanitization and destruction practices.
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 provided to their cluster. IBM Cloud monitors access of its administrators to the infrastructure and platform resources used to deliver cloud services.
11 Regularly test security systems and processes	X	X	Client is responsible for testing their implementation within the bounds of the IBM Cloud Terms of Service or Master Services Agreement. IBM Cloud 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	IBM Cloud maintains a robust information security policy. The client is responsible for their own information security policy.

3 Architecture

In this section, the IBM Cloud Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) architecture for PCI DSS-compliant usage is described. Example use cases are provided to frame architecture components and recommendations for configuration to support PCI DSS.

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

Creating a new IBM Cloud account is critical to isolate the payment-processing environment that includes IaaS and PaaS 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 / 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 Cloud Identity and Access Management (IAM) configuration can accomplish equivalent isolation by using for in-scope work. IBM Cloud IAM provides secure authentication with the IBM Cloud Platform, IBM Cloud Kubernetes Service (IKS) (for PaaS), and all resources in the account. Clients can specify who (whether a user or a service) can access which Cloud resource on the IBM Cloud Platform. For example, clients can set policies such that only a particular user has administrative access to create virtual servers or Kubernetes clusters.

Different IAM roles can be defined for developers, operators, administrators, cluster administrators, and users.

- **Developer:** a programmer, for instance, who can develop the custom components of an application for a retailer
- **Operator:** a multidisciplinary role that manages a client's cloud capabilities
- **Administrator:** a role responsible for creating teams and assigning resources to other teams. Administrators have access to the resources that are assigned to a team by the cluster administrator
- **Cluster Administrator:** this role can connect to an LDAP directory and add users and assign them to IAM roles. Cluster Administrators also create namespaces and manage workloads, infrastructure, and applications across all namespaces
- **User:** this role processes card information on behalf of merchants

For more details about IAM setup and configuration for PCI DSS-compliant usage, please refer to [Section 4.2.6, “IBM Cloud Identity and Access Management \(IAM\)”](#) in this guide.

3.1.2 Managing Authentication

For application user authentication, clients can secure resources and add authentication with IBM Cloud App ID. App ID secures the application and redirects the user to the authentication page. The client can use IAM service access roles to enable developers to perform tasks in App ID instances, such as configuring identity providers, managing users, customizing the authentication UI, and more.

For more details about App ID setup and configuration for PCI DSS-compliant usage, please refer to [Section 4.2.1, “IBM Cloud App ID”](#) in this guide.

3.2 IBM Cloud IaaS Architecture Examples for PCI DSS

IBM Cloud Bare Metal and IBM Cloud Virtual Servers are both PCI DSS-ready options for the client to receive an operating system and deploy their workload application to the IBM Cloud. The client is responsible for PCI DSS compliance for their own application.

As previously mentioned in [Section 2.2.1 “Physical Security”](#), IBM handles the physical security of all data centers and infrastructure for IBM Cloud services to restrict physical access to cardholder data.

When clients have low cost and short-term usage needs for elastic and scalable workloads, VSI servers should be preferred over bare metal. Bare metal servers will be more suited for highest performance and long-term usage needs. Clients can compare IBM Cloud Bare Metal Servers vs. IBM Cloud Virtual Servers using [these IBM demos](#).

3.2.1 IBM Cloud VSIs and Bare Metal Servers

The following use case leverages an example of a retailer using IBM Cloud Virtual Servers Instances (VSIs) or IBM Cloud Bare Metal servers to build a highly available and scalable web application. The client’s application is a simple PHP frontend with an on-premises database. This application processes credit card data.

If clients have low cost and short-term usage needs for the workload, dedicated VSI servers may be created to install PHP and a database, and cloud storage may be used to persist application files and database backups. When clients create a virtual server, they can choose between a public (multi-tenancy) environment or a dedicated (single-tenancy) environment. Due to their single-tenancy nature, dedicated hosts are a good choice as all resources are isolated from other IBM clients.

If the same workload requires high performance and long-term usage, bare metal servers are preferred as they provide the raw horsepower that is needed for processor-intensive and disk I/O-intensive workloads, including high performance, flexibility, on-demand provisioning, and control.

Both VSI and bare metal servers are included in the architecture example diagram below for clients to select based on their needs. The services used in this example and diagram include:

- [Edge Services: IBM Cloud Internet Services](#)
- [IBM Cloud Load Balancers](#)
- [IBM Cloud Virtual Servers](#)
- [IBM Cloud Bare Metal](#)
- Storage including:
 - [IBM Cloud Block Storage](#)
 - [IBM Cloud File Storage](#)
- [IBM Cloud Direct Link](#)

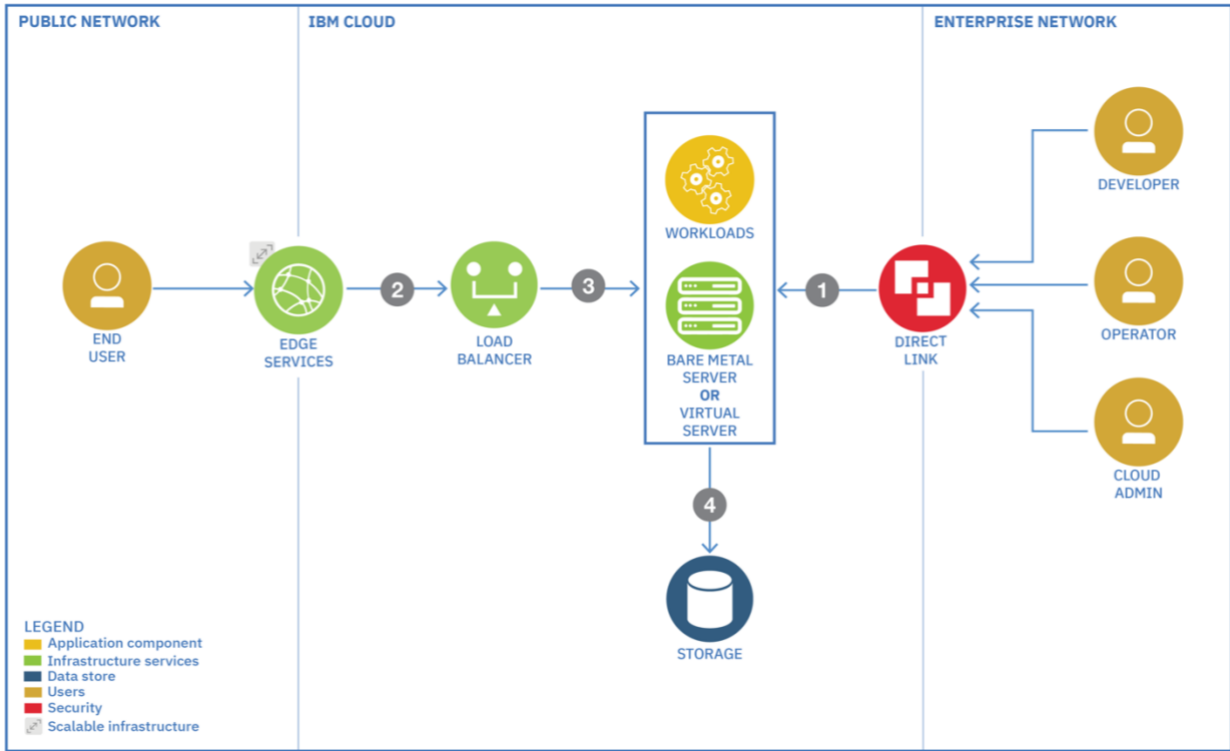


Figure 2: IBM Cloud Virtual Servers and Bare Metal IaaS architecture example for PCI DSS

The capabilities depicted above represent the following process example:

- 1 Roles including developers, operators, and administrators can connect through the Enterprise Network via IBM Cloud Direct Link over a multiple protocol layer switching (MPLS) routing technique. They can design their networking infrastructure using VSI or bare metal servers and then deploy the workload.
- 2 Users connect to the application to process credit card information.
- 3 IBM Cloud Load Balancers are provisioned to distribute requests across application servers to load balance traffic within a location.
- 4 The client’s selected server (VSI or bare metal) uses storage such as IBM Cloud Block Storage or IBM Cloud File Storage to persist application data.

The capabilities above can be extended to another location via Edge Services (IBM Cloud Internet Services) for increased resiliency and higher availability.

For more information, see [Section 4.1.1, “IBM Cloud Virtual Servers”](#) and [Section 4.1.2, “IBM Cloud Bare Metal”](#).

3.2.2 Using Firewalls and Load Balancers with VSIs and Bare Metal

Several firewall and load balancer options are available with VSIs and bare metal servers:

- IBM Cloud Internet Services (CIS): A client could use a CIS firewall (FW) and load balancer (LB). CIS also has content delivery network (CDN), distributed denial-of-service (DDoS), Internet Protocol Firewall (IP FW), global load balancing (GLB), and more. For more information, see [IBM Cloud Docs > Getting Started with IBM Cloud Internet Services](#).
- [FortiGate Security Appliance](#): A Fortigate 10Gbps firewall is recommended for Intrusion Detection System / Intrusion Prevention System (IPS/IDS) requirements.
- Clients can explore additional [firewall](#) and [load balancer](#) options to meet their specific requirements.
- For provisioning a load balancer server to distribute workloads across application servers, see [IBM Cloud Docs > Solution Tutorials > Use Virtual Servers to build highly available and scalable web app](#).

For more information, see [Section 4.1.6, “IBM Cloud Load Balancer Options”](#).

3.2.3 Using Storage with VSIs and Bare Metal Server

If extra storage is needed, clients can order IBM Cloud Block Storage and IBM Cloud File Storage (20 - 12,000 GB) when they provision a VSI or bare metal server. Clients need to connect the add-on storage after their server provisions. For more information about block and file storage:

- [IBM Cloud Docs > Learn about IBM Cloud Block Storage](#)
- [IBM Cloud Docs > Learn about IBM Cloud File Storage](#)

For more information, see [Section 4.1.3, “Storage \(Block Storage, Cloud Object Storage, and File Storage”](#).

3.3 IBM Cloud PaaS Architecture Examples for PCI DSS

A common use case requiring PCI DSS compliance that leverages the PaaS architecture is a client accepting a payment card as payment on its online site/form. IBM suggests an architecture design using IBM Cloud Kubernetes Service (IKS) for developing and deploying a CDE (Cardholder Data Environment) and a non-CDE cluster for processing payment card information (PCI).

Each environment will have its own cluster. IBM manages the security for the control plane, which includes all of the functions and processes that determine which path to use. The client has the responsibility to secure the data plane, which includes all of the functions and processes that forward packets/frames from one interface to another.

The payment-processing flow is as follows:

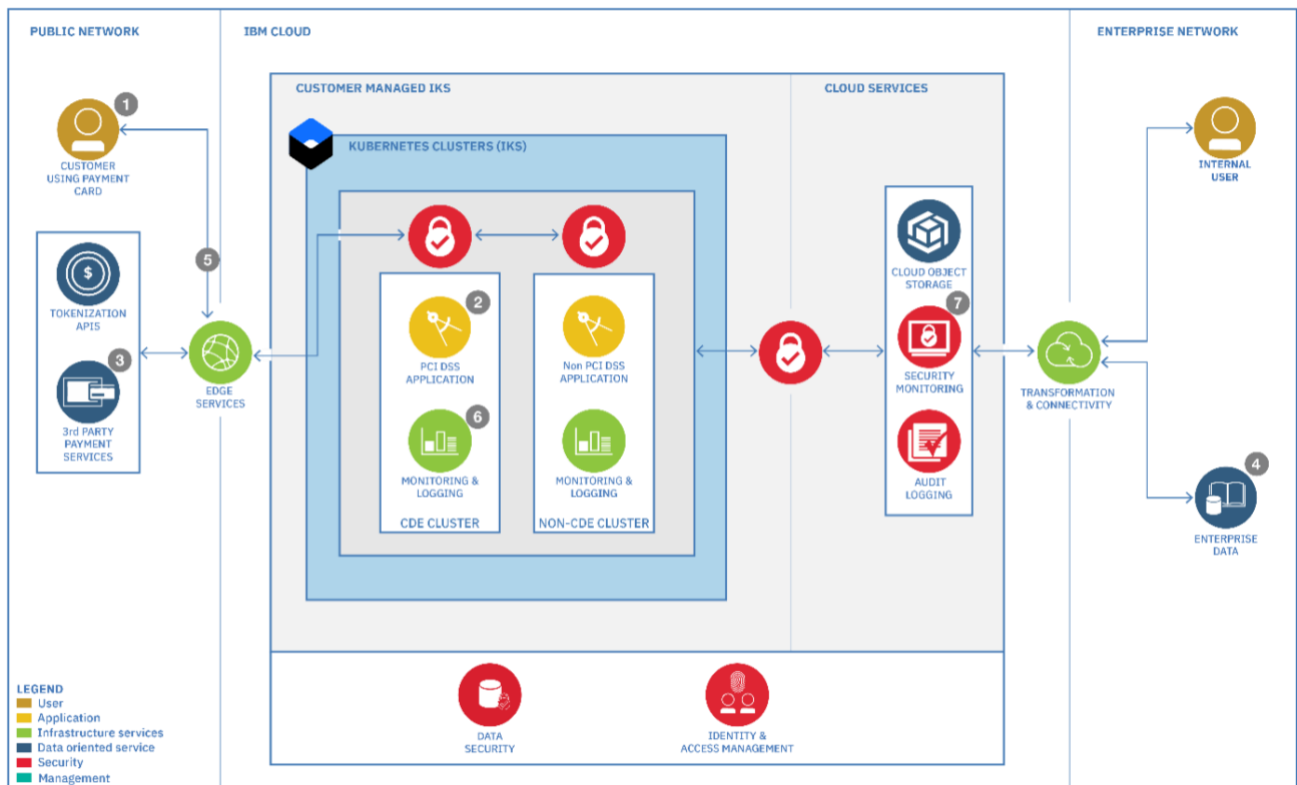


Figure 3: IBM Cloud PaaS architecture example for PCI DSS

- 1 The client's customer enters their payment card information into a payment form that the client owns and maintains. This information passes via Edge Services (IBM Cloud Internet Services (CIS)) to IKS.

- 2 When the client's customer submits their information, the form information is first validated internally in the CDE cluster via the PCI DSS application, including intrusion detection and prevention (IDS/IPS, as indicated by the red lock at the top of the CDE Cluster).

- 3 Next, the form information is securely passed on to a third-party payment processor. The third-party payment processor checks the payment card information and then charges or declines the card.

- 4 The payment processor sends a response back to the payment application. The message is transmitted through the Enterprise Network into storage for archiving purposes.


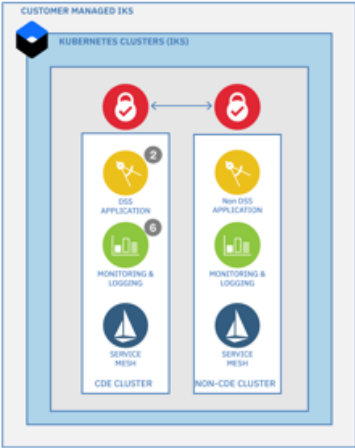

- 5 The same message is transmitted to the client's customer application.






- 6 All of these interactions are logged and monitored with Logging and Monitoring.





- 7 The client can detect cybersecurity attacks and network breaches, enabling proactive responses including any critical data losses.

3.3.1 Explaining PaaS Architecture components

PaaS architecture components supporting the payment-processing flow are shown in Figure 3 above. The architecture frames both Cardholder Data Environment (CDE) and non-CDE clusters.

PaaS Architecture Item	Description
	<p>Edge Services provide the network capability to deliver payment card information through the internet (DNS, CDN, firewall, load balancer).</p> <p>IBM Cloud Internet Services (CIS) provides a combined service for firewall, load balancer, CDN, DNS. For IPS/IDS, a Fortigate 10GB firewall can be used for IKS clusters via Ingress.</p>
 <p>KUBERNETES CLUSTERS (IKS)</p>	<p>IBM Cloud Kubernetes Service (IKS) provides a Kubernetes environment to create a cluster of compute hosts and deploy highly available containers. A Kubernetes cluster lets clients securely manage the resources that they need to quickly deploy, update, and scale applications.</p> <ul style="list-style-type: none"> - CDE Cluster: An IKS cluster that is PCI DSS-compliant and able to process payment card information. - Non-CDE Cluster: A cluster that does not process payment card information and is not PCI DSS-compliant. - Worker Nodes: Worker nodes carry the deployments and services that make up an application. When hosting workloads in the public cloud, clients want to ensure that an application is protected from being accessed, changed, or monitored by an unauthorized user or software. The client owns the worker node and is responsible for securing it. Clients should not run production workloads on free clusters. - Clients can explore various firewalls to protect CDE or non-CDE clusters (red lock indicated on top of clusters in the diagram above). Learn more in IBM Cloud Docs > Opening required ports and IP addresses in your firewall. When data from IKS moves to a cloud service, a security service for encryption like TLS are used to protect data in motion (as indicated by the red lock).
 <p>IDENTITY & ACCESS MANAGEMENT</p>	<p>Setting up proper user roles and permissions is key to limit who can access resources and the damage that a user can do when legitimate permissions are misused.</p> <p>Ingress exposes HTTP and HTTPS routes from outside the cluster to services within the cluster. Access to Ingress nodes is controlled via IBM Cloud Identity and Access Management (IAM).</p>

PaaS Architecture Item	Description
 <p data-bbox="331 443 490 491">TOKENIZATION APIS</p>	<p data-bbox="646 302 1373 499">Tokenization APIs are third party services that can render the Primary Account Number (PAN) unreadable per PCI DSS Requirement 3. Tokenization may help limit the scope of the defined CDE. Clients can use an IBM Cloud Hardware Security Module (HSM) to encrypt PAN. 3rd Party payment services also provide Tokenization APIs.</p>
 <p data-bbox="321 653 500 695">3rd PARTY PAYMENT SERVICES</p>	<p data-bbox="646 558 1393 688">Payment-processing information is passed securely to a third-party payment processor through an API. The third-party payment service checks the payment card information and then charges or declines the card.</p>
 <p data-bbox="331 961 490 1010">MONITORING & LOGGING</p>	<p data-bbox="646 747 1414 848">The key to detect malicious attacks in a cluster is the proper monitoring and logging of metrics and all of the events that happen in the cluster and is one of the key PCI DSS requirements.</p> <p data-bbox="646 869 1382 970">Monitoring and Logging also provides a view of cluster capacity and availability of resources for an application, enabling better planning to protect applications from downtime.</p> <p data-bbox="646 991 1393 1087">IBM Cloud uses IBM Cloud Activity Tracker with LogDNA for monitoring and logging. Clients can configure the LogDNA agent on every worker node in the IKS cluster.</p>
 <p data-bbox="363 1276 457 1325">AUDIT LOGGING</p>	<p data-bbox="646 1134 1398 1331">Kubernetes (IKS) auditing provides a security-relevant chronological set of records documenting the sequence of activities that have affected the system by individual users, administrators or other components of the system. IBM Cloud Activity Tracker with LogDNA can be used to monitor the activity of an IBM Cloud account.</p>
 <p data-bbox="337 1539 482 1587">SECURITY MONITORING</p>	<p data-bbox="646 1377 1414 1612">A security monitoring cloud-based service allows a client to focus on reviewing anomalous conditions and patching the most important asset vulnerabilities. IBM QRadar on Cloud (QRadar) offers Security Information and Event Management (SIEM) to help security teams accurately detect and prioritize threats across the enterprise and provides intelligent insights that enable teams to respond quickly to reduce the impact of incidents.</p>

PaaS Architecture Item	Description
 <p data-bbox="331 510 490 562">CLOUD OBJECT STORAGE</p>	<p data-bbox="646 260 1417 667">IBM Cloud Object Storage (COS) is persistent, highly available storage. Data stored is encrypted in transit and at rest, dispersed across multiple geographic locations, and accessed over HTTP by using a REST API. By default, all objects that are stored in COS are protected at-rest by using randomly generated keys and an all-or-nothing-transform (AONT) encryption type. Clients can enable the security benefits of Bring Your Own Key (BYOK) by importing their own root of trust encryption keys, called Customer Root Keys (CRKs), into the service. Logs for IDS information are stored in COS. Its accompanying metadata, as well as payment card acceptance or decline responses, are stored in an on-premises database.</p>
 <p data-bbox="318 842 506 894">TRANSFORMATION & CONNECTIVITY</p>	<p data-bbox="646 718 1398 848">The connection to the enterprise network is established through the transformation and connectivity component. IBM Cloud Direct Link helps ensure the security of sensitive data to and from the IBM Cloud.</p>
 <p data-bbox="344 1058 477 1110">ENTERPRISE DATA</p>	<p data-bbox="646 932 1393 1094">Enterprise data is typically used by applications and users in an enterprise. Enterprise data is accessed over the direct link to the enterprise network. Clients can use their enterprise-specific on-premises database in their enterprise network for archiving cloud database data.</p>
 <p data-bbox="358 1295 462 1348">DATA SECURITY</p>	<p data-bbox="646 1146 1390 1346">Data security discovers, categorizes, and protects cloud data and information assets with a strong focus on protection of data at rest or in transit. Data security services such as IBM Key Protect for IBM Cloud help key management. IBM Cloud Certificate Manager helps manage and deploy SSL/TLS certificates for client apps and services.</p>

3.3.2 Setting up the PaaS environment

This section describes how to set up a payment-processing environment. Setup includes the following:

- Clients should setup a new IBM Cloud account for the CDE and manage user identity and access as suggested in [Section 3.1, “Account Setup and Managing User Identity, Access, and Authentication”](#).
- To create IBM Cloud Kubernetes Service clusters, follow the steps referred to in [Section 4.2.9, “IBM Cloud Kubernetes Service”](#).
- To restrict access to the environment and securing the network refer to [Section 4.2.9.6, “Restricting access to the environment and securing the network”](#).

3.3.3 IBM Cloud Kubernetes Service (IKS) Configuration

IBM Cloud Kubernetes Service (IKS) provides many features for cluster components so that a client can deploy containerized applications in a security-rich environment. These features are relevant to PCI DSS and are recommended to clients to protect their cluster infrastructure and network communication, isolate their compute resources, and ensure security compliance across their container deployments. The client can extend the level of trust in their cluster to better ensure that what happens within their cluster is what they intended to happen. The client can implement trust in their cluster in various ways, as shown in the following diagram.

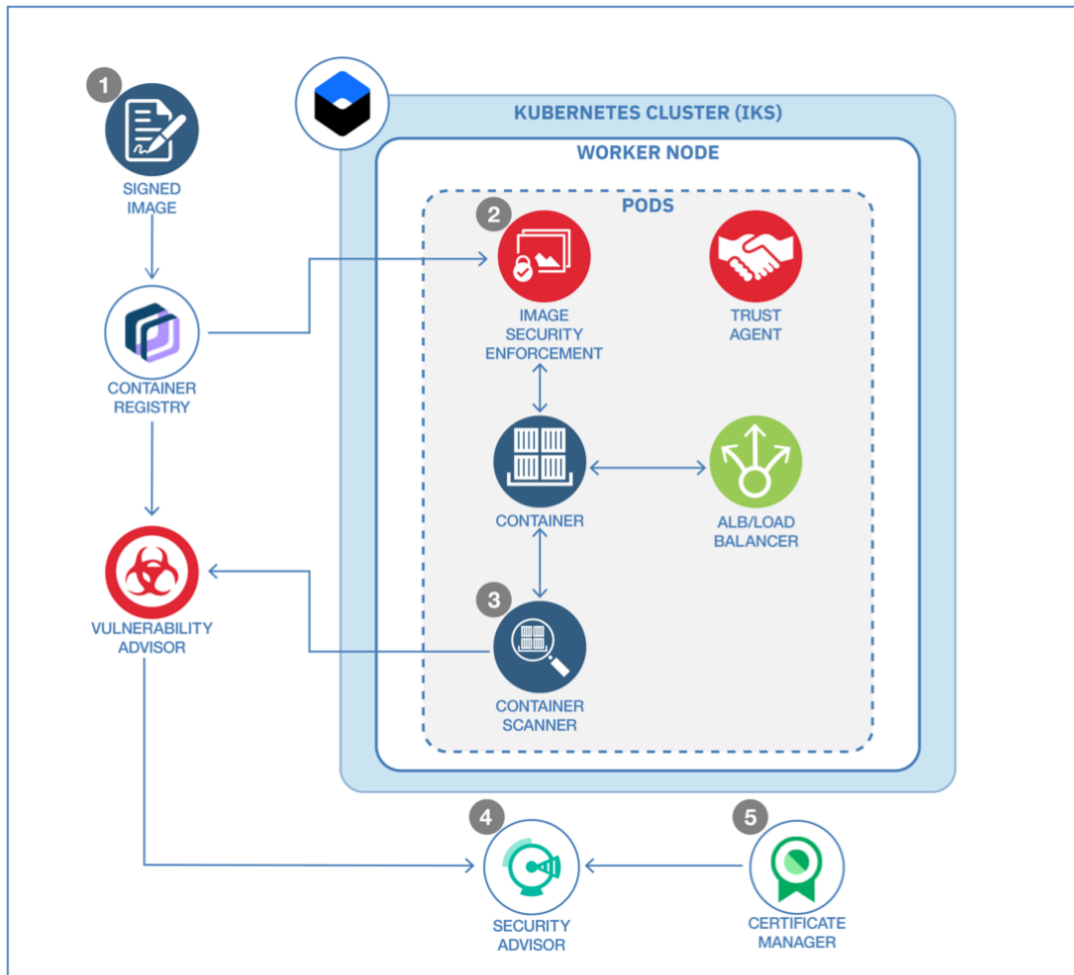


Figure 4: IKS configuration detail to enable trust in cluster

For more information about enabling trust in IKS clusters, see [IBM Cloud Docs > Security for IBM Cloud Kubernetes Service](#).

The steps for a runtime of images and containers are as follows:

- 1 Container Registry – Content Trust for client images:**

Ensure the integrity of the images by enabling content trust in the [IBM Cloud Container Registry](#). With trusted content, the client can control who can sign images as trusted. After trusted signers push an image to the registry, users can pull the signed content so that they can verify the source of the image and this verification is required for PCI DSS applications. For more information, see [IBM Cloud Docs > IBM Cloud Container Registry > Signing images for trusted content](#).

- 2 Container Image Security Enforcement:**

With Container Image Security Enforcement, the client controls where the images are deployed from and ensures that they meet [Vulnerability Advisor](#) policies or [content trust](#) requirements. If a deployment does not meet the policies that the client sets, security enforcement prevents modifications to their cluster. For more information, see [IBM Cloud Docs > IBM Cloud Container Registry > Enforcing container image security](#).

- 3 Container Scanner and Vulnerability Advisor:**

By default, Vulnerability Advisor scans images that are stored in Container Registry to find potential security vulnerabilities. This helps clients to manage vulnerability requirements for PCI DSS. To check the status of live containers that are running in the cluster, the client can install the container scanner. For more information, see [IBM Cloud Docs > Managing image security with Vulnerability Advisor](#).

- 4 Security Advisor:**

With [IBM Cloud Security Advisor](#), the client can easily perform an assessment of the current configuration of the resources in IKS. The Config Advisor assessment combines known security and compliance policies and best practices to identify potential issues in IKS configuration including network and edge protection issues. For more information, see [IBM Cloud Docs > IBM Cloud Security Advisor > Config Advisor](#).

- 5 IBM Cloud Certificate Manager:**

If the client wants to [expose their application by using a custom domain with TLS](#), they can store their TLS certificate in Certificate Manager. Expired or about-to-expire certificates can also be reported in their [Security Advisor](#) dashboard. For more information, see [IBM Cloud Docs > Getting started with Certificate Manager](#).

3.3.4 Summary: Secure Flow for an IKS Application

No application architecture is complete without a clear understanding of potential security risks and how to protect against such threats. As per PCI DSS, it is required to protect card holder data and maintain and monitor a secure network and systems. The following architecture and steps explain a security-oriented, end-to-end view that achieves these objectives:

- Encrypt content in storage buckets with their own encryption keys.
- Require users to authenticate before accessing an application.
- Monitor and audit security-related API calls and other actions across cloud services.

The services used in the following architecture diagram include:

- [IBM Cloud Kubernetes Service](#)
- [IBM Cloud Activity Tracker with LogDNA](#)
- [IBM Cloud Container Registry](#)
- [IBM Key Protect for IBM Cloud](#)
- [IBM Cloud App ID](#)
- [IBM Cloud Certificate Manager](#)
- [IBM Cloud Object Storage](#)

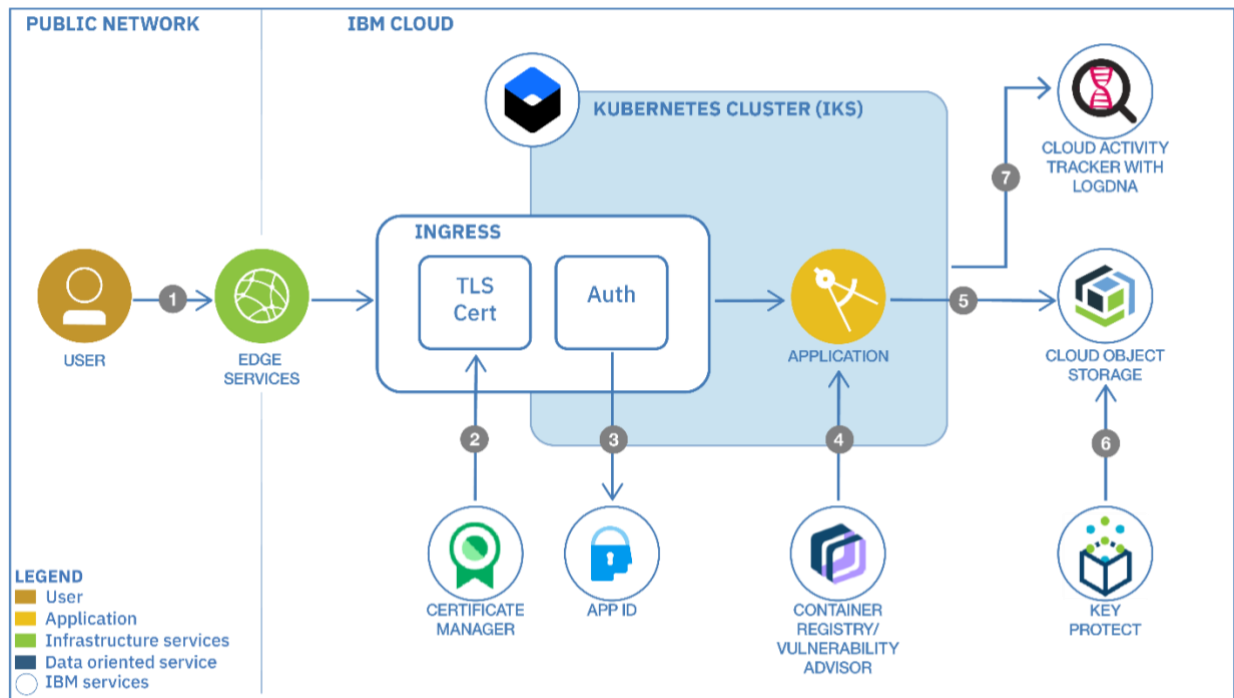


Figure 5: End-to-end secure flow for an IKS application

The steps to achieve this end-to-end view include:

- 1 User connects to the application.

- 2 If using a custom domain and a TLS certificate, the certificate is managed by and deployed from Certificate Manager.

- 3 App ID secures the application and redirects the user to the authentication page. Users can also sign up.

- 4 The application runs in a Kubernetes cluster from an image stored in the Container Registry. This image is automatically scanned for vulnerabilities.

- 5 Uploaded files are stored in Cloud Object Storage (COS).

- 6 File Storage buckets leverage a user-provided key to encrypt data.

- 7 Application management activities are logged by IBM Cloud Activity Tracker with LogDNA.

For more details, see the [IBM Cloud Docs > Solution Tutorials > Apply end to end security to a cloud application](#) tutorial.

4 Securing the Client's Services for PCI DSS

A view of PCI DSS-ready IBM Cloud Platform services, including options to request a PCI DSS Attestation of Compliance (AOC) and detailed Service Responsibility Matrix (SRM), can be found at <https://www.ibm.com/cloud/compliance>. Additional IBM services may be PCI DSS-ready but are not yet listed on the IBM.com page.

IBM Cloud is continuously deploying new and innovative services into the IBM Cloud Catalog. Based upon market demand, the capabilities of these services continue to be enhanced. While not all offerings available in the Cloud Catalog, nor all offerings mentioned in this guide, may currently be PCI DSS-ready (i.e., have a PCI DSS AOC available), clients can still use those offerings. The client should discuss compliance requirements for their specific architecture with their QSA. For example, IBM QRadar on Cloud does not have a PCI DSS AOC available, but it runs on IBM Cloud's compliant infrastructure. If you use IBM QRadar on Cloud for your in-scope PCI DSS web applications, you must demonstrate that your usage meets the relevant PCI requirements.



IBM Cloud 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 (SSC).

In addition to considering general secure engineering leading practices, clients deploying IBM Cloud services should keep in mind the following recommendations in this section for PCI DSS-compliant usage.

4.1 IBM Cloud Infrastructure Services and PCI DSS

Earlier in this guide, [Section 3.2, "IBM Cloud IaaS Architecture Examples for PCI DSS"](#) provided use case and architecture examples for building a PCI DSS-compliant environment using IBM Cloud Infrastructure Services. Additional details for PCI use cases for IaaS offerings follow below in this section.

4.1.1 IBM Cloud Virtual Servers

[IBM Cloud Virtual Servers](#) are scalable and come with dedicated core and memory allocations. The hypervisor is fully managed by the IBM Cloud. A client can perform configuration and management tasks by using both the IBM Cloud client portal and the API. Virtual Servers are deployed to the same VLANs as bare metal servers, enabling workloads to be spread across Virtual Servers and bare metal servers while maintaining interoperability.

The client retains all responsibility for configuring any resource provisioned onto IBM Cloud VSIs in order to maintain PCI DSS compliance. IBM Clients use the IBM Cloud Console to provision and configure the public virtual server instance.

A use case example including IBM Cloud Virtual Servers is featured earlier in this guide in [Section 3.2.1, “IBM Cloud VSIs and Bare Metal Servers”](#).

To learn more about how to provision and configure VSI servers:

- See [IBM Cloud Docs > IBM Cloud Virtual Servers > Provisioning Public Instances](#)
- Follow [IBM Cloud Docs > Solution Tutorials > Use Virtual Servers to build highly available and scalable web app](#)

IBM Cloud Virtual Servers have a PCI DSS AOC available. Applicable PCI DSS Requirements:

Build and Maintain a Secure Network and Systems	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Maintain a Vulnerability Management Program	6. Develop and maintain secure systems and applications

4.1.2 IBM Cloud Bare Metal

[IBM Cloud Bare Metal](#) servers provide users with sole access to the entire server. IBM Cloud Bare Metal servers can be acquired in a preconfigured form or custom-configured to exact specifications.

The client retains all responsibility for configuring any resource provisioned onto IBM Cloud Bare Metal servers in order to maintain PCI DSS compliance.

A use case example including IBM Cloud Bare Metal servers is featured earlier in this guide in [Section 3.2.1, “IBM Cloud VSIs and Bare Metal Servers”](#).

For more information on provisioning bare metal servers, see the [IBM Cloud Docs > IBM Cloud bare metal servers > Getting started tutorial](#).

IBM Cloud Bare Metal has a PCI DSS AOC available. Applicable PCI DSS Requirements:

Build and Maintain a Secure Network and Systems	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Maintain a Vulnerability Management Program	6. Develop and maintain secure systems and applications

4.1.3 Storage (Block Storage, Cloud Object Storage, and File Storage)

IBM Cloud includes options for Block Storage, Cloud Object Storage (COS), and File Storage. The client retains all responsibility for configuring any resource provisioned onto IBM Cloud storage options in order to maintain PCI DSS compliance.

IBM Cloud Block Storage, IBM Cloud Object Storage, and IBM File Storage have a PCI DSS AOC available. Applicable PCI DSS Requirements for all Storage options:

Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components

Storage options were mentioned earlier in this guide in [Section 3.2.1, “IBM Cloud VSIs and Bare Metal Servers”](#). Additional information to support storage usage for PCI DSS use cases includes:

4.1.3.1 IBM Cloud Block Storage

[IBM Cloud Block Storage](#), sometimes referred to as block-level storage, is a technology that is used to store data files on Storage Area Networks (SANs) or cloud-based storage environments. Developers favor block storage for computing situations where they require fast, efficient, and reliable data transportation.

- By default, there is encryption of data using AES-256 standard, including snapshots and replicas of encrypted volumes, and encryption keys are managed in-house using industry standard Key Management Interoperability Protocol (KMIP). For more information, see [IBM Cloud Docs > IBM Cloud Storage - Block Storage > Provider-managed Encryption-At-Rest](#).
- Clients using RedHat Enterprise Linux (RHEL) can enable full disk encryption of block devices with Linux Unified Key Setup-on-disk-format (LUKS). This aids in protecting the contents on mobile devices and removeable media. For more information, see [IBM Cloud Docs > IBM Cloud Storage - Block Storage > Achieving full disk encryption with LUKS in RHEL6](#).

For more information on configuring Block Storage, see [IBM Cloud Docs > Getting started with Block Storage](#).

4.1.3.2 IBM Cloud Object Storage

[IBM Cloud Object Storage](#) (COS) makes it possible to store practically limitless amounts of data, simply and cost effectively. It is commonly used for data archiving and backup, for web and mobile applications, and as scalable, persistent storage for analytics. Flexible storage class tiers with a policy-based archive let you effectively manage costs while meeting data access needs.

IBM Cloud Object Storage was mentioned earlier in this guide in [Section 3.3.1, “Explaining PaaS Architecture components”](#) as well as [Section 3.3.4, “Summary: Secure Flow for an IKS Application”](#). Additional information for PCI DSS use cases:

- **Encryption:** By default, all objects that are stored in COS are protected at-rest by using randomly generated keys and an all-or-nothing-transform (AONT). If it is necessary for the user to control the keys, root keys can be provided on a per-object basis using SSE-C.
 - COS buckets should be encrypted and protected using IBM Key Protect for IBM Cloud, which encrypts data at rest as specified in PCI DSS Requirement #3, “Protect stored cardholder data”.
 - You can enable the security benefits of Bring Your Own Key (BYOK) by importing your own root of trust encryption keys, called Customer Root Keys (CRKs), into the service. With the Key Protect API, you can use a CRK to wrap (encrypt) and unwrap (decrypt) the keys that are associated with your data resources, so you control the security of your encrypted data in the cloud.
 - Key Protect does not process Payment Card Industry (PCI) information. However, Key Protect keys can be used to encrypt/decrypt data encryption keys used by data services to protect data which may include PCI that is stored within the cloud. For more information about Key Protect, see [Section 4.2.8, “IBM Key Protect for IBM Cloud”](#).
- **Setting bucket level permissions:** IBM Cloud Identity and Access Management (IAM) access policies and credentials management can be used to control access to the individual COS buckets which are used to create logical segregation of objects stored. Bucket-level permissions can be set via UI or API to grant specific access roles to certain users.
- **Setting COS bucket firewall:** COS provides the ability to restrict access to buckets by using a bucket-level firewall that will only allow access if the request originates from a trusted network. Access can be restricted to a specific IP address within your network. Read more about this feature at [IBM Cloud Docs > Cloud Object Storage > Setting a firewall](#).

For more information on configuring Cloud Object Storage, see:

- [IBM Cloud Docs > Cloud Object Storage > Getting started tutorial](#)
- [IBM Cloud Docs > Cloud Object Storage > Your responsibilities when using IBM Cloud Object Storage](#)

4.1.3.3 IBM Cloud File Storage

With [IBM Cloud File Storage](#), clients can deploy and customize flash-backed NFS-based file storage from 25 GB to 12,000 GB capacity with up to 48,000 IOPS, and increase storage capacity or adjust performance on the fly to quickly adjust to changes in workload demands.

By default, there is encryption of data using AES-256 standard, including snapshots and replicas of encrypted volumes, and encryption keys are managed in-house using industry standard Key Management Interoperability Protocol (KMIP). For more information, see [IBM Cloud Docs > IBM Cloud Storage - File Storage > Provider-managed encryption-at-rest](#).

For more information on configuring File Storage, see [IBM Cloud Docs > Getting started with File Storage](#).

4.1.4 IBM Cloud Direct Link

[IBM Cloud Direct Link](#) helps ensure the security of sensitive information (such as credit card data) to and from the IBM Cloud.

A use case example including IBM Cloud Direct Link is featured earlier in this guide in [Section 3.2.1, “IBM Cloud VSIs and Bare Metal Servers”](#).

IBM Cloud Direct Link is configured with an isolated virtual routing and forwarding (VRF) table that effectively removes it from the Internet. Information and restrictions regarding the use of VRF are available at [IBM Cloud Docs > Direct Link > More about using VRF](#).

For more information on configuring Direct Link, see [IBM Cloud Docs > Getting started with IBM Direct Link](#).

IBM Cloud Direct Link has a PCI DSS AOC Available. Applicable PCI DSS Requirements:

Protect Cardholder Data	4. Encrypt transmission of cardholder data across open, public networks
--------------------------------	---

4.1.5 Hardware Security Module

[IBM Cloud Hardware Security Module](#) is a centralized, high-assurance capability for cryptographic processing, key generation, and key storage. As client data for PCI DSS use cases will likely contain credit card data, clients can use HSM to protect the cryptographic infrastructure by securely managing, processing, and storing cryptographic keys inside a hardened, tamper-resistant device. The IBM Cloud HSM offering uses the network-attached general purpose HSM, SafeNet Luna Network HSM, manufactured by Thales (formerly Gemalto). A FIPS 140-2 Level 3 validated, single-tenant, password-authenticated device, this HSM is made available by IBM Cloud for client use and configuration.

4.1.5.1 HSM Password and Authentication

IBM employs and makes available extensive password and authentication capabilities:

- **Enablement of TLS Ciphers:** The SafeNet Luna Network HSM uses a default set of cipher suites for TLS communications, such as client connections; if the default list is not suitable, it can be modified.
- **Appropriate setting of the System Date and Time:** Functionality is available to set the date and time manually using the appliance's internal clock, or by synchronizing the appliance with a network time protocol (NTP) server. NTP provides a reliable, consistent, and accurate timing mechanism using Coordinated Universal Time (UTC) and is the recommended option for providing an accurate date and time. Accurate time is paramount for security auditing and troubleshooting of logs.
- **Generation of the HSM Server Certificate:** IBM recommends generating a new HSM server certificate before placing the HSM in service. Do not use the default certificate generated at the factory but regenerate the server certificate once the HSM is in service. If there is a need to generate a new certificate, update client NTLS links to use the new certificate.
- **Binding the NTLS or SSH Traffic to a Device:** It is possible to configure the service to restrict NTLS or SSH traffic to a specific network device (or IP address for SSH traffic):
 - NTLS is used to securely transport the cryptographic messages exchanged between a client and the HSM across the network. Bind the NTLS traffic to a specific network device, a bonded network device, or all network devices.
 - SSH is used to securely transport the administrative messages exchanged between LunaSH and the appliance or HSM across the network. By default, SSH traffic is unrestricted. SSH binding is optional.

4.1.5.2 HSM Initialization

Initialization prepares a new or existing HSM for use. There is a need to initialize the HSM before objects can be generated or stored. The following are key steps:

- Creation of a Network Trust Link Between the Client and the Appliance: Leverage the cryptographic resources to create a secure Network Trust Link (NTL). After that, it is possible to configure links to individual partitions on the appliance using NTL or Secure Trusted Channel (STC).
- Creation of a Secure Trusted Channel (STC) Link Between a Client and a Partition: If there is a need for higher level security for the network links than is offered by NTLS, utilize the STC to provide secure client-partition links. STC offers the following features to ensure the security and integrity of client-partition communications:
 - All data is transmitted using symmetric encryption; only the endpoints can decrypt message
 - Message authentication codes prevent an attacker from intercepting and modifying any command or response
 - Mutual authentication of the HSM and the endpoint ensure that only authorized entities can establish an STC connection
 - Configuring the SafeNet Luna Network HSM appliance to use a Network Time Protocol (NTP) server

For more information, please see [IBM Cloud Docs > Getting started with IBM Cloud HSM](#).

IBM Cloud Hardware Security Module has a PCI DSS AOC Available. Applicable PCI DSS Requirements:

Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data

4.1.6 IBM Cloud Load Balancer Options

[IBM Cloud Load Balancers](#) distribute traffic among your application servers residing locally within IBM data centers. Clients can explore various [load balancers](#) options to meet their specific requirements.

Load Balancers were mentioned earlier in this guide in [Section 3.2.1, “IBM Cloud VSIs and Bare Metal Servers”](#).

For more information, please see [IBM Cloud Docs > Configuring Load Balancing Parameters](#).

Applicable PCI DSS Requirements:

Protect Cardholder Data	4. Encrypt transmission of cardholder data across open, public networks
--------------------------------	---

4.2 IBM Cloud PaaS Offerings and PCI DSS

Earlier in this guide, [Section 3.3, “IBM Cloud PaaS Architecture for PCI DSS”](#) provided use case and architecture examples for building a PCI DSS-compliant environment using IBM Cloud PaaS offerings. Additional details PCI use cases for PaaS offerings follow in this section.

4.2.1 IBM Cloud App ID

[IBM Cloud App ID](#) allows you to easily add PCI DSS authentication controls to web and mobile applications with zero code changes and no redeploy required. Enhance your apps with advanced security capabilities, such as multi-factor authentication (MFA), single sign-on (SSO) and user-defined password policies. You can also use App ID's scalable user registry to let users manage their own accounts.

App ID was included in [Section 3.3.4, “Summary: Secure Flow for an IKS Application”](#). Additional information for PCI DSS use cases:

- **Secure Passwords:** As the account owner, a client can enforce more secure passwords for Cloud Directory by configuring a set of rules that user passwords must conform to. Examples include the number of attempted sign-ins before lockout, expiration times, minimum time span between password updates, or the number of times that a password cannot be repeated.
- **Logging and Auditing:** IBM Cloud Activity Tracker with LogDNA can be used to review and build charts for management and runtime activity. Audited events include configuration changes, user management, user logins, password resets and more.
- **Connection Security:** App ID will reject any connections which are not HTTPS and TLS 1.2 and above. This ensures that the communication channel between the client's application and App ID is using the highest level of encryption.
- **Profile Update Restrictions:** The developer or operator can decide whether end-users can make updates to their profiles using their applications. If users should not update their profiles, this capability can be disabled in the App ID Dashboard.
- **Service Access Roles:** The client can use IBM Cloud IAM service access roles to enable developers to perform tasks in App ID instances, such as configuring identity providers, managing users, customizing authentication UI and more.

For more information, please see *IBM Cloud Docs > IBM Cloud App ID > [Getting started tutorial](#)*.

IBM Cloud App ID has a PCI DSS AOC Available. Applicable PCI DSS Requirements:

Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data

4.2.2 IBM Cloud Certificate Manager

[IBM Cloud Certificate Manager](#) helps you manage and deploy SSL/TLS certificates for your apps and services. Certificate Manager provides a secure repository for your certificates and their associated private keys, and helps prevent outages by sending notifications when your certificates are about to expire.

Certificate Manager was included earlier in this guide in [Section 3.3.3, “IBM Cloud Kubernetes Service \(IKS\) Configuration”](#), [Section 3.3.4, “Summary: Secure Flow for an IKS Application”](#). Additional information for PCI DSS use cases:

- **Certificate Expiration:** The client should configure Certificate Manager to send notifications well in advance of certificate expiration. The expiration notification can be configured to trigger an automated process to renew and deploy certificates.
- **Service Access Roles:** The client can use service access roles in Certificate Manager to restrict users from executing certain tasks in Certificate Manager instances, such as importing, downloading, editing, or deleting certificates.
- **Logging and Auditing:** Certificate Manager is integrated with the IBM Cloud Activity Tracker with LogDNA service to track how users and applications interact with the Certificate Manager service in the IBM Cloud. Clients can then monitor the activity of their IBM Cloud account and investigate abnormal activity and critical actions to comply with PCI DSS requirements. In addition, they can be alerted on actions as they occur. The events that are collected comply with the [Cloud Auditing Data Federation \(CADF\)](#) standard.
- **Key Management:** Any keys stored in the services should be managed according to key management best practices. At a minimum, the key management procedures in PCI DSS Requirement 3 should be followed. For instance, access policies for certificates and keys should be configured. All access to and activities regarding keys and certificates should be audited, with the logs retained for at least a year.

More information on configuring IBM Cloud Certificate Manager can be found at [IBM Cloud Docs > Certificate Manager > Getting started tutorial](#).

IBM Cloud Certificate Manager has a PCI DSS AOC available. Applicable PCI DSS Requirements:

Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data

4.2.3 IBM Cloud Container Registry

[IBM Cloud Container Registry](#) allows storage and distribution of container images in a fully managed private registry. Private images can be pushed to conveniently run them in the IBM Cloud Kubernetes Service and other runtime environments. Images are checked for security issues, so informed decisions can be made about your deployments.

Container Registry was included earlier in this guide, with details and configuration information, in [Section 3.3.3, “IBM Cloud Kubernetes Service \(IKS\) Configuration”](#) as well as [Section 3.3.4, “Summary: Secure Flow for an IKS Application”](#). Additional information for PCI DSS use cases:

- **Establish a Private Docker registry for images to be stored:** This can be accomplished via the IBM Cloud Container Registry Setup. IBM Cloud enforces an account/namespace hierarchy for granting access to resources like IBM Cloud Container Registry.

More information on configuring IBM Cloud Container Registry can be found at [IBM Cloud Docs > Getting Started with IBM Cloud Container Registry](#).

IBM Cloud Container Registry has a PCI DSS AOC Available. Applicable PCI DSS Requirements:

Maintain a Vulnerability Management Program	6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know

4.2.4 IBM Event Streams for IBM Cloud Enterprise

Built on open source Apache Kafka, [IBM Event Streams](#) is an event-streaming platform that helps you build smart applications that can react to events as they happen. IBM Event Streams benefits from the years of operational expertise IBM has running Apache Kafka for enterprises, making it perfect for mission-critical workloads.

- **Do not place sensitive information in topic names:** Topic names and consumer groups are encrypted for transmission between Event Streams and clients as a result of TLS. However, Event Streams does not encrypt these values at rest. Therefore, you are not recommended to use confidential information in your topic names. Learn more in [IBM Cloud Docs for Event Streams: Data Security and Privacy](#).
- **Encrypt your message data at the application layer:** Users should ensure that they encrypt their message data at the application layer before sending to the service.

IBM Event Streams for IBM Cloud Enterprise has a PCI DSS AOC available. Note, the Classic (deprecated), Lite, and Standard plans for IBM Event Streams for IBM Cloud are not included in the PCI DSS AOC. Applicable PCI DSS Requirements:

Protect Cardholder Data	3. Protect stored cardholder data
--------------------------------	-----------------------------------

4.2.5 IBM Cloud Foundry Enterprise Environment

With [IBM Cloud Foundry Enterprise Environment \(CFEE\)](#), you can instantiate multiple, isolated, enterprise-grade Cloud Foundry platforms on-demand. Instances of the CFEE service run within your own account in IBM Cloud, and the environment is deployed on IBM Kubernetes Service clusters.

Clients have full control over the environment, including access control, capacity management, change management, monitoring, and accessed cloud services. As such, the client is free to use the service instance for anything it is capable of supporting. The client should ensure that CFEE and dependent services should have access to the least amount of sensitive data as possible.

It should be made clear, however, that even though the CFEE control plane (via UI/API/CLI) does process sensitive data (e.g., PCI DSS relevant data), it is the responsibility of the client to ensure that they use their CFEE responsibly, since all dependencies are managed and owned by the client in their IBM Cloud account.

More details available at [IBM Cloud Docs > Your responsibilities by using IBM Cloud Foundry Enterprise Environment](#).

*IBM Cloud Foundry Enterprise Environment has a PCI DSS AOC available.
Applicable PCI DSS Requirements:*

Build and Maintain a Secure Network and Systems	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data
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

4.2.6 IBM Cloud Identity and Access Management (IAM)

[IBM Cloud Identity and Access Management](#) enables clients to securely authenticate users for platform services and control access to resources consistently across IBM Cloud. A set of IBM Cloud services are enabled to use IBM Cloud IAM for access control and are organized into resource groups within an IBM Cloud user account to give users quick and easy access to more than one resource at a time. IBM Cloud IAM access policies can be used to assign users and service IDs access to the resources within an account. Users and service IDs can be added into an access group to easily give all entities within the group the same level of access.

IAM was included in [Section 3.3.1, “Explaining PaaS Architecture components”](#), as well as in [Section 3.3.2 “Setting up the PaaS environment”](#). Additional information for PCI DSS use cases:

- To control access to their Kubernetes clusters and environments, clients can utilize the IAM tool to set authentication and authorization rules.
- IAM gives clients the ability to tie in authentication into an existing LDAP or SAML service and manage authorization rules based on pre-defined roles in IAM.
- Use IAM to enable the access rules documented in the latest version of the PCI DSS.

4.2.6.1 How IAM access policies provide access

A policy consists of a subject, target, and role. The subject in this case is the access group. The target is what you want the subject to access, such as a set of resources, a service instance, all services in the account, or all instances of a service. The role defines the level of access that is granted to a user.

The most commonly used roles are viewer, editor, and administrator. The viewer role provides the least amount of access for viewing instances and resource groups in an account. The editor role has more access for creating, editing, deleting, and binding service instances. The administrator role includes everything for working with a service instance and can assign access to others. However, two different categories of roles are available to consider: platform and service.

For more information about the roles that can be assigned, see the [IBM Cloud Docs > Managing identify and access > Cloud IAM roles](#).

4.2.6.2 Assigning access to access groups

You can organize resources in a resource group and users and service IDs into an access group to make assigning access as simple as possible. After you set up each one, you can create access policies for the access groups to give users in your account access to the resources that you created.

1. Click Manage > Access (IAM) and select Access Groups.
2. Select the name of the access group that you want to assign access.
3. Select the **Access policies** tab, and then click **Assign access**. You have the following options for assigning access:
 - **Assign access to resources within a resource group:** Use this option to give the two-part policy that is needed for users who create resources from the catalog and assign the resources to a resource group. When you use this option, you can give access to the resource group itself, and all resources in a particular resource group or just one service or instance in the resource group.
 - **Assign access to resources:** Use this option to assign access to all IAM-enabled services across the account or to a single service in the account, but not to an instance level.
 - **Assign access to Account Management Services:** Use this option to provide a user access to account management services as a way to delegate some of your account owner capabilities. For example, you can delegate the ability to view billing and usage, invite and remove users, manage access groups, manage catalog services, or manage service IDs. You can provide access to all account management services or just one.

More information about configuring IBM Cloud Identity and Access Management can be found at [IBM Cloud Docs > Getting started with IAM tutorial](#).

*IBM Cloud Identity and Access Management has a PCI DSS AOC Available.
Applicable PCI DSS Requirements:*

Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data

4.2.7 IBM Cloud Internet Services

[IBM Cloud Internet Services](#), leveraging Cloudflare®, includes Domain Name Service (DNS), global load balancer (GLB), distributed denial-of-service (DDoS) protection, web application firewall (WAF), Transport Layer Security (TLS), and caching to bring market-leading security and performance to your internet applications.

IBM Cloud Internet Services was included, along with example usage and process flow, in this guide in [Section 3.2.1, “IBM Cloud VSIs and Bare Metal Servers”](#) as well as [Section 3.3, “IBM Cloud PaaS Architecture for PCI DSS.”](#) Additional information for PCI DSS use cases:

- **IP Firewall:** IBM Cloud Internet Services offers several tools for controlling the client’s traffic so that they protect their domains, URLs, and directories against volumes of traffic, certain groups of requesters, and specific requesting IPs.
- **IP Rules:** The IP Rules allow clients to control access for specific IP addresses, IP ranges, specific countries, specific ASNs, and certain CIDR blocks. Available actions on incoming requests are:
 - Whitelist
 - Block
 - Challenge (Captcha)
 - JavaScript Challenge (IUAM challenge)

For example, if clients notice that a specific IP is causing malicious requests, they can block that user by IP address.

- **User-Agent Blocking Rules:** User-Agent Blocking rules allow the client to take action on any User-Agent string they select. This capability works like Domain Lockdown as described previously, except the block examines the incoming User-Agent string rather than the IP. Clients can choose how to handle a matching request with the same list of actions as they have established in the IP Rules (Block, Challenge, and JS Challenge). Note that User-Agent blocking applies to their entire zone. The client cannot specify sub-domains in the same manner they can Domain Lockdowns. This tool is useful for blocking any User-Agent strings that are deemed suspicious.
- **Domain Lockdown:** Domain Lockdown allows the client to whitelist specific IP addresses and IP ranges such that all other IPs are blacklisted. Domain Lockdown supports:
 - Specific sub-domains. For example, clients can allow IP 1.2.3.4 access to the domain foo.example.com and allow IP 5.6.7.8 access to domain bar.example.com, without necessarily allowing the reverse.
 - Specific URLs. For example, clients can allow IP 1.2.3.4 access to directory example.com/foo/* and allow IP 5.6.7.8 access to directory example.com/bar/*, but not necessarily allow the reverse. This capability is useful when the client needs more granularity in their access rules. With the IP Rules, they can either apply the block to all sub-domains of the current domain, or all domains on their account, and they cannot specify URIs.
- **Challenge Passage:** Located in the Advanced security settings, Challenge Passage allows the client to control how long a visitor that passed a challenge or JavaScript challenge will gain access to their site before being challenged again. This is based on the visitor's IP and, therefore, does not apply to challenges presented by WAF rules, because they are based on an action the user performs on their site.

- **Browser Integrity Check:** Located in the Advanced security settings, the Browser Integrity Check looks for HTTP headers that are commonly abused by spammers. It denies traffic with those headers access to their page. It also blocks or challenges visitors that do not have a user agent, or who add a non-standard user agent (this tactic is commonly used by abuse bots, crawlers, or APIs).
- **Disable Content Caching:**
 - The origin server can set no-cache in the Cache-Control header for the regulated content.
 - The CIS Page Rules can be used to disable caching for any content on a specified path, even if the origin does not send a no-cache Cache-Control header.

More information on IBM Cloud Internet Services is available at [IBM Cloud Docs > Getting started with IBM Cloud Internet Services](#).

IBM Cloud Internet Services has a PCI DSS AOC Available. Applicable PCI DSS Requirements:

Build and Maintain a Secure Network and Systems	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Implement Strong Access Control Measures	<ol style="list-style-type: none"> 7. Restrict access to cardholder data by business need to know

4.2.8 IBM Key Protect for IBM Cloud

[IBM Key Protect for IBM Cloud](#) helps secure sensitive data from unauthorized access or inadvertent employee release while meeting compliance auditing standards. It provides mandatory control of user access requests to encryption keys and manages the entire lifecycle of keys from creation through application use, key archival, and key destruction. Key Protect provisions and stores cryptographic keys using FIPS 140-2 Level 3 certified (Federal Information Processing Standard) hardware security module (HSM) devices located within secure IBM data centers.

Clients can enable the security benefits of Bring Your Own Key (BYOK) by importing their own root of trust encryption keys, called Customer Root Keys (CRKs), into the service. With the Key Protect API, clients can use a CRK to wrap (encrypt) and unwrap (decrypt) the keys that are associated with data resources, for clients to control the security of their encrypted data in the cloud.

Key Protect does not process Payment Card Industry (PCI) information. However, Key Protect keys can be used to encrypt/decrypt data encryption keys used by data services to protect data which may include PCI data that is stored within the cloud.

Key Protect was included earlier in this guide in [Section 3.3.4, “Summary: Secure Flow for an IKS Application.”](#) Additional information for PCI DSS use cases:

4.2.8.1 Manage Access for Key Operations

Users and key access policies for creating, deleting, or rotating encryption keys are managed by the IBM Cloud IAM (identity and access) rules established when setting up an IBM Cloud account.

4.2.8.2 Securely Transport a BYOK

If using BYOK it is important to provide for secure transport of keys from on-prem into Key Protect. Key Protect offers two features to increase key transport security:

- Creating a transport encryption key for the Key Protect service instance. Transport keys are used to encrypt and securely import root key material into Key Protect based on the policies that the user specifies.
- Connect to Key Protect by using a private endpoint. This is accomplished by enabling virtual routing and forwarding (VRF) and service endpoints for the user infrastructure account. When VRF for is enabled for the user account, a user can connect to Key Protect by using a private IP that is accessible only through the IBM Cloud private network.

4.2.8.3 Use Secure Key Names

It is recommended to not to use any personal, financial, or health related information for the encryption key names. (“Key Name”: A unique, human-readable alias for easy identification of your key.) Key Protect has no mechanism to prevent sensitive information from being used in the key name. If it is necessary to import keys into Key Protect, verify that no part of the key contains PCI data.

4.2.8.4 Audit Key Operations with IBM Activity Tracker with LogDNA

All Key Protect API call logs are sent to the IBM Activity Tracker with LogDNA service where users and applications interaction may be monitored for abnormal activity.

More information about IBM Key Protect for IBM Cloud is available at [IBM Cloud Docs > Key Protect > Getting started tutorial](#).

IBM Key Protect for IBM Cloud has a PCI DSS AOC available. Applicable PCI DSS Requirements:

Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know

4.2.9 IBM Cloud Kubernetes Service

[IBM Cloud Kubernetes Service](#) is a managed container service for the rapid delivery of applications that can bind to advanced services like IBM Watson® and blockchain. As a certified K8s provider, IBM Cloud Kubernetes Service provides intelligent scheduling, self-healing, horizontal scaling, service discovery and load balancing, automated rollouts and rollbacks, and secret and configuration management. The Kubernetes service also has advanced capabilities around simplified cluster management, container security and isolation policies, the ability to design your own cluster, and integrated operational tools for consistency in deployment.

IBM Cloud Kubernetes Service was featured earlier in this guide in [Section 3.3, “IBM Cloud PaaS Architecture for PCI DSS”](#), with examples and configuration guidance throughout the subsections. To create an IBM Cloud Kubernetes Service cluster, follow these steps:

- Create an IKS cluster (standard subscription) on a dedicated virtual machine using the account.
- Select Classic infrastructure. Select hardware VM size based on workload. Select master service end point as Private end point only, and check the Encrypt local disk.
- Select OS (Ubuntu 16 or 18).
- For more details of how to create IKS clusters visit [IBM Cloud Docs > Creating Kubernetes clusters](#).

For the worker node and the PODs within them supplied by IBM, all fix packs and patches will be published by IBM. The client must apply these patches to ensure security compliance for their worker nodes.

The client is responsible for meeting all requirements of this section on any software components / applications that they deploy into the worker nodes.

Additional general information about IKS is available at [IBM Cloud Docs > Getting Started with IBM Cloud Kubernetes Service](#). Specific additional information and links are contained in the IKS sections below in this guide.

IBM Cloud Kubernetes Services has a PCI DSS AOC Available. Each item below will list the Applicable PCI DSS requirements.

Additional information for PCI DSS use cases:

4.2.9.1 Package a single process per container

A container is not a virtual machine, and, as such, the client should not package applications in the same way. IKS Containers are designed to have the same lifecycle as the application that it hosts, so each container should only contain one application. When the application stops, so should the container. Failure to follow this guideline can result in containers ending up in an unknown state, where core components have crashed or become unresponsive which in turn means that Kubernetes cannot tell whether the container needs to be restarted without additional health checks.

Applicable PCI DSS Requirements:

Build and Maintain a Secure Network and Systems	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Maintain a Vulnerability Management Program	6. Develop and maintain secure systems and applications

4.2.9.2 Do not run container processes as Root

Namespaces isolate processes that are running in one container from processes that are running in another on the same host system. By default, the user namespace for containers is the same as that of the host. Specifically, the root user inside the container is the root user of the host system, which means that if a process breaks out of the container sandbox it has the potential to compromise the entire host.

Therefore, where possible, applications in containers should not be run as root. This can be achieved by using the USER statement inside a Dockerfile and setting it to a number that does not correspond to an existing user on their worker node. Picking a value like '1001' would achieve this, with the end result being that if a process escapes the container; it would not have any permissions on anything on the host that it doesn't already own.

Applicable PCI DSS Requirements:

Maintain a Vulnerability Management Program	6. Develop and maintain secure systems and applications
--	---

4.2.9.3 Do not store secrets in Containers

Many applications might need secret information, such as private keys (including those for SSL certificates), encryption keys etc. Such secrets should never be stored inside a container image, its Dockerfile, environment variables, etc., because they are then available to anyone who pulls the image from a Registry (or can view the config of the running container). They should instead be stored in a secret management solution with the values mounted into the container at runtime, if needed.

Applicable PCI DSS Requirements:

Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
--------------------------------	--

4.2.9.4 Build the smallest image possible

To protect their applications from attackers, it is best practice to reduce the possible attack surface by including as little unnecessary software as possible. The best way to do this is to package single binaries in a scratch container, but where this is not possible the client should use a Linux distribution that is optimized to contain as little additional software as possible, such as Alpine, rather than a large distribution such as Ubuntu.

Applicable PCI DSS Requirements:

Build and Maintain a Secure Network and Systems	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Maintain a Vulnerability Management Program	6. Develop and maintain secure systems and applications

4.2.9.5 Monitor image vulnerabilities using IKS Vulnerability Advisor (VA)

IBM Cloud provides CLI and API access to VA for determining the number of known vulnerabilities in a given image stored in the IBM Cloud Container Registry service, as documented at [IBM Cloud Docs > IBM Cloud Container Registry CLI](#) and [IBM Cloud Docs > Vulnerability Advisor for IBM Cloud Container Registry](#). Application owners should periodically check the status of their images and remediate vulnerabilities as required.

Applicable PCI DSS Requirements:

Build and Maintain a Secure Network and Systems	2. Do not use vendor-supplied defaults for system passwords and other security parameters
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
Regularly Monitor and Test Networks	11. Regularly test security systems and processes

4.2.9.6 Restricting access to the environment and securing the network

All IKS containers are protected by [predefined Calico network policy settings](#) that are configured on every worker node during cluster creation. By default, all outbound network traffic is allowed for all worker nodes. Inbound network traffic is blocked, except a few ports that are opened so that network traffic can be monitored by IBM and for IBM to automatically install security updates for the Kubernetes master. Access from the Kubernetes master to the worker node's kubelet is secured by an OpenVPN tunnel. For more information, see the [IBM Cloud Docs > IBM Cloud Kubernetes Service architecture](#).

If the client wants to allow incoming network traffic from the internet, they must expose the apps with a NodePort service, a network load balancer (NLB), or an Ingress application load balancer (ALB). Learn more at [IBM Cloud Docs > IBM Cloud Kubernetes Service > Understanding Kubernetes service types](#).

Applicable PCI DSS Requirements:

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data

4.2.9.7 Authentication and Authorization

- Identity management for microservices is provided by Service Accounts. It is accepted practice to establish one account per application. When this is not unique to the end-user, the end-user and consumer account should be cross-referenceable in logs produced by the microservice. Please note, that PCI data should never be logged. Instead, logging the account and end-user should be such that logs can be cross referenced to stored PCI data.
- Password policy breaches are scanned for as part of Vulnerability Advisor (i.e. password older than 90 days, password length less than 8, etc.). You can set password readiness by adding the following to the Docker file:

```
RUN \
sed -i 's/^PASS_MAX_DAYS.*/PASS_MAX_DAYS 90/' /etc/login.defs && \
sed -i 's/^PASS_MIN_DAYS.*/PASS_MIN_DAYS 1/' /etc/login.defs && \
sed -i 's/sha512/sha512 minlen=8/' /etc/pam.d/common-password
```

- Container network accessibility should be limited by leveraging ingress/egress traffic rules in Kubernetes natively.
- Only private registries should be used to minimize tampering with sensitive data.
- An administrator needs to provision the IKS under their IBM Cloud account, and as such can define access policies for the Kubernetes cluster to create different levels of access for different users. For example, an administrator can authorize certain users to work with cluster resources while others can deploy containers only.
- Access to the control plane should be minimized to only those roles responsible for managing the Kubernetes cluster. These roles would not have privileges to access the worker node containers or microservices and, therefore, would not have direct access to PCI DSS data.
- IBM Log Analysis with LogDNA service can be used to store and analyze container logs and Kubernetes cluster logs that are collected automatically by the IKS in Public and in Dedicated deployments.
- IKS will retain logs for at least one year and they will be protected against unauthorized access. Clients can choose what events they want to log for their cluster and if and where to forward your logs to.
- SSH should be disabled into containers storing or processing PCI DSS data. Instead, use Kubectl exec to gain authorized access into a running container. This will provide the appropriate logging needed.

Each provider tenant must be isolated from one another. The underlying Container/Cloud Provider must ensure that adequate controls are in place to isolate tenants on all infrastructure including compute, storage and network.

Applicable PCI DSS Requirements:

Build and Maintain a Secure Network and Systems	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs
Implement Strong Access Control Measures	8. Identify and authenticate access to system components
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data

4.2.10 LogDNA services: IBM Log Analysis and IBM Cloud Activity Tracker

[IBM Log Analysis with LogDNA](#) and [IBM Activity Tracker with LogDNA](#) services offer easy to use and powerful log and event collection, search, and archive abilities. The services by default meet needs as simple as prototyping to enterprise complexity with regulated data. When using the offerings in certain environment it is recommended users review and take the relevant configuration steps helping ensure the service helps fulfill business needs.

LogDNA was included earlier in this guide throughout [Section 3.3, “IBM Cloud PaaS Architecture Examples for PCI DSS”](#). Additional information for PCI DSS use cases:

- **Setup Absence Alerting:** Absence alerting tests for the absence of data flowing into their service instance. If data is not flowing into the system, it may indicate an issue in the application or environment. Absence duration is unique to workload and can be customized within the UI.
- **Prepare a proper Object Storage location:** LogDNA can archive to client-configured IBM Cloud Object Storage. There are many ICOS configurations helping clients meet a variety of needs. Data may need to be replicated across Regions to meet business and regulated requirements. Alternatively, data may need to be restricted to certain locations to meet data locality requirements.
- **Setup Archival Logs:** Archive, when sent to the properly configured COS account, may provide the application or environment the necessary backup of data.

LogDNA as a service does not store an independent backup copy of client data.

More information about LogDNA is available at:

- [Cloud Docs > IBM Cloud Activity Tracker with LogDNA > Getting started tutorial](#)
- [Cloud Docs > IBM Log Analysis with LogDNA > Getting started tutorial](#)

The LogDNA services have a PCI DSS AOC Available. Applicable PCI DSS Requirements:

Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data
--	---

4.2.11 IBM Cloud Security Advisor

[IBM Cloud Security Advisor](#) enables centralized security management through a unified dashboard that alerts security admins to issues and guides them to understand, prioritize, manage, and resolve security issues that are related to their cloud applications and workloads.

- **Security risk and posture:** Application security remains important with constant news articles that announce a new data breach or hack. Security risks will always be a part of development and although attacks can be difficult to predict, one way to prevent them is by closely monitoring your cloud deployments. For example, the risks can be related to vulnerabilities in your container images that are in use, expiring certificates that can cause outage of your cloud service or application or suspicious clients or servers with a known bad reputation interacting with your clusters.

- **Centralized security management:** You can see a consolidated view of all of your IBM Cloud security services and integrated partner services. You can select and subscribe to different services from the IBM Cloud catalog.

Security Advisor was included in [Section 3.3.3, “IBM Cloud Kubernetes Service \(IKS\) Configuration”](#).

Additional configuration information and detailed tutorials are available in [IBM Cloud Docs > About Security Advisor](#).

Applicable PCI DSS Requirements:

Protect Cardholder Data	4. Encrypt transmission of cardholder data across open, public networks
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data

4.2.12 IBM QRadar on Cloud

[IBM QRadar on Cloud](#) is network security intelligence and analytics offering that can help clients detect cybersecurity attacks and network breaches in order to take action before any considerable damage is done or begin to immediately respond to any critical data losses. Security Information and Event Management (SIEM) insights help security teams accurately detect and prioritize threats across the enterprise, enabling quick response to reduce the impact of incidents.

IBM QRadar on Cloud was included in [Section 3.3.1, “Explaining PaaS Architecture components”](#). Additional information for PCI DSS use cases:

- All access to human readable sensitive data as defined by the PCI DSS should be attributed to a unique user. Ensure that your feeds to IBM QRadar on Cloud are capturing the right data.
- Any activity undertaken by a root or administrative user must be logged.
- Ensure your IBM QRadar on Cloud instance is time synchronized to the same authoritative source as the rest of your IBM Cloud resources.
- Limit the access to audit trails to those with a need-to-know.
- Implement file integrity monitoring on log files to ensure they cannot be illicitly modified.
- Store at least one year of logs.

Applicable PCI DSS Requirements:

Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data
--	---

5 Conclusion

IBM Cloud Platform offers a large number of key capabilities to support a client's PCI DSS-compliant environment. This guide addresses related issues.



Cloud security is a shared responsibility between the cloud service provider and its clients. IBM Cloud 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 Index: IBM Cloud Infrastructure and PaaS Offerings

A

Activity Tracker with LogDNA · 17, 29, 30, 36, 41
App ID · 11, 21, 29

B

Bare Metal · 7, 11, 12, 13, 23, 24, 25, 28, 34
Block Storage · 12, 13, 25

C

CDN · 13, 16
Certificate Manager · 18, 20, 21, 30
CFEE · 32
CIS · 13, 16, 35
Cloud Object Storage · *See* COS
Cloudflare · *See* CIS
Config Advisor · 20
Container Registry · 20, 21, 31, 39
content delivery network · *See* CDN
COS · 18, 25, 26, 41

D

DDoS · 13, 34
Direct Link · 12, 18, 26, 27
distributed denial-of-service · *See* DDoS

E

Event Streams · 31

F

File Storage · 12, 13, 25, 26
firewall · *See* Fortigate
Fortigate · 13, 16

G

GLB · 13, 34
global load balancing · *See* GLB

H

HSM · 17, 27, 28, 35

I

IAM · 10, 11, 16, 26, 29, 32, 33, 35
IBM Cloud Activity Tracker · *See* Activity Tracker with LogDNA
IBM Cloud App ID · *See* App ID
IBM Cloud Bare Metal · *See* Bare Metal
IBM Cloud Block Storage · *See* Block Storage
IBM Cloud Container Registry · *See* Container Registry
IBM Cloud Direct Link · *See* Direct Link
IBM Cloud File Storage · *See* File Storage
IBM Cloud Foundry Enterprise Environment · *See* CFEE
IBM Cloud Hardware Security Module · *See* HSM
IBM Cloud Identity and Access Management (IAM) · *See* IAM
IBM Cloud Internet Services · *See* CIS
IBM Cloud Kubernetes Service · *See* IKS
IBM Cloud Load Balancers · *See* Load Balancers
IBM Cloud Security Advisor · *See* Security Advisor
IBM Cloud Virtual Servers · *See* Virtual Servers
IBM Event Streams for IBM Cloud · *See* Event Streams
IBM Key Protect for IBM Cloud · *See* Key Protect
IBM QRadar on Cloud · *See* QRadar
IKS · 10, 14, 16, 17, 19, 20, 21, 25, 29, 30, 31, 35, 37, 39, 40, 42
Internet Protocol Fire Wall · *See* IP FW
Intrusion Detection System / Intrusion Prevention System · *See* IPS/IDS
IP FW · 13
IPS/IDS · 13, 16

K

Key Protect · 21, 26, 35, 36
Kubernetes · *See* IKS

L

load balancer · *See* Load Balancers
Load Balancers · 12, 28
Log Analysis with LogDNA · 40, 41
LogDNA · 17, 21, 29, 30, 36, 40, 41

Q

QRadar · 17, 23, 42

S

Security Advisor · 20, 41, 42
Security Information and Event Management ·
 See SIEM
SIEM · 17, 42

V

virtual server · *See* Virtual Servers
Virtual Servers · 11, 12, 13, 23, 24
VSI · *See* Virtual Servers
VSIs · *See* Virtual Servers
Vulnerability Advisor · 20, 39, 40

7 Disclaimers

© Copyright IBM Corporation 2020

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
March 2020

IBM, the IBM logo, ibm.com, and IBM Cloud 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.