WHITE PAPER

A Primer on PCI Compliance with Pivotal Cloud Foundry

By John Field

Table of Contents

Introduction 3
Demonstrating Compliance 3

Requirement 1 4
Interpretation for PCF 4
- Firewalls 4
- Cardholder data flows across networks 5
- Networking Roles and Responsibilities 5
- Justification for Services, Protocols, and Ports 6
- Limiting in- and out-bound networking traffic 6

Requirement 2 7
Interpretation for PCF 7
- Default accounts and passwords 7
- Maintaining Enterprise Configuration Standards 7
- Single Function Virtualization 8
- Minimizing Attack Surface 8
- Strong Encryption for Admin Access 8
- Tenant Isolation 8

Requirement 3 9

Requirement 4 9

Requirement 5 9
Interpretation for PCF 9

Requirement 6 9
Interpretation for PCF 10
Vulnerabilities Notifications 10
PCF's Vulnerability Management Program 10
PCF Defines and Enforces a Strict, Resilient Change Control Process 10

Requirement 7 11
Interpretation for PCF 11
- Controlling Access to Cardholder Data 11

PCF Capabilities to Verify Data Access Policies 11

Requirement 8 12
Interpretation for PCF 12
- Integrating PCF with an Enterprise IdM System 12
- Remote Access Authentication 12
- Access to Cardholder Databases 13

Requirement 9 13

Requirement 10 13
Interpretation for PCF 13
- Log All the Things! 13
- Application Logging 14
- Platform Logging 14
- Log Contents 14
- Time Synchronization 14
- Log Preservation 15
- Log Procedure Validation 15

Requirement 11 15
- Vulnerability Scanning 15
- Penetration Testing 16

Requirement 12 17
Interpretation for PCF 17

Conclusion 18

Appendix A: 19

Appendix B: 21

Introduction

This document provides a practical "how to" guide for customers that plan to deploy Pivotal Cloud Foundry (PCF), and need to comply with the requirements of the Payment Card Industry Data Security Standard (PCI DSS). The advice in this document is valuable to all PCF deployers and operators, but was specifically developed with the PCI DSS Level 1 category in mind. Any customers that plan to deploy the PCF platform as a component of their PCI Cardholder Data Environment (CDE) should review and follow this guidance.

It is important to recognize that as a general software platform, PCF itself cannot be assessed as being "compliant", or "not compliant" with PCI. Only an actual CDE—which may include a PCF deployment, along with all of the related technology infrastructure, and associated people and processes—can be assessed for compliance with PCI. The goal of this document is to provide Pivotal's customers, and their Qualified Security Assessors (QSAs), with the additional information they will need when assessing a CDE that includes a PCF deployment.

This document was initially developed by the PCF Security Engineering team with reference to PCI DSS v3.1, and was reviewed by TrustedSec, a certified Qualified Security Assessor company. It has been updated for PCI DSS 3.2, and the current release of PCF. While neither Pivotal, nor TrustedSec, can guarantee that any specific deployment of PCF will pass a PCI DSS audit, we believe that the guidance contained in this document should be sufficient to enable customers to properly configure their PCF deployment, and to be prepared to engage with their chosen QSA.

Demonstrating Compliance

As with other audit and compliance standards, satisfying the PCI DSS standard is not simply a matter of installing and configuring the software. Compliance with PCI requires both technical and non-technical controls to be in place. A generally recurring theme throughout the PCI standard is the need to demonstrate that the necessary technical controls exist within the CDE, and that these controls are being properly managed as a normal part of doing business. That is, the organization must show evidence that the necessary technical controls are active within the CDE. In addition, the organization must then show that the associated policies and management procedures are documented, in use, and known to the people who are responsible for maintaining these controls within the CDE. This is often summarized with the phrase "People, Process, and Technology." The scope of a PCI DSS audit will cover all three.

Requirement 1

Any organization that operates a CDE has a responsibility to protect their cardholder data from unauthorized access. That protection begins with a firewall. It is necessary to show that the organization has implemented a properly configured firewall infrastructure, and that they manage it correctly. The firewall infrastructure will serve to separate the "inside" zone from the "outside" zone, as well as separating the less sensitive inside zones, from the more sensitive ones. The CDE itself is considered to be the most sensitive of the inside zones.

The use of PCF should be considered orthogonal to the use of perimeter firewalls. PCF deployers should plan to review the locations and configurations of adjacent network firewalls, and assume that a similar level of application isolation will be required when deploying applications on PCF. Thus, the use of PCF does not obviate the need for a perimeter firewall, and with appropriate configuration, it should be compatible with any existing perimeter firewall.

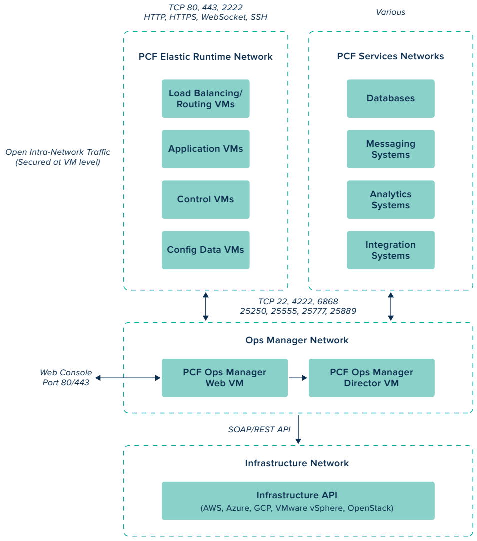
PCF deployments do require allocating a number of dedicated network subnets for the BOSH management network, the ERT, managed services, and other components. So, deployers should plan to architect their IAAS network accordingly.

The organization hosting a CDE must have a formal process for managing their firewall infrastructure, including steps for approving and testing any changes to the firewall(s). The process must be documented, in use, and known to the people responsible for maintaining the equipment. Verification of this is accomplished by reviewing the appropriate policy and procedure documents, interviewing the staff, and verifying the organization's record keeping for a sample of actual change requests.

Interpretation for PCF

Firewalls

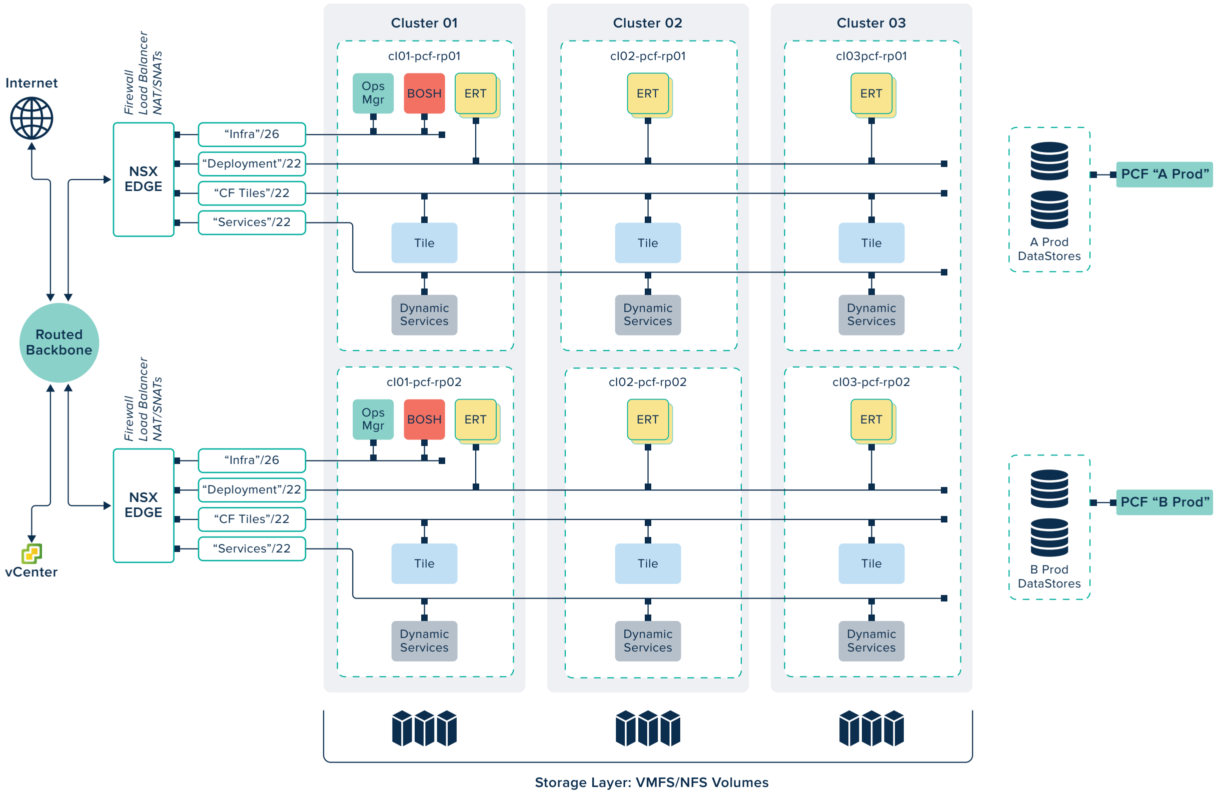
Sections 1.1.1, 1.1.4, 1.1.6, and 1.1.7 of this requirement are mostly out of scope for PCF. These sections concern the network infrastructure, and the people and processes that surround PCF. In general, Pivotal expects that customers will implement an appropriate firewall infrastructure, independent of their deployment of PCF.



Cardholder data flows across networks

Sections 1.1.2, 1.1.3, 1.1.5, and 1.1.6 have documentation requirements. The response to these sections needs to paint a picture for the QSA of all data flows within the CDE. It is important to note that section 1.1.2 requires an up-to-date network diagram that shows all connections between the CDE and other networks (including wireless if applicable). Section 1.1.3 requires an up-to-date diagram showing all cardholder data flows across all systems and networks. 1.1.5 is required to show a detailed description of all groups, roles, and responsibilities for the management of the network components in the CDE. Lastly, 1.1.6 requires documentation for all services, protocols, and ports used in the CDE and why they are needed.

The following figure illustrate the network connections required in a PCF deployment on VMware vSphere. It may be used as a starting point to satisfy these documentation requirements. This diagram is provided as a representative example only. Customers will need to adjust this generic diagram to reflect the exact configurations being used in their specific CDE. However, the level of abstraction and details captured here is typically considered the right starting point to satisfy these PCI requirements.



Additional reference architectures are available online.

Networking Roles and Responsibilities

Section 1.1.5 specifically concerns maintaining clear roles and responsibilities. The QSA must verify that the organization's IT policies and procedures provide clear lines of responsibility for properly maintaining network security. The goal is to avoid something falling through the cracks, because everyone thought it was someone else's job to maintain a particular piece of network gear.

Pivotal recommends that the organization must maintain an appropriate separation of duties between the roles of the PCF deployer, and the IaaS network manager(s). In particular, PCF is a user of the IaaS network. The PCF deployer must assign a specific CIDR subnet such as a 10.0.16.0/20 to the PCF runtime. This is done by obtaining a larger 10.0.0.0/16 allocation from the network team, and then carving up that /16 subnet appropriately, between the PCF Elastic Runtime, and the services network, and so on.

For the purposes of compliance with this section of PCI, it should be sufficient to review the appropriate policy and procedures document(s) to ensure that there are no ambiguities in the definition of roles and responsibilities surrounding the deployment of PCF. For example, the policy document could state, "The PCF operations team should only configure network information within the PCF deployment that has been approved and provided by the responsible network engineering team."

Justification for Services, Protocols, and Ports

Section 1.1.6 requires that the organization provide documentation to the QSA explaining why the organization uses the services, protocols, and ports that they use. Basically, the organization needs to provide evidence that the services running in production are there because a conscious business decision was made to enable them, and they are not there just by default, or by some accident, or negligence. PCF Ops Manager provides the enterprise with clear insight into all the VMs that are running in a deployment. For the PCF deployment, the BOSH manifest(s) serve(s) as the single source of truth; it is an authoritative reference that shows all the VMs, services (jobs) that are present, and provides QSAs with a complete inventory of what is in use.

A detailed view of these components is in Appendix B.

Limiting in- and out-bound networking traffic

Section 1.2.x requires that network access be limited into and out of the CDE as appropriate.

As described in the referenced tracker story, all application traffic into a PCF deployment should enter through the customer’s load balancer and the CF Router, running over TLS. All other inbound traffic should be rejected.

Outbound traffic from application containers is controlled with Application Security Groups (ASG). ASG rules are analogous to firewall “allow” rules. The operator must create explicit allow rules to enable connections between an application and its end user.

A QSA may use the Ops Manager application or the CF CLI to query what ASGs have been enabled for the CDE applications. A QSA may also use these tools to confirm that the associated protocols and port numbers are allowing egress to PCI-related resources only as appropriate.

As a general best practice, common allow rules should be configured at the Org level, while more specific allow rules should be configured at the Space level. However, to achieve PCI DSS compliance, the allow rules that permit access to the PCI-related resources should be defined only on the specific Orgs and Spaces needed for the CDE applications. Having these allow rules defined too broadly, such as at the Org level rather than at the level of a specific Space, can lead to an inadvertent loss of isolation.

Note that the QSA should audit the complete set of ASG rules. That is, the QSA must check that access to any PCI-related resources is limited to the identified CDE applications, and also that network access to PCI resources is **not** being granted to any non-PCI applications.

PCF supports the isolation of network traffic with Isolation Segments. Operators can use this feature to isolate deployment workloads into dedicated resource pools. Speak with your PCI auditor to see if this option makes sense for your deployment.

Requirement 2

A common technique for gaining unauthorized access to a system is to attempt to authenticate using default credentials. That is, to log in using an account that is present in the system when it is shipped by the supplier. It's also important to remove any old or unused accounts from production systems.

Interpretation for PCF

Default accounts and passwords

Requirements 2.1.a through 2.1.c concern not using any vendor supplied defaults for any credentials. The QSA is expected to review vendor documentation, interview staff, and test deployed systems in order to confirm that the CDE is in compliance.

PCF is compliant with this requirement. There are no default or "guest" user login ids present in the PCF deployment.

It should be noted that PCF requires a large number of credentials that are configured for inter-component authentication. These intra-system user accounts will exist on every PCF deployment, however the passwords for these logins are generated uniquely during the installation. That is, different deployments of PCF will have different values for these passwords. They are all machine generated, and long enough to be unguessable. These credentials cannot be obtained by searching the internet, or the vendor documentation.

Maintaining Enterprise Configuration Standards

Requirement 2.2 concerns configuration guidance for systems in the CDE. The QSA is expected to confirm the existence of enterprise configuration standards, interview staff, and examine the deployed systems to ensure that the configuration standards are actually in use. This requirement seems to imply that the organization is maintaining individual, standalone servers.

Of course, one of the benefits of the PCF platform is the consistency it provides when managing a large pool of compute resources. Customers no longer have to manage the configuration of individual machine instances, as Ops Manager and BOSH will do this for them, removing the chance of misconfiguration or out of compliance configuration by humans. With PCF, the configuration of any newly deployed VMs is determined by the stem cells contained in the BOSH release. The BOSH stemcells have basically been pre-hardened, and the site-specific configuration is limited to setting, e.g., the localized login banner text. In fact, if the configuration of any VM within

PCF were to drift, it would be corrected by BOSH at the next deployment. Thus, PCF provides an infrastructure that essentially obviates the need for manual configuration management. The intent of the requirement is to ensure that deployed systems are appropriately configured before they are deployed, and that the configuration is driven by industry best practices. PCF inherently provides this capability via Ops Manager and BOSH. Details of how the stemcell is configured can be found on the stemcell hardening docs page. It is recommended that the customer review and update any existing configuration guidance documentation to state that the configuration of any VMs contained within the PCF deployment are to be managed via PCF, and administrators should never perform manual configuration of these machines.

Single Function Virtualization

Requirement 2.2.1 concerns isolation. It states, "Where virtualization technologies are in use, implement only one primary function per virtual system component." The PCF platform infrastructure complies with this requirement. Each VM that is part of the PCF infrastructure—such as CF Router, UAA, or Ops Manager, or MySQL, or Diego, etc.—serves only one specific purpose. After all, complexity is the enemy of security!

Minimizing Attack Surface

The remainder of sections 2.2.2 and 2.2.3 are focused on minimizing the attack surface of the CDE. As discussed above, PCF satisfies these requirements by virtue of using Ops Manager, BOSH, and the associated deployment manifest(s) to ensure that each VM in the environment is always running in a known state, and to eliminate any configuration drift. If necessary, the customer may implement any additional security features via dedicated BOSH deployments (e.g. IPsec Add-on, ClamAV Add-on, FIM Add-on, etc.).

Strong Encryption for Admin Access

Requirement 2.3 states that all non-console administrative access must be protected using strong cryptography. PCF is compliant with this requirement. Section 2.3 requires that the QSA sample a number of system components in order to determine whether strong encryption (such as TLS v1.2) is being used to administer the platform. For PCF, this would include access to Ops Manager, BOSH, as well as the Apps Manager, and CF CLI tools. All of these interfaces provide administrative level functionality, and all support the use of TLS.

Documentation around PCF concepts and its security controls can be found on the Pivotal Cloud Foundry Concepts page. Additional information on security is available on the security concepts page. Documentation on the administrative permission model can be found on the Orgs, Spaces, Roles, and Permissions page.

Tenant Isolation

Finally, section 2.6 states requirements for multi-tenancy. In a nutshell, the intent of the requirements in section 2.6 (and Appendix A.1.1. through A.1.4) is to ensure appropriate isolation between tenants and workloads when a service provider infrastructure is hosting more than one organization. In general, the design of PCF enables the service provider to comply with all of these requirements.

Requirement 3

At the end of the day, it's all about the Card Holder Data (CHD). Any organization that processes credit card payments must take steps to protect the cardholder's Primary Account Number (PAN), the Personal Identification Number (PIN), and Card Verification Value Code (CVV2/CVC2/CID). PCI Requirement 3 discusses the specific steps that an organization must take in order to safeguard this sensitive cardholder data. The requirements include everything from having documented data retention policies, to appropriate management and use of encryption keys that protect CHD. These are some of the most important security requirements in the PCI DSS document. Application data is the responsibility of the application developer. PCF is responsible for its own configuration data.

PCF supports compliance in this area when the underlying IaaS disk encryption is enabled.

Requirement 4

While Requirement 3 was all about protecting data at rest, Requirement 4 is all about protecting data in transit. The goal is that sensitive cardholder data being transferred into or out of the CDE must not be visible to an attacker. The emphasis is on transmission over publicly accessible networks. Most of this section discusses using the recent versions of well known cryptographic protocols, and using them correctly. As with Requirement 3, this requirement is mostly out of scope for PCF. The choice to deploy PCF as part of the CDE should not have any material impact on the customer's ability to remain in compliance with Requirement 4.

Pivotal Cloud Foundry offers an optional module that may factor here: IPsec Add-On. The PCF IPsec Add-On encrypts all network traffic within a Cloud Foundry Elastic Runtime deployment, and prevents an unauthorized actor from observing data in transit.

Requirement 5

Requirement 5 involves maintaining anti-virus protection and preventing malware infections in the CDE.

Interpretation for PCF

It is unclear whether a QSA will require a deployer to install anti-virus software on the VMs within a PCF deployment. This is somewhat of a grey area, as it is up to the individual QSA to determine what constitutes a system that is "commonly affected by malicious software." A very good argument can be made that this is not necessary for PCF. However, if the assessor does require antivirus on Linux, PCF operators may deploy the PCF Add-on for ClamAV. If the operator prefers another antivirus solution, Pivotal also supports the installation of 3rd party agents on stemcells, as long as the agent is packaged as a BOSH release.

Requirement 6

Security is not a once-and-done endeavor. It's a repeatable process, like “Lather, Rinse, Repeat.” The focus of this requirement is on the lifecycle issues: vulnerability management, patch management, following secure software development practices, and having good change control. It is essential that organizations have an efficient and effective process to maintain the security posture of their CDE, even as new vulnerabilities are continuously discovered, and new patches for applications and systems become available. The intent is to ensure the ongoing security of the CDE in an environment of continuous change. In addition, this section requires the organization to conduct penetration tests at least annually, and after any significant changes to the environment. With the emphasis on life cycle processes, the burden of proving compliance for Requirement 6 will rest more on the CDE management team, rather than with PCF itself.

Interpretation for PCF

Section 6.1 requires the organization operating the CDE to establish a vulnerability management program. The scope of this requirement is primarily on the Pivotal customer. It is the PCF deployer's responsibility to establish a vulnerability management program, and to follow it.

Vulnerabilities Notifications

Pivotal supports our customer's efforts by maintaining a vulnerability management program of our own. As described in the PCF product documentation, Pivotal does continuous vulnerability scanning of the upstream Ubuntu OS stem cell images, as well as the PCF rootfs. Pivotal will publish security alerts categorized as "high," "medium," or "low," and will send e-mail alerts to all registered subscribers who have opted in to receive these security alerts. Any vulnerability that is reported to be high priority will be patched as soon as possible. Security vulnerabilities that are classified as medium or low priority will be patched in the next regularly scheduled maintenance release, which is done monthly. Customers that must maintain a vulnerability and patch management program for PCI compliance can leverage these Pivotal updates as one part of their compliance efforts. Thus, Pivotal provides all of the update services necessary to ensure that the PCF platform can be operated in a manner that is compliant with the lifecycle requirements specified in PCI section 6.1.

Pivotal recommends that the QSA acceptance procedure for section 6.1 and section 6.2 should begin with the QSA visiting the PCF product documentation, the Pivotal Network Web site, as well as the Pivotal Application Security Team page. These pages provide the resources needed to prove compliance with Requirement 6 for PCF.

PCF's Vulnerability Management Program

Vulnerability management is a business-as-usual process within Pivotal product teams, as demonstrated by the regular product updates that are being released. Pivotal follows modern agile best practices for software development, and documents its security-related policies and procedures for customers on the PCF docs security page. In addition, Pivotal has asked an independent 3rd party to conduct a penetration test of PCF, and all findings have been fed back to the respective product development teams, as stories in their respective backlogs.

In addition to Pivotal's internal efforts to produce secure software, it is a recommended best practice that customers deploy a 3rd party Web Application Firewall (WAF) as a supplementary control.

PCF Defines and Enforces a Strict, Resilient Change Control Process

Sections 6.4 and 6.4.5 require the CDE management team to follow strict change control procedures. For example, development and production environments must be separated by both procedural and technical access controls. The goal is to avoid outages or other security failures, whether inadvertent or deliberate. In support of these requirements, PCF provides role-based access control for users, and can partition resources within the PCF deployment based on the concepts of "Orgs" and "Spaces." In addition, the PCF platform itself is designed to provide continuous uptime, even during upgrades of the platform itself. PCF easily enables Blue-Green style deployments, which can help ensure no downtime during application upgrades, and assist with rollbacks. Independent of PCF, many organizations adopting PCF also chose to adopt Concourse as a tool for managing their continuous integration processes. In short, PCF has been designed in a manner that is consistent with the requirements of section 6.4. Actually ensuring compliance is ultimately the responsibility of the CDE management team, but adopting PCF and Concourse can make the job easier.

Requirement 7

This requirement can perhaps best be summarized by quoting the classic cliche, "That information is given out only on a need-to-know basis, and you have no need to know." This section is all about maintaining logical access controls in the CDE. The organization is required to implement controls to limit access to system components, and cardholder data, to only those individuals whose job requires such access.

Interpretation for PCF

Controlling Access to Cardholder Data

Sections 7.1 through 7.3 provide an extensive framework for managing access to cardholder data. The PCF platform provides a number of features that will support the organization's efforts to comply with these requirements.

PCF enables the organization to control access to resources in the platform via role-based access controls. Resources such as applications, and their bound services, are partitioned into logical groups called "Orgs" and "Spaces." Users can be added into the platform as members to one or more Orgs and Spaces, and then assigned specific roles such as Manager, Developer, or Auditor within a given Org and Space.

User identities can be introduced to the platform via integration with the existing enterprise Identity Management systems. Logins for PCF can be accomplished via UAA which is, in turn, backed by the existing enterprise LDAP or Active Directory. Logins may also be managed locally, within the PCF UAA database. Users may also authenticate to the platform via an industry-standard SAML v2 assertion, issued from a trusted IdP.

It is up to the management team to define and document the appropriate access management strategy for the CDE, and then use these PCF features appropriately.

PCF Capabilities to Verify Data Access Policies

Pivotal recommends that the QSA can use tools such as the CF CLI, the Cloud Controller API, and/or the Apps Manager application in order to gather the evidence needed to prove compliance with this requirement.

The QSA acceptance procedures to prove compliance with sections 7.1.4 and 7.2.x will include the steps of reviewing the written policy that describes who should have access to what, and then using the appropriate PCF tools to validate that the actual access controls match the written policy.

The PCI DSS recommends that the QSA review the documented policies, interview the staff, and then do sampling in the target environment. The PCF Apps Manager application provides a convenient GUI for manually inspecting the permissions and scope available to the users in the PCF environment. The QSA should log in as an Org Manager or Org Auditor role in order to inspect the permissions that have been granted to the member users within the given Org. The QSA should also observe a subset of those users logging into Apps manager as themselves, and confirm that the authorization profile available to those users meets expectations. The same information is also available via the CF CLI, and/or the Cloud Controller API. Using the the CLI or API, rather than the GUI, could potentially enable the QSA to automate assessments that demand large sample sizes.

Requirement 8

This requirement is all about enterprise Identity Management (IdM). The QSA must verify that the organization has the policies, procedures, and infrastructure in place to ensure proper authentication and authorization of all the people who have access to the CDE. As usual, requirements that are focused strictly on written policy and procedure will be out of scope.

PCF satisfies most of the remaining requirements out of the box, or via integration with the existing enterprise IdM system. In some specific cases, the native features of PCF alone will be insufficient to achieve compliance, and therefore the PCF deployment must be supplemented with additional procedural and technical controls.

Interpretation for PCF

Integrating PCF with an Enterprise IdM System

The requirements found in section 8.1.1 through 8.1.7 are focused on IdM policy and procedures. All the requirements for written documents, and adherence to these, are the responsibility of the CDE management. The remainder of the operational requirements can be satisfied by delegating PCF user authentication to the existing enterprise Identity Management system.

In particular, the UAA can can be configured to support integration with SAML v2, and/or LDAP and OpenID Connect providers. For example, an enterprise that has an existing SAML v2 identity infrastructure may configure UAA to accept a SAML v2 assertion from their trusted IdP. This enables the deployer to delegate the user authentication to the IdP. The IdP can, in turn, implement any required policies for password complexity, lifecycle management, and multi-factor authentication. The CDE applications themselves could and should also leverage the enterprise IdM system. They may do this directly, with some third-party support, or they may do this via integration with the PCF SSO service.

Remote Access Authentication

Requirement 8.3 concerns use of multi-factor authentication for non-console administrative access and remote access. As noted, PCF user authentication can and should be delegated to the enterprise IdM system. In particular, it is also important to consider protecting access to the PCF Ops Manager interface using two-factor authentication (2FA). Regardless of whether PCF is deployed inside the enterprise, e.g., on vSphere, or in a public IaaS cloud such as AWS, access to Ops Manager must be protected via 2FA, and a jump box. This interface could be a high value target for an attacker, and must be protected accordingly. In the case of AWS, it is recommended that the Ops Manager VM be deployed in a dedicated AWS security group. Access to this security group should be configured to allow connection only from the enterprise VPC gateway. Similarly, when PCF is deployed on vSphere, the Ops Manager VM must be deployed on a dedicated management subnet, access to which is protected via 2FA.

Access to Cardholder Databases

Requirement 8.7 covers access to cardholder databases. When a cardholder database is deployed outside of PCF (but perhaps accessed as a PCF user-provided service), the specific, dedicated credentials used by the application to access that database must be configured directly at the target database, and may then be configured in PCF by an authorized PCF user. The supplied credentials are then stored in the PCF Cloud Controller database and can only be accessed via authorized PCF users. The protection of the target database itself is out of scope for PCF.

When the cardholder database is hosted in PCF as a managed service, the feature set of PCF is sufficient to enable the CDE to achieve compliance. The database must be configured to be part of a specified Org and Space, and the people who are granted access to see the application's database credentials, and/or actually connect to the service endpoint, can be sufficiently restricted through a combination of logical access controls, and policy and procedure. The CDE management must ensure that application developers, or other end users do not have logins to the production CDE. Instead, access to the production CDE must be limited to, e.g., the continuous deployment pipeline, and associated operations staff. The QSA may assess these protections using the detailed acceptance procedures that are contained in the linked tracker story.

Requirement 9

This requirement focuses on the necessary physical security measures, such as issuing identification badges, using video cameras in sensitive areas, and having locks on the doors that control access to the data center. This section also requires that the organization maintain a visitor log, use temporary badges for visitors, and secure physical media (i.e. paper, disks, and tapes) to ensure data is not physically exfiltrated from the CDE.

We note only that PCF supports integration with LDAP or Active Directory, which enables an organization to provision PCF user logins via their existing enterprise Identity Management system. Depending upon the capabilities of the enterprise IdM system, this may also enable correlation of logical access controls within PCF, with any corresponding physical access controls that are managed from that same identity store.

Requirement 10

Requirement 10 covers logging. The scope of this requirement includes both the CDE applications, and the associated infrastructure components, such as PCF itself. The detailed requirements cover not only what must be logged, but also how the collected logs should be used, and how the lifecycle of the collected logs is to be managed.

Interpretation for PCF

Log All the Things!

Requirement 10.1 specifies the overarching requirement that logging needs to be enabled for all CDE system components, and that those logs need to track the actions of individual users. PCF provides a comprehensive set of logging features for both the platform itself, and the applications that it hosts.

Requirements 10.2.1 through 10.2.7 dig into all the details.

Application Logging

With respect to access to cardholder data, this logging will be the responsibility of the CDE application(s). Application logs that are generated within PCF are first written locally to the Diego cell (virtual machine) on which they were generated. PCF may be configured to stream all application logs to a third party log management system, such as Splunk, LogStash, or Papertrail, etc. The QSA must review the application log itself, in order to verify the completeness of the contents. In addition, the QSA must verify whether the necessary PCF platform configuration has been done in order to enable log streaming to a third party. Acceptance procedures for these steps have been included in the tracker story for requirement 10.2.1.

Platform Logging

Deployers may stream the platform logs to a remote syslog aggregator. The PCF platform logs are aggregated and streamed into the Loggregator, which should be drained to a provided syslog-compliant log archive such as Splunk, LogStash, etc. These logs capture all significant operational events that occur in the platform. Examples of log events included in this stream are add/update/delete actions on all objects native to the PCF environment, including Orgs, Spaces, Applications, Services, and so on. Security events are logged using the Common Event Format (CEF), and all user events (creation, successful / failed authentication, etc) are also logged. Logs are also kept on platform in intermediate buffers for configurable periods.

The PCF platform logs themselves are recorded in the Cloud Controller database. These logs will be retained for 90 days, giving the CDE management team enough time to backup or copy these logs off to secondary storage. These PCF platform logs may also be easily interactively queried via HTTPS at the Cloud Controller endpoint URL, /V2/events. The /v2/events endpoint provides a robust, RESTful API that enables any authorized caller to query and search the platform logs as needed.

Pivotal recommends that deployers leverage the capability to transfer the platform logs to a suitable 3rd party log management system, with associated archival storage.

Full documentation of this API and the necessary Ops Manager configuration steps are available for review.

Log Contents

Requirement 10.3 defines the detailed acceptance criteria for the contents of the logs being assessed. The QSA must confirm that these logs contain, at minimum: the user who performed the action, type of event, date and time stamp, disposition of the event (i.e. success or failure indication), the source of the event, and the target of the event. The PCF platform logs are in compliance with this requirement.

The contents of the CDE application logs are the responsibility of the application developer, and are out of scope for PCF.

Time Synchronization

Requirement 10.4 specifies that the CDE must use a standard time synchronization protocol. PCF supports the use of NTP, and is compliant with this requirement. A QSA acceptance procedure has been provided in the linked story.

Log Preservation

Requirement 10.5 states that audit logs must be preserved so that they cannot be altered. PCF provides a sufficient feature set to enable an organization to integrate PCF with a dedicated log management system. The acceptance procedure for the QSA to confirm integration of PCF with a third party logging system was covered in the tracker story for requirement 10.2.1. The QSA acceptance procedure(s) to confirm proper management and operation of the third party logging system are out of scope.

Log Procedure Validation

Requirements 10.6 , 10.7 and 10.9 relate to validating the operational procedures used by the CDE staff, and are out of scope for PCF. Requirement 10.8 is still considered best practice only, and is not considered enforceable until Feb. 1, 2019. In any case, PCF logging is currently sufficient to enable the CDE to comply with this requirement.

Requirement 11

If there is a vulnerability in the CDE software, we'd like to find it and patch it before it is exploited by an attacker. This requirement covers the need for regular vulnerability scanning to confirm the actual state of the systems deployed within the CDE. The first part of Requirement 11 concerns wireless networks, and so is completely out of scope for PCF (it is definitely not recommended that the PCF private subnet be a wireless network). The remaining sections cover regularly scheduled vulnerability scanning, penetration testing, and required intrusion detection capabilities.

Vulnerability Scanning

Section 11.2 concerns internal and external vulnerability scanning. The security team responsible for the CDE is expected to perform an internal vulnerability scan the PCF VMs (using, e.g. Nessus, Symantec, McAfee, Qualys, or some other equivalent) on a quarterly basis. As usual, all of the documentation requirements are out of scope for PCF, other than the fact that an enterprise's existing CDE policy and procedures documents may need to be updated to include PCF.

The PCF Elastic Runtime deployment is built using stemcell images which are based on the Ubuntu Linux OS. The Pivotal security engineering team performs standard scans of all PCF stemcell images for both configuration settings and vulnerabilities before they are shipped. As new vulnerabilities are identified, Pivotal issues updates to the stemcell images on a regular basis. Pivotal recommends that before performing a scan, the CDE security team confirm the specific Ubuntu stemcell release version that is used in their PCF deployment, and use the appropriate benchmark version. Running a more recent benchmark against an older deployment will result in false positives, and other invalid results.

There are two additional issues to be aware of when performing the internal scans against a PCF deployment. The first is that IP addresses within a PCF deployment are not static, and are not guaranteed to remain stable over time. One of the benefits of the Pivotal Elastic Runtime deployment is to make optimal use of the available physical resources. An organization may choose to scale the number of hosts being used for a specific function or application deployment, either up or down. For example, from one quarter to the next, the range of IP addresses used for Diego cells may grow or shrink. This may affect the range of IP addresses that are in use as part of the PCF deployment. Because IP addresses assignments are not guaranteed to be static and/or stable, the QSA must use care when attempting to correlate quarterly reports that may have been sorted based on IP address.

In addition, Pivotal recommends that any internal scanning of PCF VMs be done using a remote, authenticated scan whenever possible. The credentials needed to authenticate to any VM within the deployment will be available via the Ops Manager interface. The security team may collect the required SSH credentials for each of the targeted VMs, and configure these in their scanning tools, as appropriate. Deployers may also choose to use an open source BOSH Add-on such as os-conf-release in order to customize the user logins that would be used for a remote authenticated scan. As noted, the installation of 3rd party agents is also supported via the creation of a BOSH Add-on release, but would be the responsibility of the deployer.

Finally, it should be noted that the routing and/or firewall rules of the IaaS network configuration may need to be adjusted to allow the internal network scan of the PCF Elastic Runtime private subnet. It is a security feature of PCF that all traffic must normally traverse the CF Router as the front door to the cloud. Any direct access to the individual VMs and ports inside the cloud is normally denied. Therefore, in order to perform the scan, the CDE security team should work with their network team to ensure that the machine(s) initiating the scan will be able to reach the target VM addresses within the PCF deployment.

Penetration Testing

Requirement 11.3 states that a penetration test must be conducted. Pivotal has contracted a qualified third party to perform a penetration test of Pivotal Cloud Foundry. The results of that testing have been reviewed with the responsible engineering teams, and stories have been added to their respective backlogs, as needed.

Pivotal requests that if any security issues with PCF are identified, these should be immediately reported to security@pivotal.io.

Requirements 11.4 and 11.5 discuss intrusion detection and prevention measures. Pivotal recommends that customers deploy the PCF Add-on for File Integrity Monitoring. This solution can be used to monitor all critical files on the stemcell filesystem, and ensure that any unexpected changes will not go unnoticed by the operator. Any changes to the monitored files and/or directories will be detected in real time, and detailed messages will be sent to syslog. Enterprise security teams may configure appropriate security alerts using their existing log monitoring solution.

It should be noted that because the FIM Add-on will monitor all critical stemcell directories across the platform, any action involving a BOSH deploy (or Ops Manager “Apply Changes” action) may generate corresponding FIM events. These alerts on changes to the platform would of course be expected, and operators should plan accordingly. On the one hand, these FIM alerts may serve as confirmation that the deployment is proceeding. Operators might also choose to suppress these alerts as redundant, in order to avoid the false positive detection.

Finally, the standard Linux audit daemon has been included in the BOSH stemcell image, and the Linux audit rules have been configured with a robust set of rules. Enterprise security operations teams may monitor syslog for Linux audit events.

Requirement 12

Requirement 12 is a comprehensive statement of process and policy and procedure requirements in an organization that takes information security seriously. We need to consider how complying with Requirement 12 may be different after a customer adopts PCF as part of the CDE. In general, the decision to move to a PaaS based environment may be driven by the application delivery team, but it implies a commitment to update procedures and train staff in adjacent functions, such as change management, audit, and incident response.

Interpretation for PCF

Policy and procedure documentation is understood to be an essential part of all information security control standards, and management frameworks, such as PCI DSS v3.2, NIST 800-53r4, or the ISO 27000-series publications. In short, information security policy documents provide the business basis for the security controls that are deployed. In addition, the enterprise's procedure documents describe the actual work processes to be performed, given the chosen technical controls.

A well-written information security policy document will be independent of any particular implementation technology, and should not need to be updated when a new technology is deployed. However, enterprise information security procedures are frequently technology-specific, and these will need to be updated when a new tool or platform is deployed. This is particularly true in the case of PCF. Adopting a cloud native approach to application deployment implies that the enterprise is choosing to make significant changes to existing operational procedures. The enterprise dev-ops team should be plan to invest in updating procedure documents, such as: DR plans, incident response plans, operations run books, and so on, if and as needed. This is a non-trivial—but often overlooked requirement—in satisfying an information security compliance audit. Basically, all existing policies and procedures will need to be reviewed to make sure they are "PCF-aware," if and as appropriate.

For example, section 12.7 states that an organization must have an existing policy or procedure concerning the screening of employment candidates, in order to reduce the risk of insider attacks. It's safe to say that policy will not be affected by the adoption of PCF, and can remain unchanged.

On the other hand, section 12.5 defines the responsibilities of an information security team, including incident response. It is very possible that an organization's incident response plan may need to be updated to accommodate the adoption of PCF. Customers should review their existing incident response procedures to verify whether the workflow processes they describe will fulfill their intended purpose in a PCF environment.

As a simple example, consider what would happen if an administrator is responding to a security incident in a CDE application, and the approved response procedure includes shutting down the VM in question. If this is done out-of-band, i.e., by directly logging into a VM, the results will not be as expected. PCF will notice that the application is no longer available, and will take the necessary steps to resurrect it. This may come as a surprise to a security administrator who is unfamiliar with PCF. Of course, this is not to say that it is impossible to shut down an application in PCF. Rather, the incident response team needs to be re-trained on how to accomplish application shutdown using the appropriate interface, such as CF CLI, or PCF Apps Manager.

As another example, it is possible that an organization's existing risk management plan may include a provision to reassess the CDE whenever there is any significant change to the infrastructure. In a traditional ITIL-based management framework, the phrase "significant change" may reasonably be understood to include the (re-)allocation of the IP address assigned to a dozen different applications. However, in a PCF environment, this is a non-event—just routine operations. The Cloud Controller and Diego will stage and deploy an application to any available diego cell. There is no expectation that a given application will be assigned the same IP address and port forever. Instead, it is the PCF route that should be considered stable. Thus, that ITIL-based risk management policy may have to be amended to become a "PCF-aware" policy.

Because Requirement 12 addresses management concerns rather than technical controls, there are no specific stories being maintained in the Pivotal PCI tracker. However, a corresponding tracker epic has been created as a placeholder, and suggestions on specific stories that may help PCF adopters to satisfy Requirement 12 are always welcomed.

Conclusion

As with all compliance programs, achieving compliance of Pivotal Cloud Foundry with the PCI DSS standard is not just a technical question. Rather, it is a matter of people, process, and technology. In this paper we have described how to interpret the PCI DSS requirements in the context of a Pivotal Cloud Foundry deployment, and how to work with your chosen QSA to prove compliance. For requirements that are considered out of scope, we have explained why that is the case. For requirements that concern documented policies and/or procedures, we have explained how those documents may be impacted by the adoption of PCF. Finally, for the requirements that are in scope, we have provided a discussion of how PCF satisfies the requirement, and how the QSA can gather the evidence that proves compliance.

As with all compliance programs, this is a living document that we expect to evolve over time. One of our goals in publishing this document is to encourage collaboration within the community. If you have suggestions for how to make this document better, such as identifying a better or cheaper compensating control, or a shorter acceptance procedure, and so on, please contribute! The PCF Security Team would like to make customers that need to comply with PCI DSS successful, and we recognize that the best way to do that is to openly collaborate.

Appendix A:

Supplementary and Compensating Controls

The following table summarizes some additional controls that customers may choose to implement as part of deploying PCF in the CDE. These are suggested controls to enhance the security of the PCF deployment. When used to meet or exceed the original PCI DSS requirement these are considered compensating controls, otherwise they are identified as supplementary controls.

REQ.	ADDITIONAL CONTROL	TYPE	DISCUSSION
2.2	BOSH + stemcell ensures consistency in the deployment. BOSH maintains, and provides protection against configuration drift. The stemcell is hardened by Pivotal and may be scanned using Nessus or similar tool.	Supplementary	Stemcell configuration is follows Ubuntu 14.04 LTS, but has been tailored for tailored for cloud-native platform deployment.
2.2.3	BOSH + Stemcell ensures consistency in the deployment. PCF private subnet is restricted and not an open, public network. Deployers can also use IPsec BOSH Add-on, to implement encryption across all platform-managed VMs.	Compensating	Protects all IP traffic in the PCF private subnet, including HTTP, TCP, and UDP.
2.3	Use certificates issued from the enterprise CA or a well-known, public CA.	Supplementary	None.
4.1.x	Use only approved algorithms and protocols. Same as 2.2.3, and 2.3	Supplementary	None.
5.1 5.2 5.3	Deployers may install the PCF Add-on for ClamAV, or their favorite antivirus agent (packaged as a BOSH release).	Supplementary	Enterprise should deploy a local mirror for keeping antivirus signatures up to date. This is not part of the BOSH release.
6.3 6.6	Install a Web Application Firewall in front of Ops Manager and/or Apps Manager.	Supplementary	Pivotal recommended best practice. Required control when these interfaces are accessible externally.
6.5.3	Regenerate credentials via periodic redeployment.	Supplementary	Recommend using a Concourse to enable continuous deployment of both the platform and applications.
8.2.1	Use IaaS provided disk encryption to protect credentials in BOSH manifest in BOSH Director VM.	Compensating	PCF also natively supports AWS EBS and S3 encryption.
8.5.x	Install Ops Man on restricted management subnet. Require 2 factor authentication via PAM integration for all Ops Man users to access, e.g., the jump box. Deploy UAA integration for BOSH and Ops Manager. Ensure that /v2/events log is correlated to SSH authentication time at jump box.	Compensating	Recommended best practice.

10.2.3	Ensure that the PCF deployment is configured to send all platform syslog output to a highly available syslog endpoint.	Supplementary	Choices include platform logs directly via syslog, or Firehose log which can include all platform and application logs, or individual application log drains.
11.5.x	Install PCF Add-On for FIM to enable file integrity monitoring.	Compensating	Similar to ClamAV antivirus Add-on. Deployers may also choose to deploy other 3rd party agents, packaged as a BOSH release.

Appendix B:

A Summary of Services present in a Pivotal Elastic Runtime v.1.11.x.x deployment.

PCF JOB	FUNCTIONAL DESCRIPTION
Consul	Service discovery
NATS	Message bus for system components
etcd	Distributed configuration service
Router	Application request routing
Cloud Controller	Workload provisioning management
Clock Global	Time synchronization
Cloud Controller Worker	Workload provisioning capacity
UAA	Authentication and authorization
Diego Brain	Workload management
Diego Cell	Workload capacity (x N instances)
Diego BBS	Diego persistence subsystem interface
Doppler Server	Log forwarding agent
Loggregator Traffic Controller	Log management subsystem
Ops Manager	Web-based management console
OM Director	Platform operations service
OM Director DB	Platform operations database
CredHub	Management for user-generated and system-generated credentials