

Preparing an RFI for Virtualization and the PCI Data Security Standard

Protecting cardholder data is a critical and mandatory requirement for all organizations that process, store or transmit information on credit or debit cards. Requirements and guidelines for securing cardholder data are specified in the Payment Card Industry (PCI) Data Security Standard (DSS) version 2.0. This international standard is maintained by the PCI Security Standards Council, whose founding members include American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. The card brands have incorporated PCI DSS as part of the technical requirements for each of their data security programs. Organizations subject to PCI DSS must deploy appropriate technical controls and processes to ensure security of cardholder data and verify compliance with the standard.

Virtualization technology can help organizations simplify compliance with PCI DSS with scope reduction. It entails segmenting the cardholder data environment from an entity's other information systems. To help evaluate virtualization solutions for PCI DSS compliance, HyTrust recommends that your organization solicit vendor product and/or service-related input with a formal Request for Information. The RFI invites responses to questions for each Requirement of the PCI DSS with a focus on addressing security issues with virtualization. The suggested format below includes relevant RFI templates that may be copied or adapted to particular requirements of your organization.

RFI Format

- 1. Your Standard RFI Introduction Boilerplate**
- 2. Project Scope**
- 3. Proposal Profile & Qualifications**
- 4. Capabilities for Requirements of PCI DSS 2.0**
- 5. Your Standard RFI Closing Boilerplate**

2. Project Scope

Describe your organization's goals for virtualization, especially pertaining to compliance with PCI DSS. The Project Scope section should include specific technical objectives of special interest to your organization. Bulleted objectives in the RFI Template are examples of typical security issues related to virtualization.

RFI Template:

Our organization is evaluating virtualization technology for use in the cardholder data environment. It's important that the solution you propose will enable compliance with the PCI Data Security Standard v2.0. Your response to this Request for Information must address all Requirements of the PCI DSS v2.0. Information about the solution must pertain to our organization's IT infrastructure and its associated virtual environment. Information must address risks to our ____ network devices, ____ production servers, ____ applications, and to our virtualization components, which include ____ virtual machines, ____ virtual switches, ____ distributed virtual switches, ____ virtual portgroups, ____ virtual appliances, ____ virtual datastores, ____ virtual templates, ____ hypervisors, ____ virtualization management servers, and ____ virtualization management clients. These assets are located in [describe cities, states, countries, continents]. Virtualization technologies include VMware vSphere platform [describe additional virtualization technologies]. Our technical objectives include:

- Protect cardholder data wherever it is processed, stored, or transmitted in our virtual cardholder data environment, whether on our infrastructure or by a service provider.
- Address PCI DSS controls on all Virtual Machines (VMs), located on any host or network.
- Create 24x7 visibilities on virtual security and compliance status by extending compliant logging capability throughout the virtual environment.
- Integrate alerts for virtual resources with our legacy IT security and management systems.
- Ensure that hypervisor configurations are strictly controlled throughout the virtual environment, and implement automated configuration management.
- Monitor and manage all virtual access.

3. Proposer Profile & Qualifications

The complexity of solutions for virtualization and PCI DSS compliance requires that vendors demonstrate technical and

operational qualifications for their manufacture, deployment, and ongoing support. Questions are similar to what you would ask of any vendor proposing to play a significant role in your IT operations.

RFI Template:

Provide the following Profile & Qualifications information:

- Primary contact
- Description of company
- Primary business
- Virtualization-related products and services for PCI DSS compliance
- Date and country of Proposer's incorporation
- Registered office address and company registration number
- Location of headquarters
- Details about ultimate holding company, such as that listed on a publicly traded stock exchange
- Number and location of offices worldwide
- Number of staff worldwide
- Number of staff worldwide related to security
- List industry awards and recognition
- Provide assurance about financial stability of your company
- Number of virtualization-related customers
- Three reference customers similar to our business area and scale

Firm Qualifications: Describe length of time your company has provided virtualization products and/or services for PCI DSS compliance along with related specific experience in our industry. Illustrate your company's unique attributes or competitive advantages that distinguish it from other firms. Provide specific descriptions of your company's competence relating to virtualization security and compliance with PCI DSS.

Engagement Team Qualifications: Provide job level and names of firm personnel who would be involved with our deployment and ongoing support. Include profiles of key engagement personnel, resumes, certifications, and narratives describing industry experience and other qualifications. List number of virtualization security deployments in which each team member has participated.

4. Capabilities for Requirements of PCI DSS

Requirement 1: Install and maintain a firewall configuration to protect cardholder data.

Firewalls are vital for controlling traffic into and out of an organization's network – including internal segments related to the cardholder data environment. Legacy firewalls and related management solutions do not automatically extend to virtualized security zones and their related virtual firewalls and other virtual network devices. Technical controls are thus required to validate the configuration of a virtual firewall, and to detect and alert if tampering occurs.

RFI Template:

Describe how your solution relates to installation and/or maintenance of virtual firewalls. Detail the role of your offering with respect to the creation of virtual segmentation for cardholder data processing, storage, and/or transmission. This could include logical policy based infrastructure segmentation, virtual NICs, virtual switches, virtual port profiles, VLANs and pVLANs, virtual firewalls, and other components used to establish and manage segmentation and protection of cardholder data.

Specific issues to address for Requirement 1:

- Describe your virtual firewall capabilities.
- Describe the process for determining where your solution places virtual firewalls in the network system.
- How does your solution enforce infrastructure segmentation based on policies? Does your solution provide protection from VM escape or VM hopping? Does your solution provide cardholder data protection on the network packet level, for example, how does it discriminate against inappropriate and/or malicious traffic using networking communications effective for the environment (e.g., if bridging is used instead of routing).
- How does your solution prevent tampering with and/or disabling virtual firewalls?
- Describe how your solution prevents the accidental or non-authorized act of turning power off on servers running virtual firewalls?
- How does your solution integrate with legacy firewalls and firewall management systems?
- Provide details of your role-based management capability for virtual firewalls.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

Trying default passwords is the easiest way for hackers to access your cardholder data environment. Some vulnerability management tools can spot the use of default passwords, but their capability may

stop with virtual environments where entire networks of virtual machines are hidden from legacy solutions. The use of virtualization in the cardholder data environment also requires password controls for hypervisor and virtual infrastructure management utilities.

RFI Template:

Describe how your solution for provisioning virtual system components ensures that their default settings are correctly changed prior to deployment in the cardholder data environment. Explain how your controls harden hypervisors and manage device configurations in virtual infrastructure. Detail how your solution protects its vault of stored passwords and configuration data.

Specific issues to address for Requirement 2:

- Describe how your solution provides root password vaulting to eliminate the need for our administrators to know root passwords.
- How does your solution support the implementation and assurance of a secure configuration baseline for the hypervisor hosts?
- Describe how your solution uses industry best practices to govern how it hardens hosts and VM containers.
- How does your solution monitor configuration drift in the hardening posture of any virtual device?
- Explain the automation processes controlling remediation of non-compliant hosts.
- Requirement 2.2.1 notes: "Where virtualization technologies are in use, implement only one primary function per virtual system component." Does your solution comply with this requirement? If not, explain how your solution will comply as a Compensating Control.

Requirement 3: Protect stored cardholder data.

Cardholder data is all information printed, processed, transmitted or stored in any format on a payment card. The PCI DSS urges no storage of cardholder data unless absolutely necessary, and deleting it immediately after use is a safe precaution. However, deletion is challenging to verify in a virtualized environment with VM mobility, data replication, and storage virtualization spreading cardholder data across connected storage subsystems. Secure deletion requires perfect knowledge of the location of all data copies. The process of secure deletion is only possible through the destruction of entire storage arrays or erasure of encrypted storage keys. It's mandatory to make all stored cardholder data unreadable by using encryption or tokenization and key management. It's much easier to "delete" Virtualized stored cardholder data by erasing the associated key.

RFI Template:

Describe how your solution ensures that stored cardholder data is protected in a virtual environment. Explain how the solution tracks where cardholder data is actually stored in the virtual environment - including virtual disk and virtual memory. Describe how the solution effectively deletes cardholder data stored anywhere in a virtual environment.

Specific issues to address for Requirement 3:

- How does your solution address the problem of "remnants" of stored cardholder data on virtual resources? For example, memory that was previously stored only as volatile memory can, in virtual systems, be written to disk as "stored" by taking snapshots of systems. Describe how your solution knows that there are no remnants of stored data in virtual systems.
- How does your solution protect data exposed on internal networks, such as memory data transmitted during VMotion or on the connections to distributed storage such as NFS.
- How are cardholder data in virtual memory resources and other shared virtual resources protected from unauthorized access?
- Describe how your solution prevents unauthorized snapshotting of VMs in the cardholder data environment.
- Explain how your solution ensures deletion of cardholder data stored on virtual systems that are powered off.

Requirement 4: Encrypt transmission of cardholder data across open, public networks.

Virtualization flattens the data plane architecture. With virtualization, network layer encryption must therefore extend to the virtual NIC or be supplemented by additional control to prevent eavesdropping on the virtualized network. The hypervisor also presents an attack surface through which encryption technologies may be bypassed. Privileged access must be audited and controlled via virtualization-aware technologies.

RFI Template:

Describe how your solution provides encrypted transmission of cardholder data across open, public networks. The solution must address encryption in a virtualized environment where the network layer extends into the virtual NIC and hypervisor.

Specific issues to address for Requirement 4:

- Describe how your solution addresses encryption in a virtualized network environment.
- How does your solution prevent eavesdropping through virtual system components prior to encryption of cardholder data?
- Describe how your solution protects traffic between its management console and virtual system components.

Requirement 5: Use and regularly update anti-virus software or programs.

To comply with Requirement 5, your anti-virus software and signature updates must track the virtual machine lifecycle. Virtual infrastructure may be sensitive to performance issues associated with scheduled scan activities.

RFI Template:

Describe how your solution will help us to use and regularly update anti-virus software or programs deployed in a virtual cardholder data environment.

Specific issues to address for Requirement 5:

- How does your solution distinguish whether virtual system components in the cardholder data environment are commonly affected by viruses and other malware, or if they are not susceptible to those risks?
- How does your solution identify virtual systems that have changed configurations, and require an anti-virus software or signature update?
- Describe how your solution ensures that anti-virus software on virtual system components in the cardholder data environment is properly configured and running the most recent version of software and signatures?
- What process does your solution follow for distributing patches to virtual system components?
- How does your solution protect VM management servers in the cardholder data environment?
- How will implementing your solution for updating anti-virus software or programs affect performance of our virtual infrastructure?

Requirement 6: Develop and maintain secure systems and applications.

Legacy vulnerability management does not automatically integrate with virtual asset and infrastructure databases. It is infeasible to assure vulnerability management without tight integration with virtualized asset configuration and inventory. Change control processes must be updated to support virtual machine mobility and

provisioning. Application security must be integrated with virtual infrastructure inventory controls.

RFI Template:

Describe how your solution will help us develop and maintain secure virtual systems and applications for our cardholder data environment. Explain how your solution helps support the related processes of creating, implementing, and maintaining the virtual environment hosting cardholder data and related applications.

Specific issues to address for Requirement 6:

- How does your solution address the problem of “VM Sprawl,” which is creating more VMs than are necessary? Specify how your solution controls the building, copying, placement, and deletion of virtual images in the cardholder data environment?
- Explain how your solution controls who can power off VMs, move VMs to different hosts, and connect VMs to different networks.
- How does your solution support backup up of cardholder data in virtual systems?
- Describe how your solution supports the virtual systems component of disaster recovery and business continuity.

Requirement 7: Restrict access to cardholder data by business need to know.

Legacy access control systems do not automatically comply with Requirement 7 within the virtualized data center. System and application level access controls must be enforced throughout the virtualized cardholder data environment.

RFI Template:

Access controls are an essential element for compliance with Requirement 7. In a virtual cardholder data environment, access controls are necessary for hosts, applications, virtual components, and storage of these components before provisioning. Describe how your solution provides these controls for compliance.

Specific issues to address for Requirement 7:

- How does your solution limit access to virtual system components and cardholder data only to those individuals whose job requires such access?
- Describe access controls provided by your solution for each virtual system component. Are they set to “deny all” unless specifically allowed?
- Detail the multi-factor authentication capability provided by your solution.

- Explain how your solution's access controls operate for different security zones in the virtual cardholder data environment.
- Specify granular capabilities for role-based and workload-based access and management.
- How does your solution control access by authorized administrators such that none are able to log into virtual systems as "administrator" or "root?"
- How does your solution enforce separation of duties for access to virtual servers as opposed to virtual networks? Ditto for separating virtual backup administration from management of virtual servers and management of virtual networks.
- Explain how your solution controls access to hypervisor management, particularly for restricting local access for administrators to hypervisor management via centralized console access only.
- Describe logging capabilities for every administrative access attempt (whether allowed or denied).

Requirement 8: Assign a unique ID to each person with computer access.

Legacy Identity and Access Management systems do not properly protect virtual data center management, particularly for "headless" hypervisors such as VMware ESXi. Secure access policy management must include capability for virtual inventory controls.

RFI Template:

Describe how your solution ensures that every action affecting security of the virtual cardholder data environment can be traced back to a specific individual.

Specific issues to address for Requirement 8:

- How does your solution assign all users a unique user name before allowing them access to virtual system components or cardholder data?
- Specify the directory service used by your solution for authenticating administrator and user access to virtual systems in the cardholder data environment.
- What directory service is used when a virtual cardholder data environment is hosted by a cloud provider as opposed to a private cloud hosted on our in-house resources?
- Describe how your solution stores privileged account (root) passwords for all protected virtual hosts. Are these passwords perpetual or granted on a temporary basis to one individual at a time?
- Describe the multi-factor authentication used by your solution, and its integration capabilities with AD, RSA SecurID, and Smart Card.

Requirement 9: Restrict physical access to cardholder data.

The virtual infrastructure client may allow remote users unrestricted physical access to virtual machine files. Remote network access to the hypervisor service console, CLI, storage management, or Virtualization Management Console may be exploited to grant a remote user the equivalent of physical access to virtualized systems. Traditional physical access controls also must be implemented and enforced for systems hosting virtual services for cardholder data.

RFI Template:

Restricting physical access to virtual systems that process, store or transmit cardholder data is the heart of Requirement 9. However, physical access control may be circumvented if physical access to a hypervisor enables logical access to other virtual components and storage in the cardholder data environment. Describe how your solution protects against these vulnerabilities.

Specific issues to address for Requirement 9:

- Describe how controls in your solution prevent access from a hypervisor to root passwords stored in the virtual cardholder data environment's Identity and Access Management system.

Requirement 10: Track and monitor all access to network resources and cardholder data.

Legacy network security systems are unable to track asset and infrastructure access events between virtualized components residing within individual hypervisor nodes. This will result in a critical visibility gap across the virtual data center. Legacy audit systems do not provide fine grained auditing and controls for hypervisor management events, nor do they support virtual system forensics. Traditional application and system logs must be securely maintained for the virtual cardholder data environment.

RFI Template:

Robust logging is the key to complying with Requirement 10. However, many virtual system components do not provide logging capability on par with their physical counterparts. This is particularly true in systems designed for troubleshooting, as they provide insufficient event and system log detail. Requirement 10 specifies that logs are stored in a central location that is independent of the virtual systems being logged, and to support forensic analysis. Describe how your virtualization solution will help us comply with Requirement 10.

Specific issues to address for Requirement 10:

- Describe how your solution logs all access to virtual systems in the cardholder data environment - especially administrative access.
- Detail the types of data captured in logs, such as user identification, type of event, date and time, success or failure indication, origination of event, and identity or name of affected data, virtual system component or resource.
- What types of automated audit trails are created by your solution? Examples include all individual user accesses to cardholder data; all actions by any individual with root or administrative privileges to virtual systems; access to all audit trails; invalid logical access attempts; use of identification and authentication mechanisms; initialization of audit logs; creation and deletion of system-level objects.
- Where does your solution store log records?
- Describe the security controls protecting log records from alteration or deletion.
- Describe the time synchronization technology used by your solution.
- How does your solution comply with the requirement to retain audit trail history for at least one year, and to provide at least three months of history for immediate analysis?

Requirement 11: Regularly test security systems and processes.

Virtual machines do not follow a linear vulnerability management life cycle: VMs may be shut down for extended periods of time and miss critical updates or patches; VMs may also revert to a snapshot, undoing previous installation of patches and updates. The vulnerability management and Inventory management systems must automatically update as VMs are deployed, moved, turned-on, or reverted. Malicious or accidental configuration errors will completely blind non-virtualized vulnerability management tools. Effective virtual vulnerability management requires automated detection and assessment capabilities deployed within the virtual infrastructure layers and integrated with virtual management APIs. Malicious activity occurring within virtual systems will be hidden from non-virtualized incident response tools. Further, incident response and network forensic efforts require the capability to capture all virtual network packets for the purposes of analysis and investigation. Virtualization aware and virtualized security technologies must be deployed to support incident response. Traditional pen testing and application specific vulnerability management is required.

RFI Template:

Testing security systems and processes for virtual systems in the cardholder data environment entails different requirements from physical testing processes being applied to virtual infrastructure. Describe how your solution deals with virtualized infrastructure challenges such as periodic power shutdowns, movement or reversion of VMs, missing routing patching cycles, and tracking and enforcing standard configurations. In particular, your virtualization solution must address compliance with Requirement 11.5, which specifies deployment of file integrity monitoring tools to regularly monitor and notify the unauthorized changes of critical system files, configuration files, or content files within the virtualized cardholder data environment.

Specific issues to address for Requirement 11:

- How does your solution monitor drift from approved virtual host hardening configurations?
- Describe how your solution automatically remediates drift in virtual infrastructure and how frequently this can occur.

Requirement 12: Maintain a policy that addresses information security for all personnel.

The dynamic and elastic nature of virtual infrastructure requires the implementation of automated and comprehensive technical controls to support a well-managed security policy. Traditional documentation management, security training, personnel review, and auditing are also required. Toward this end, best practices dictate adoption of a comprehensive information security management system (ISM) such as ISO 27000, NIST SP-800, or the COSO/COBIT framework.

RFI Template:

Describe how your solution will help us to extend our PCI DSS policy to virtualized systems. Your response should address unique risks of a virtualized cloud environment, including policies for forensics, employee background checks, vendor agreements, and virtual asset tracking processes and system updates.

Specific issues to address for Requirement 12:

- How does your solution implement policy labels for virtual assets, such as owner, contact information, and purpose?
- If you are a service provider who will store, process or transmit our cardholder data, how does your virtualization solution monitor your compliance with PCI DSS, and support independent audit and forensic requirements?

Appendix A: Shared hosting providers must protect the cardholder data environment.

Shared hosting providers are expected to protect your hosted environment and data. They must follow four guidelines. First is ensuring that your organization only run processes that have access to your cardholder data environment. Next, they must restrict your access and privileges to your own cardholder data environment. Logging and audit trails must be established for your cardholder data environment. And they must support forensic investigation in the event of a compromise.

RFI Template:

Describe how your service complies with Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.

Specific issues to address for Requirement 12:

- How does your service ensure that our virtual systems are only running processes that have access to our cardholder data environment?
- Describe how your service restricts our virtual systems access and privileges to our own cardholder data environment only.
- How does your service ensure that logging and audit trails are enabled and unique to virtual systems hosting our cardholder data environment, and are consistent with PCI DSS Requirement 10?
- Detail your processes that enable timely forensic investigation in the event of a compromise.

[END]