

Special Report: Cyber crime reporting in India
 Learn how you can help put a stop to cyber crimes today!
[Read this special report only on SearchSecurity.IN!](#)



Home > Topics > Security management > Business compliance management > PCI DSS compliance checklist for virtualized environments

PCI DSS compliance checklist for virtualized environments

Swati Sharma, contributor



The use of virtualization in information technology (IT) has a corroborative impact on infrastructure frameworks, processes and operations. As a result, organizations dealing with cardholder data have been impacted by virtualization. Although virtualization has a definite edge and offers greater return of investment than other technologies, it raises many information security and compliance issues.

The Payment Card Industry Security Standards Council's (PCI SSC) recently released PCI Data Security Standard (DSS) version 2.0 states that system components also include virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors. Therefore, adapting virtualization for the cardholder data environment (CDE) without proper evaluation may lead to unexpected issues.

Cardholder environments that rely on virtualization can be secured using operation and process level improvements. This is achievable by embedding information security during the planning, deployment, and maintenance stages. Here is a PCI DSS compliance checklist to protect the CDE:

PCI DSS compliance checklist for planning and evaluation

- Risk-based approach should be a part of your [PCI DSS compliance checklist](#) in order to decide the scope of virtualization. Identify the servers to be consolidated and take a call as to whether to include critical servers (for example, database servers
- storing cardholder data).
- Evaluation of server virtualization technologies is the next step in your PCI DSS compliance checklist. Take the call between full, para or operating system (OS) level virtualization. For consolidating critical servers, full virtualization should be preferred over para or OS level virtualization.
- Estimation of vendor specific security features is critical to ensure the desired level of security, including alerts for newly discovered vulnerabilities.

- [Hectic race to meet Visa's PCI-DSS compliance deadline](#)
- [PCI DSS certification boosts customer confidence at Zenta](#)
- [PCI DSS certification: Three myths that affect its success in India](#)
- [PCI-DSS standard compliance becomes reality for Bank of India](#)

SHOW ME MORE

[More on Business compliance management](#)

[Get help from the community](#)

Powered by: IT KNOWLEDGE EXCHANGE

You May Also Be Interested In...

MORE BACKGROUND

- ① [The effects of PCI DSS, compliance requirements on the security industry](#)
- ① [Default deny security: How to implement a positive security model](#)

MORE DETAILS

- ① [PCI self assessment questionnaire \(SAQ\) checklist for small merchants](#)
- ① [Select PCI DSS compliant service providers in India with these tips](#)

REFERENCE DESK

Business compliance management

NEWS, TIPS & MORE

- [IT \(Amendment\) Act 2008 and its effect on the Indian...](#) (ARTICLE)
 - [Learning to manage risk-based internal controls must...](#) (TIP)
 - [Looking to better manage insider security risks? Try...](#) (TIP)
 - [Massive T-Mobile UK security breach involves insiders](#) (ARTICLE)
 - [Are you too small for an email retention and archiving...](#) (TIP)
- [-> VIEW MORE](#)

Editors Pick for Best Content

Demystifying PKI technology based two factor authentication

Learn the pros and cons of using PKI for two factor authentication and more!

[Join us on SearchSecurity.IN to know more!](#)



SEE ALSO

- **Related Topics:** [Incident response management best practices](#), [Enterprise risk management strategies](#)

GET E-MAIL UPDATES

Submit your e-mail below to receive Information Security-related news, tech tips and more, delivered to your inbox.

- Support infrastructure requirement and capacity planning is critical to achieve or maintain PCI DSS compliance in virtual environments like audit and logging.
- Evaluation of business continuity planning/disaster recovery planning and high availability plan is the next critical PCI DSS compliance checklist item. This should be achieved with respect to attacks involving sniffing, capturing and/or modifying virtual machine (VM) traffic during migration.
- Draft or modify policies and procedures as per virtualization and PCI DSS compliance requirements. For instance, develop a mandatory security hardening document for the hypervisor.

PCI DSS compliance checklist for secure deployment

- Isolate critical servers containing cardholder data from the rest of guest OS. It's critical to ensure that only one primary function is implemented per virtual system component.
- The PCI DSS compliance checklist should include appropriate network segmentation to ensure that all inbound and outbound traffic to the CDE hosted on virtual server(s) are restricted by the firewall.
- Secure configuration. Harden the guest OS as well as underlying hypervisor as per PCI DSS compliance requirements—remove or disable all unnecessary services.
- Access control comes next on your PCI DSS compliance checklist. All access should be provided based on least privilege. This includes communication between hypervisor and the guest OS (hosting critical server) as well as between the guest OS (hosting critical server) and other guest OS. For access control, the hypervisor's access feature can be integrated using Active Directory technologies.
- The deployed antivirus should also provide protection from malware (such as Blue Pill/SubVirt or Vitriol) that target the hypervisor or virtualization layer.
- File integrity monitoring or other such solutions should be deployed to get alerts in case of changes to hypervisor configuration/new VM deployment.
- Deploy a VM-centric intrusion detection system/intrusion prevention system.
- Management console and management server protection is the last item of this part of your PCI DSS compliance checklist.

PCI DSS compliance checklist for maintain and monitor

- Changes in the virtual environment are extremely dynamic. Therefore, a proper change management process is critical to test and approve all changes, including those pertaining to the virtual system.
- The latest patches provided by your virtualization technology vendor should be deployed within a month (or as per your risk-based approach). Newly discovered vulnerabilities related to the hypervisor and virtualization should be signalled via alerts.
- A vital component of the PCI DSS compliance checklist at this stage includes undertaking audits and log reviews.
- Risk assessment should be conducted considering all threats related to virtualization technologies.
- Review of file integrity monitoring (FIM) alerts to ensure that there are no rogue virtual machines.
- Training and awareness sessions should include information security guidelines specific to virtualization.
- Incident management plan should include incidents related to virtualization technologies.

To sum up, all aspects of virtualization need to be duly considered prior to deployment. Also, the PCI DSS compliance checklist should be referred to at every phase to protect CDE in a virtual environment.

About the author: Swati Sharma is an associate consultant at SISA Information Security (CISSP & MS (Information Security)) and can be reached at swati.sharma@sisa.in. The views expressed are personal. Virtualization and PCI DSS was one of the topics discussed in the PCI DSS Implementation Workshop (<http://www.sisa.co.in/Upload/Excerpts PCI DSS Chennai Feb2011.pdf>) conducted by SISA

Security Management

Compliance

Email:

Not a member? We'll activate your FREE membership with your subscription.

2020software.com, trial software downloads for accounting software, ERP software, CRM software and Business Software Systems

in Chennai on February 24 & 25, 2011.

Dig Deeper

PEOPLE WHO READ THIS ALSO READ...

- [Differences between varchar and nvarchar in SQL Server](#)
- [Stored procedures vs. functions](#)
- [What is Sarbanes-Oxley Act \(SOX\)? - Definition from Whatis.com](#)
- [What is database? - Definition from Whatis.com](#)
- [What is e-commerce \(electronic commerce or EC\)? - Definition from Whatis.com](#)

RELATED TAGS

[3g](#), [4g](#), [active directory tutorial](#), [cdma](#), [crm](#), [database](#), [ddo](#), [http](#), [playstation network](#), [pop3](#), [sap](#), [ssl](#), [theserverside](#), [what is internet](#), [what is sap](#)

Show me more

Published: 09 Mar 2011

Advertisement

[Access our CISSP preparation guide to help you tackle one of the leading security certifications in India.](#)

Disclaimer: Our Tips Exchange is a forum for you to share technical advice and expertise with your peers and to learn from other enterprise IT professionals. TechTarget provides the infrastructure to facilitate this sharing of information. However, we cannot guarantee the accuracy or validity of the material submitted. You agree that your use of the Ask The Expert services and your reliance on any questions, answers, information or other materials received through this Web site is at your own risk.

BACK TO TOP ▲

ADS BY GOOGLE

[APC-PCI ELISA Kit](#)

Measure activated protein C complex
Manage severe sepsis & Xigris
www.bioporto.com

[Answer for Industry](#)

Our need for security impacts
every facet of modern life!
www.siemens.com/answers

[Security Metrics](#)

Join to gain access to powerful
security benchmark data.
www.securityexecutivecouncil.com

[Windows Azure Virtual](#)

Build Host Manage Troubleshoot
With Your Same On-Premise Tools
microsoft.com/windowsazure/

News ▲

Information Security
Topics ▲

Tutorials ▲

Expert
Advice ▲

White
Papers ▲

SEARCH



More from Related TechTarget Sites



CIO

DATA CENTER

BUSINESS INTELLIGENCE

SECURITY

SMB SECURITY

FINANCIAL SECURITY



Legacy application modernization: Make SOA work for you

Service-oriented architectures can help enterprises modernize their legacy applications. Here are some ways to make them work.

Mobile device management in the workplace: A guide for CIOs

Mobile devices enable flexibility previously unimaginable in the workplace, but they carry concerns about security and compliance. Learn more in our mobile device management guide.

Would you pay more for quality?

Would the enterprise apps require AMC if they had no bugs and / or needed no patches? Does the business value delivered by apps fully justify the cost presently incurred on them?