

Achieving Compliance in a Virtualized Environment



Table of Contents

Introduction..... 3

When Does Virtualization Impact Regulatory Compliance 3

What We Need To Achieve and Demonstrate Compliance 4

Access Controls 4

Change and Configuration Controls 5

Operational Controls 6

Lower Risk Areas Can Be Distractions 6

Virtualization Capabilities That Enable Compliance 6

Secure Foundation..... 6

Enterprise Features for Management Controls 7

Example: Achieving and Demonstrating PCI Compliance 8

Security First..... 8

Design for Compliance 8

Understand the Scope of PCI Requirements..... 8

Ensure that Controls are Comprehensive 8

Don't Rely on Technology Alone 8

Assign the Right Project Manager 9

Collaborate with the Auditor 9

Working with Service Providers 9

Conclusion 9

About the Authors 10

Achieving Compliance in a Virtualized Environment

Introduction

High profile information security failures resulting in the loss of cardholder data, confidential information, and personally identifiable information (PII) have substantially increased regulatory pressure. Many organizations must now comply with standards such as PCI, regulations like SOX-404 or HIPAA, and state privacy laws. Traditional IT auditors and security assessors have been focused on the physical components of the IT infrastructure. However, virtualization technologies are increasingly being used in business processes that have IT compliance requirements.

The goal of this paper is to present the unique considerations that virtualization presents to regulatory and standards compliance, and then prescriptively describe how to mitigate those risks:

- Discuss the different regulatory and contractual compliance objectives.
- Explain how to achieve and demonstrate compliance.
- Take a look at secure virtualization technologies.
- Provide a detailed example of achieving and proving compliance with PCI.

When Does Virtualization Impact Compliance

The number of regulations and contractual obligations that we must comply with continues to grow each year. But we should not rely on auditors, whether they are from an external CPA firm, PCI assessor, government certification and accreditation information system security officer or Designated Approving Authority (DAA) to arbitrarily establish what part of the virtualized environment is in scope for compliance to a particular standard. While compliance with applicable standards is by no means necessarily guaranteed in a virtualized environment (or for that matter any environment), this white paper describes a framework for reviewing such issues. Instead, we should proactively determine how virtualization impacts these standards. We do this by first documenting the compliance objectives for the standard, identifying the compliance risks, and determining how virtualization could impact compliance. Table 1 shows how to do this for some well-known regulations and standards with which organizations must achieve and prove compliance. It is also suggested that companies consult with their own legal departments and compliance professionals regarding such matters.

Regulation or Standard	Compliance Objectives	Risks	Virtualization Implications
Payment Card Industry Data Security Standard (PCI DSS)	Protect cardholder data	Cardholder data is disclosed, either in transit or in storage	Cardholder data transits virtualized networks, or is stored on virtualized infrastructure
SOX-404	Ensure accurate financial reporting	Errors in calculations and fraud	Calculations or key reports done on virtualized infrastructure
HIPAA	Protect patient healthcare data	Private patient healthcare records are disclosed	Patient healthcare records transits or is stored on virtualized infrastructure

Table 1: Examples of some common compliance arenas

By first linking the critical virtualization functionality to the compliance objective that may facilitate a determination if a problem with the virtualization technology jeopardizes compliance. Additionally, controls may not be required where there is no underlying business risk.

To illustrate how this approach works, consider the case of PCI DSS compliance. Virtualization technologies may be used in the business processes associated with credit card processing. However, a virtualized inventory management system running on virtualization may not technically appear to be in scope for PCI, because cardholder data typically does not transit and is not stored in those systems.

Similarly, for the SOX-404 regulations, if no critical IT functionality is performed on virtualized infrastructure (e.g., authorization workflow, key reports or calculations) that could lead to an undetected material financial reporting error, and virtualization may be out of scope. For example, if a materials management system runs on virtualized infrastructure, but all key reports are generated by a downstream business process, then the materials management system may be out of scope for SOX-404.

The remainder of this paper will describe how to potentially mitigate the risks for virtualized systems that are indeed subject to compliance standards, and demonstrate to auditors that appropriate controls exist and are effective, both in design and operation. Some of these controls will be provided by your IT

infrastructure vendors, and some must be performed continually by your own IT management.

What We Need To Achieve and Demonstrate Compliance

When auditing virtualized computing environments, auditors often ask the following questions, for which we should be prepared to answer and substantiate with documentation and other evidence.

- Are all computing environments and data adequately segregated?
- Who has privileged access to the virtualization infrastructure?
- How do you ensure that they are all authorized personnel?
- How is separation of roles designed and enforced?
- How are proper configuration documented and enforced?
- How are unauthorized changes detected and handled?
- How is the virtualized computing environment monitored for unauthorized access?
- How are technology vulnerabilities tracked and managed?

Regardless of the compliance objective, controls can generally be divided into three categories¹ :

- **Preventative controls:** prevent errors, omissions, or security incidents from occurring. Examples include access controls, separation of duty, configuration standards and settings, organizational policies, firewalls and network segregation, vulnerability management program
- **Detective controls:** detect errors or incidents that occur, such detecting unauthorized access, incorrect configuration settings, detecting unauthorized and untested changes, and other monitoring and measurement, intrusion detection, vulnerability scanning
- **Corrective controls:** quickly correct errors and restore normal operations, such as procedures and technologies to remove unauthorized users, unauthorized changes and restore service

What are the risks that we need to prevent, detect and correct? We can categorize IT control objectives and control activities in many ways—for example, using COBIT or ISO17799—but one of the easiest to apply and most useful categorizations emerged out of the Guide to Assessment of IT Risk (GAIT) project from the Institute of Internal Auditors (IIA)². This series of guides describes three broad categories of IT control objectives:

Access and user administration: What access restrictions must we set? For example, what restrictions should we set for physical and logical access and how should we separate duty and roles? Also, given that privileged virtualization management accounts are all-powerful accounts how should we restrict them?

Change and configuration: What systems, code and configurations must be configured and changed properly? Items we should consider include host configuration, configuration of virtual networks and storage, other virtual objects such as resource pools and clusters, and security settings.

Operations: What controls must we operationally put into place to properly handle planned and unplanned events? Planned activities could include regular backups, restoration testing, security and event monitoring, batch jobs, disaster and recovery testing, vulnerability management and patching, review of logs, awareness training. Unplanned activities typically include exception handling, incident/problem management, security incident handling, and so forth.

Once we have characterized IT control objectives in this manner, it may be relatively straightforward to identify how to implement these controls for the virtualization infrastructure layer.

Access Controls

One of our primary security responsibilities is to restrict access to authorized personnel via user administration, authorization and authentication. These restrictions also apply to the virtualized infrastructure, since these privileged accounts can perform actions and make changes like powering off virtual machines, copying data stores, disabling security controls, reconfiguring virtual networks, etc. These actions may affect the entire infrastructure, exposing IT systems to risk of disrupted service and creating unnecessary vulnerabilities for malicious and criminal

1. Insitute of Internal Auditors, "Global Technology Audit Guide: IT Controls," 2004.

2. "The GAIT Principles,"The Institute of Internal Auditors, January 2007 (<http://www.theiia.org/guidance/technology/gait/>)

acts that could jeopardize organization and compliance objectives. Because of these potential risks, we should control access to the virtualization layer and to all the virtualization management tools.

Access Control Type	Examples
Preventive	<p>Segregate duties. Because the virtualization administrator account is powerful, we may want to limit risk by defining appropriate roles and granting them access to only specific areas in the virtualized infrastructure.</p> <p>For example, we may group all virtual machines supporting a specific application, and then define roles such that individuals administering those virtual machines are distinct from individuals administering the virtualization layer.</p> <p>Segregate data. Virtualization can provide data and system isolation to separate and protect virtualized resources from each other. Specific mechanisms that provide this isolation are network controls such as VLANs, vSwitches, firewalls, and storage such as LUNs and datastores.</p>
Detective	<p>Monitor privileged virtualized infrastructure user account additions, removals and changes, wherever they are stored (for example, /etc/passwd, LDAP, Active Directory). Privileged accounts include service accounts that do system monitoring (for example, scheduler, motherboard monitoring agents).</p> <p>Reconcile each privileged virtualized infrastructure user account add, remove and change with an authorized change order from the IT manager. This reconciliation process may be manual (a signed paper form) or automated (for example, a BMC Remedy work order).</p> <p>Verify network controls. For example, by monitoring network traffic or ensuring that the network controls have not been disabled or changed.</p>

Table 2: Principles for applying access controls

Change and Configuration Controls

As with any complex application, virtualized infrastructures have configuration and logical security settings designed to limit the risk of human error, fraud and security incidents. Examples include proper password settings for the system BIOS, host operating system settings and permissions for virtualized infrastructure, network configuration settings and virtual machine

policies. However, risk can be introduced if these settings are improperly configured.

We should ensure that these virtualized infrastructure configuration settings are properly defined, implemented and verified. In addition, we need to authorize and test all changes to code and configurations. Once virtualized infrastructures are in a known, documented and trusted state, changes made to the virtualized infrastructure should be authorized, scheduled and substantiated by appropriate change management.

Change and Configuration Control Type	Examples
Preventive	<p>Apply organizational configuration standards. We should make use of guidance from numerous respected third parties and virtualization vendors for configuring virtualized infrastructure settings.</p> <p>These include:</p> <ul style="list-style-type: none"> • VMware ESX Server 3.x Benchmark Version 1.0, from the Center For Internet Security (CIS) • VMware Infrastructure 3, Security Hardening, from VMware • VMware ESX Server Security Technical Implementation Guide (STIG), from the Defense Information Systems Agency (DISA) <p>Develop and enforce organizational change policies. We should have a change management policy that describes the steps required to authorize, schedule, implement and verify changes. A Change Advisory Board might run this process.</p>
Detective	<p>Monitor for non-standard configurations. We should monitor configuration settings of the virtualized infrastructure against our internal security policies, external compliance requirements and industry best practices and report on any variances. We should verify that actions to correct non-compliant configurations are properly implemented in the required time frame.</p> <p>Monitor for unauthorized and untested changes. To prove compliance with change management processes, we should have evidence that production changes to the virtualized infrastructure can be reconciled with approved change requests. When unauthorized changes are made, we should have evidence that management took corrective actions.</p>

Table 3: Principles for applying change and configuration controls

Operational Controls

Operational controls encompass a variety of planned and unplanned activities, such as monitoring, logging, backups, vulnerability management, scheduled maintenance, capacity expansion, etc. Operational controls are typically the required planned actions necessary to deliver continuous service, and the unplanned activities needed to restore service when disrupted at inopportune times, as well as to recover from security incidents or failures.

Operational Control Type	Examples
Preventive	<p>Manage logs. PCI DSS and most other mandates require us to deploy centralized log aggregation and analysis tools and to retain logs for one year. These requirements apply to both virtual machines and the virtualized infrastructure.</p> <p>Manage vulnerability. Vulnerability scanning and management tools add greater system visibility and enable us to discover vulnerabilities in virtual machines and virtualized infrastructure host platforms.</p>
Detective	<p>Deploy network intrusion detection and prevention systems to protect both physical and virtual networks by warding off and notifying our security personnel of intrusion attempts.</p> <p>Perform an external vulnerability scan. Although quarterly external vulnerability scans are typically a compliance requirement, we should have an ASV (approved scanning vendor) conduct a vulnerability scan prior to an audit. Acting on any discovered vulnerabilities will help us pass the audit.</p> <p>Monitor events: To satisfy PCI DSS, FISMA and many other compliance requirements, we should have the ability to track all basic virtual machine lifecycle events such as power on/off, migration, reconfiguration and security-relevant events.</p>

Table 4: Principles for applying operational controls

Overall, the above control and visibility framework enables us to bring virtual machine environments in compliance with government laws, industry mandates and “best practices” frameworks as well as local security policies and procedures.

Virtualization Capabilities That Enable Compliance

The following section discusses the capabilities we should look for when choosing virtualization technology for our IT infrastructure.

Secure Foundation

Before considering a virtual infrastructure for compliance environment, we should confirm that the technology chosen provides a sufficient degree of isolation and protection of the

Lower Risk Areas Can Be Distractions

Auditors and security practitioners unfamiliar with virtualization technologies may spend time and resources on high profile, but low-risk areas, at the expense of higher risk areas. Examples include:

- **Exploits of the virtualization layer that are theoretically possible but which in reality have never been discovered in the wild.** Not only are vulnerabilities rare at this layer, but exploits are generally difficult and would involve breaking through multiple other security barriers, such as virtual machine OS-level protections, that typically are used in a production environment. An example would be the so-called “Blue Pill” exploit.
- **Vulnerabilities that exist in non-enterprise virtualization implementations.** Hosted virtualization refers to an architecture in which virtual machines run in a virtualization layer that sits on a general-purpose host OS. Such implementations typically have deliberate channels for sharing information between the virtual machine and the host OS. However, this architecture is not appropriate when the virtual machines cannot be trusted, as is the case when the virtual machines are on a public-facing network or on a network that is exposed to an insecure or only lightly-controlled network. Regardless of whether vulnerabilities exist with such implementations, these implementations should never be considered for a production environment.
- **Exploits that are dependent on poor IT practices and misconfiguration.** As with all infrastructure software, there is a strict separation between interfaces into the software that are meant for management and supporting services and interfaces used for production. Typically the non-production interfaces have fewer security controls implemented, because the design assumption is that these would reside on a secure, highly controlled network. If this best practice is not followed, then the risk exposure increases dramatically because the virtualization software is not being used in the intended manner.

In reality, the greatest risk of security compromise does not come from exploiting the underlying virtualization technology, but from misconfiguration and mismanagement, both of which can be mitigated using proper IT controls. By employing best practices for secure design and deployment, risks from vulnerabilities in the virtualization technology can be reduced to levels acceptable for most compliance environments.

virtualized resources. When considering virtualization of applications the following characteristics should be considered:

- Is it possible for one application to access the data from another, either on disk or in memory?
- Can one application consume so many resources as to adversely affect the performance of the others?
- If there is a fault or failure in one application, is it possible to take down the others?
- Can the troubleshooting and maintenance of one application be performed without restrictions while not affecting the others?

Although various virtualization methods can be considered, such as application, operating system, or hosted virtualization, the only one which can provide the strongest assurance for these characteristics is bare-metal virtualization, in which individual virtual machines run in isolated partitions that are managed by a hypervisor. This approach to virtualization suggests that the guest operating systems are not aware of each other, and no process running in one is able to communicate with a process running in another one except through standard networking channels that the administrator explicitly configures.

This requirement of independence can be limited to the VMs; under the covers, the virtualization layer can perform various optimizations such as memory and disk deduplication without violating isolation. Isolation can also be maintained while virtualizing other aspects of the infrastructure, such as networking (VLANs) and storage (LUNs).

In addition to selecting an appropriate technology, you should also consider the maturity and acceptance of the product you choose, based on factors such as:

- How long has the product been available and supported
- How many and what type of customers run in production environments
- What certifications or standards has it achieved

Enterprise Features for Management Controls

Having a secure foundation is the first step. But as security threats grow and evolve, our security environment will need to evolve and respond to them. For this reason, we will need the ability to make changes to the security infrastructure. We will also need a virtualization solution that exposes its management controls in order to conform to requirements outlined in security standards. To achieve compliance in virtualized environments, we should have both a safe virtual computing platform with security features and also an ability to manage the security of the platform through the use of other tools and solutions.

Authentication and Authorization Capabilities

Security management starts with authentication and authorization. All virtual platform interfaces to the outside world must have authentication control as well as the ability to grant fine-grained access privileges via a flexible authorization framework. We should be able to limit the scope of these permissions to specific objects or parts of the infrastructure and grant the right access rights to the right people, without violating the principle of “least privilege.” For example, an authorization framework that limits us to a single “all-powerful” Administrator role would not typically qualify, nor would typically a framework qualify if it prevented us from creating groupings or hierarchy for the roles that can be used.

In addition, privileges for administering virtual machines should be distinct from those for administering the hosts, as a means of limiting the scope of application owners. This critical “separation of duties” (SoD) limits the scope of possible abuse by “insiders,” such as data theft by system administrators or malicious or negligent system change by data owners.

Configuration and Logging

To simplify, and therefore secure platform configurations, configuration parameters for the virtualization software must be kept in a few, well-known locations with standard or easy-to-read formats. These configuration parameters should only be accessed and modified by those authorized to do so. In addition, virtual platform components and related management tools must have detailed logs that can centrally accessed for review, analysis and controlled log retention, based on a logging and security policy.

A Flexible, Well-Defined API

To enable other external tools to do their security management tasks, the virtualization technology should have a well-defined and open API to capture and view inventory, including topology. The API must also be able to control various functions and to securely extract audit data like the earlier mentioned activity logs. In addition, a well-architected system would not involve multiple, parallel API sets that are each used for different purposes—for example, one for internal components and a similar but distinct one for external integration. Instead, having one API provides a “single source of truth,” and hence assures that all interactions can be controlled and monitored in a reliable and consistent manner. An API with these characteristics will make satisfying compliance requirements much easier.

Example: Achieving and Demonstrating PCI Compliance

Most organizations are subject to cover a wide range of preventive, detective and other controls. For example, PCI DSS makes direct references to the following technologies:

- Firewalls
- Anti-virus and other anti-malware technologies
- Network intrusion detection and prevention
- File integrity checking
- Log management
- Vulnerability management
- Web application firewalls

In addition, many other technologies as well as security processes are implied as requirements of the standard. Among these technologies and processes are security policy development, risk assessment process, security awareness programs and penetration testing.

It's important for us to keep the following in mind when preparing for a PCI audit: auditors may apply many tests to determine whether our site is compliant with the PCI DSS. And there are over 200 individual control tests. Auditors are required to complete audits based on the established "PCI Audit Procedures, version 1.1," which can be downloaded from: https://www.pcisecuritystandards.org/docs/pci_audit_procedures_v1-1.doc. We should review this document prior to designing our VMware-based environment and certainly before preparing for the audit.

The remainder of this section presents some general recommendations for PCI Compliance.

Security First

It is important that the goal for our hosted IT environment is not principally to pass a PCI audit, although that may be a secondary consideration. There are several well-publicized accounts of companies that have passed PCI compliance audits, but have still suffered serious data breaches. Audits reflect the state of an environment at a point in time, but securing our data requires a broader view. You should not over-focus on compliance with the PCI DSS at the expense of broader security goals. By understanding the security requirements of the virtualized environment, achieving compliance may become much more straightforward and manageable.

Design for Compliance

It may be easier to design an environment for security and compliance than it is to adapt an existing one to compliance requirements. A common mistake companies make is that they try to force-fit a cardholder environment to their existing IT infrastructure. Taking this approach frequently leads to higher infrastructure and management costs, and even a weakened security platform.

Understand the Scope of PCI Requirements

Companies often make the mistake of attempting to implement too many irrelevant, inappropriate, or overly complex controls. One case study involved a company that started with a flat network topology with very little segmentation. Attached to their network was a mixture of database servers (containing cardholder data), web servers and internal applications. They had a goal of making that flat network PCI-compliant. As part of their migration to a VMware environment, the approach that was finally implemented made use of architectures and access systems that completely separated the cardholder-related from the non-cardholder related environments, thus reducing scope and hence cost of attaining compliance.

Ensure that Controls are Comprehensive

When auditing and certifying a virtualized IT environment to meet PCI DSS standards, auditors may try to confirm that the required control requirements and their control intent are being met, whether through virtualized or non-virtualized controls. When reviewing network controls in a virtual machine environment, the auditor will subject all traffic to the same security standards and controls as conventional networks. All critical data traffic processed on servers, physical or virtual, and transported on networks, must have the same security controls applied and provide verifiable evidence to auditors. Virtualized network interfaces, VLAN, DMZ, firewall, IDS, and logging and monitoring elements may be possible if the architecture also allows the control intent to be addressed.

Don't Rely on Technology Alone

Some technology vendors may claim that their products are PCI compliant. This is not a responsible marketing statement. It must be remembered that usually no one technology can solve a PCI control requirement. It is more often the case that, to achieve a portion of the PCI DSS control requirements, we must use some technologies (such as firewalls) in combination with other technologies (like log management solutions) and specific documented processes. We must evaluate what we need for PCI, assess what pieces of the puzzle we already have in place, and then develop a project plan to achieve and maintain compliance.

Working with Service Providers

Outsourced IT service providers serve as an interesting case study because they heavily use virtualization technologies to reduce cost and complexity and improve reliability, and will often be involved in achieving regulatory and contractual compliance.

As mentioned, virtual machine environments may provide compelling benefits, but they also present the same, and in some cases more complex, threat and risk scenarios as traditional dedicated IT environments. Most control requirements and controls have been developed for physical infrastructure, so their application to virtual infrastructure components is not always clear cut. And just as the release of multi-tenant hosted applications demanded that previous single threaded security controls are rearchitected to allow the intent of the controls to provide the risk mitigation originally expected, now virtualized platforms must tackle similar issues that may impact the perceived efficiency and flexibility.

A common misconception is that companies who host with a provider that claims to be “PCI compliant” will

automatically be PCI compliant. Nothing is further from the truth. PCI compliance is the responsibility of hosting provider’s customer who processes credit card data.

The services offered by hosting providers vary greatly, and many aggressively market their ability to help customers achieve PCI compliance. As it applies to a hosted VMware environment, make sure you understand which controls you, versus your provider, will be managing with respect to specific PCI control requirements.

A reference architecture should be developed with your provider that, at a minimum:

- Illustrates how your required environment can be hosted effectively by your provider and whether adjustments are necessary to the provider’s standard hosting model in order to serve your broader security goals.
- Clarifies which controls you, versus your provider, will be managing with respect to specific PCI control requirements.

Assign the Right Project Manager

Planning for a PCI compliance audit may be, depending on the breadth of our IT environment, an extraordinarily complex project. We should not make the mistake of believing that spending money on technology alone is this answer. A good project manager, especially one who has knowledge of the PCI DSS and has worked with auditors, is worth his or her weight in gold, especially if that individual is involved at the outset of the design process.

Collaborate with the Auditor

It may sound unusual, but by engaging the auditor to review our plans prior to an audit, we can improve our chances of passing a PCI audit. It can be even more helpful to bring them in even earlier, letting them analyze the virtualization environment at various steps of the implementation. Acting as consultants, some auditors will also offer services to help with the design of a secure and compliant infrastructure and may offer pre-audit assessments.

Conclusion

The rise of virtualization is occurring in an increasingly regulated environment. But without a plan for how to achieve, maintain and prove compliant with relevant regulations and standards,

the cost savings and efficiencies promised by virtualized infrastructure may be erased by increased security risk and huge efforts that must be put toward achieving and proving compliance.

Good planning ensures a smoother, more cost-effective path to compliance. We need to carefully examine technologies and solutions geared toward helping achieve compliance by verifying that their features and capabilities support our IT control objectives. We can also ensure greater success by bringing individuals with experience in the compliance arena to help us plan and manage our virtualized infrastructure. We should even consider even bringing in auditors prior to the audit to help us identify potential weak areas that would result in a failed audit. But we should always keep in mind that the first goal with any infrastructure, whether virtualized or physical, is to configure for strong security. All too frequently, organizations pass compliance, but then still experience a serious security breach or service disruption.

Getting our virtual infrastructure into a compliant state does not need to be as difficult and confusing as we often think. Achieving compliance is not an arbitrary exercise. We now have distinct actions we can take to ensure that our virtualized and physical environments pass our next audit quickly and painlessly.

About the Authors

Charu Chaubal, PhD

Charu is a Senior Architect in Technical Marketing at VMware, where he enables customer adoption and drives key partnerships for datacenter virtualization. His areas of expertise include virtualization security and compliance and infrastructure management. Charu has been responsible for defining and delivering VMware's prescriptive guidance on security hardening and operations. Previously, Charu worked at Sun Microsystems, where he had over seven years experience designing and developing distributed resource management and grid infrastructure software solutions. He holds several patents in the fields of datacenter automation and numerical price optimization. Charu received a Bachelor of Science in Engineering from the University of Pennsylvania, and a Ph.D. from the University of California at Santa Barbara, where he studied theoretical models of complex fluids.

Dr. Anton Chuvakin, GCIH, GCFA

(<http://www.chuvakin.org>)

Dr. Anton Chuvakin is a recognized security expert and book author. In his current role as a Chief Logging Evangelist with LogLogic, a log management and intelligence company, he is involved with projecting LogLogic's product vision and strategy to the outside world, conducting logging research and influencing company vision and roadmap.

A frequent conference speaker, Anton also represents LogLogic at various security meetings and standards organizations. He is an author of a book "Security Warrior" and a contributor to "Know Your Enemy II", "Information Security Management Handbook", "Hacker's Challenge 3", "PCI Compliance" and an upcoming book on logs. Anton also published numerous papers on a broad range of security and logging subjects. In his spare time he maintains his security portal <http://www.info-secure.org> and several blogs such as one at <http://www.securitywarrior.org>.

Gene H. Kim, CISA, TOCICO Jonah

Gene Kim is the CTO and co-founder of Tripwire, Inc. In 1992, he co-authored Tripwire while at Purdue University with Dr. Gene Spafford. Since 1999, he has been studying high performing IT operations and security organizations. In 2004, he co-wrote the Visible Ops Handbook, codifying how to successfully transform IT organizations from "good to great." In 2008, he co-authored Security Visible Ops Handbook, a handbook describing how to link IT security and operational objectives in four practical steps by integrating security controls into IT operational, software development and project management processes.

Gene is a certified IS auditor, and is part of the Institute of Internal Auditors GAIT task force that developed and published the four GAIT Principles in January 2007, designed to help

management appropriately scope the IT portions of SOX-404. In 2007, ComputerWorld added Gene to the "40 Innovative IT People Under The Age Of 40" list, and was given the Outstanding Alumnus Award by the Department of Computer Sciences at Purdue University for achievement and leadership in the profession.

Chris Richter, CISM, CISSP

Chris is VP and general manager of security products and services at SAVVIS, a leading network, hosting and security services provider, where he is responsible for the managed-security line of business, strategy and product portfolio. He leads the effort behind implementing standardized control frameworks and risk management processes across SAVVIS' dedicated and cloud-based services. He also is in a leadership role in working on the company's "IT Utility," a virtualized hosting services platform with products currently in use by thousands of enterprises worldwide. Chris has assisted many enterprises in adapting their premise-based infrastructure risk management programs and security controls to SAVVIS' outsourced virtualized and shared-infrastructure services. He brings an IT service provider's view of control requirements for virtualized infrastructures. Chris is a member of ISSA and ISACA, and for more than 20 years has held various security and IT services management and consulting positions at companies such as Digital Equipment Corporation, Compaq Global Services, 3Com, Cable & Wireless and Sterling Software. He is a Certified Information Systems Security Professional (CISSP) and a Certified Information Security Manager (CISM), and has served as a technical advisor and board member of several Silicon Valley-based IT product and services companies.

Sean Sherman, CISA, CISSP, PMP, MCSE

With more than 22 years in IT, Sean has been involved in the development of complex IT systems for a variety of industries. He holds a number of technical certifications including CISSP, CISA, PMP and MCSE. He is active in a number of organizations and is currently a board member for a local ISACA Chapter. Sean's background includes Developer, Management of IT, Manager of Consulting Services, Program and Project Management, Senior Consultant and Practice Leader for Classified Information Services. For the past 10 years Sean has focused his energies on IT high security and assurance services for the US Government, most recently, working in that area with Tripwire, Inc (<http://www.tripwire.com>), where he leads the program to developing security compliance and best practices content for the Tripwire Enterprise product.

Revision: 20080912 Item: WP-067-PRD-01-01



VMware, Inc. 3401 Hillview Ave. Palo Alto CA 94304 USA Tel 650-475-5000 Fax 650-475-5001 www.vmware.com
© 2008 VMware, Inc. All rights reserved. Protected by one or more of U.S. Patent Nos. 6,397,242, 6,496,847, 6,704,925, 6,711,672, 6,725,289, 6,735,601, 6,785,886, 6,789,156, 6,795,966, 6,880,022, 6,961,941, 6,961,806, 6,944,699, 7,069,413; 7,082,598, 7,089,377, 7,111,086, 7,111,145, 7,117,481, 7,149, 843, 7,155,558, 7,222,221, 7,260,815, 7,260,820, 7,269,683, 7,275,136, 7,277,998, 7,277,999, 7,278,030, 7,281,102, 7,356,679, 7,409,487, 7,412,492, 7,412,702, and 7,424,710; patents pending. VMware, the VMware "boxes" logo and design, Virtual SMP and VMotion are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

