

Virtualization Security & Audit

John Tannahill, CA, CISM, CGEIT, CRISC
jtannahi@rogers.com

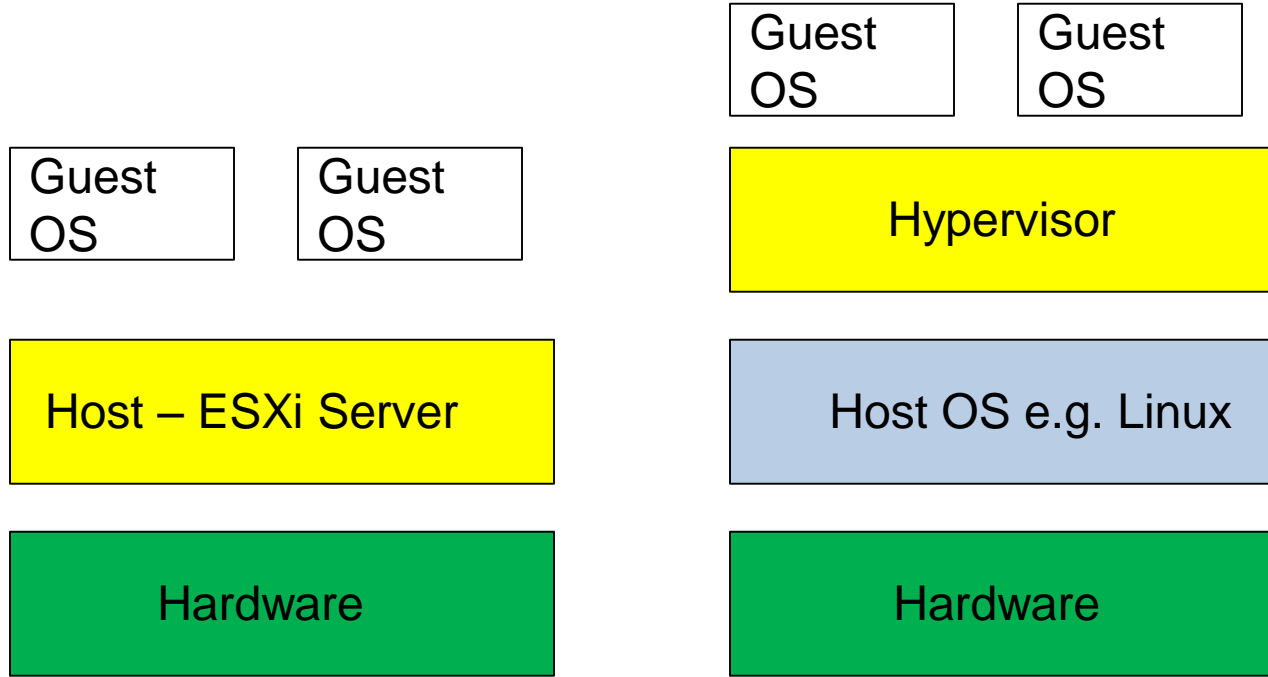


Session Overview

- Virtualization Concepts
- Virtualization Technologies
- Key Risk & Control Areas
- Audit Programs / Checklists



Virtualization Concepts



Type1:
Bare Metal Hypervisor

Type 2:
OS-Based Hypervisor

Virtualization in the Organization

- Key audit scoping issue is understanding of use of virtualization in the organization
- *Server Virtualization e.g. x86 hardware (session focus)*
- Storage Virtualization
- Network Virtualization
- Desktop Virtualization (VDI)

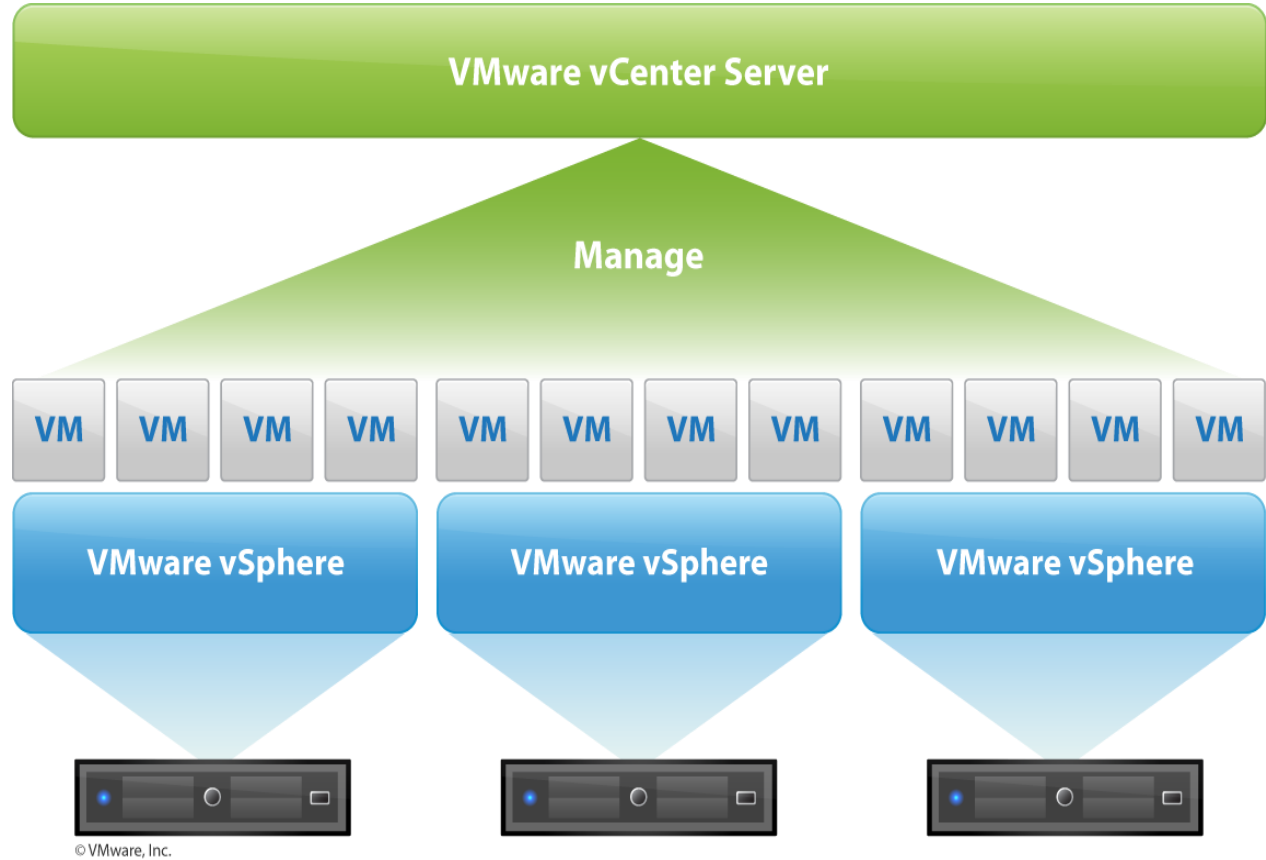


Virtualization Technologies

- VMware vSphere
- Microsoft Hyper-V
- Azure Hypervisor
- Oracle VM
- Linux KVM



vSphere



Source – VMware

Oracle VM

- X86 server virtualization
- Xen hypervisor technology
- Supports Windows, Linux, and Oracle Solaris guests
- Oracle VM components
 - Oracle VM Manager: web based management console to manage Oracle VM Servers.
 - Oracle VM Server: includes a version of Xen hypervisor technology
 - Oracle VM Agent to communicate with Oracle VM Manager for management of virtual machines
 - Minimized Linux kernel as Dom0



VMware Horizon View

(source – Wikipedia)

- VMware View provides remote-desktop capabilities to users. A client desktop operating-system – e.g. Windows 7 runs within a virtual environment on a server.
- VMware View components:
 - VMware vSphere for Desktops (includes ESXi)
 - VMware vCenter Server
 - View Composer (advanced View management, with automation and cloning)
 - View Manager (administration of the View Environment)
 - View Client (communication between View and the desktop OS)
 - VMware ThinApp (application virtualization)
 - View Persona Management (user profile management)
 - vShield Endpoint (offloaded desktop antivirus)



Best Practices for Mitigating Risks in Virtualized Environments

(source – cloudsecurityalliance.org)

- VM Sprawl
- Sensitive Data Within a VM
- Security of Offline and Dormant VMs
- Security of Pre-Configured (Golden Image) VM / Active VMs
- Lack of Visibility Into and Controls Over Virtual Networks
- Resource Exhaustion
- Hypervisor Security
- Unauthorized Access to Hypervisor
- Account or Service Hijacking Through the Self-Service Portal
- Workload of Different Trust Levels Located on the Same Server
- Risk Due to Cloud Service Provider API



Defcon 20 - VASTO



ERPScan

Security Scanner for SAP

*Invest in security
to secure investments*

**How to hack VMware
vCenter server in 60
seconds**

Alexander Minozhenko



Metasploit Framework

- Examples:
 - auxiliary/scanner/vmware/vmware_enum_users
 - auxiliary/scanner/vmware/vmauthd_login
 - auxiliary/scanner/vmware/vmware_http_login
 - auxiliary(poweron_vm)

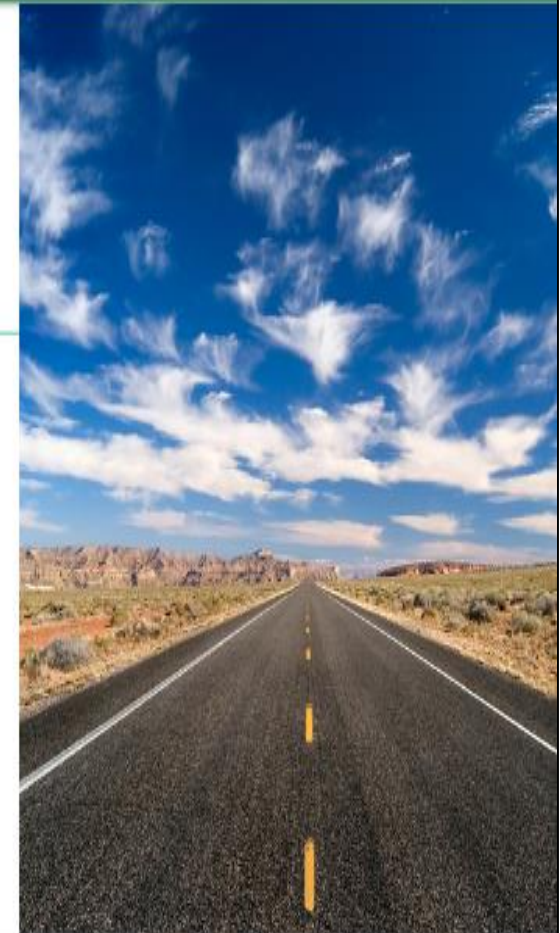


Azure Hypervisor

Compromise-as-a-Service

Our PleAZURE

Felix Wilhelm & Matthias Luft
{fwilhelm, mluft}@ernw.de



© ERNW GmbH | Carl-Bosch-Str. 4 | D-69115 Heidelberg

3/31/14 www.ernw.de

Critical Security Controls - v6

- **CSC 1: Inventory of Authorized and Unauthorized Devices**
- **CSC 2: Inventory of Authorized and Unauthorized Software**
- **CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers**
- **CSC 4: Continuous Vulnerability Assessment and Remediation**
- **CSC 5: Controlled Use of Administrative Privileges**
- **CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs**
- CSC 7: Email and Web Browser Protections
- CSC 8: Malware Defenses
- **CSC 9: Limitation and Control of Network Ports, Protocols, and Services**
- CSC 10: Data Recovery Capability




Critical Security Controls – v.6

- **CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches**
- **CSC 12: Boundary Defense**
- CSC 13: Data Protection
- CSC 14: Controlled Access Based on the Need to Know
- CSC 15: Wireless Access Control
- CSC 16: Account Monitoring and Control
- CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps
- CSC 18: Application Software Security
- **CSC 19: Incident Response and Management**
- **CSC 20: Penetration Tests and Red Team Exercises**



PCI DSS Virtualization Guidance



PCI Security Standards Council™

Standard: PCI Data Security Standard (PCI DSS)
Version: 2.0
Date: June 2011
Author: Virtualization Special Interest Group
PCI Security Standards Council

**Information Supplement:
PCI DSS Virtualization Guidelines**

Table of Contents

1	Introduction	3
1.1	Audience	3
1.2	Intended Use	4
2	Virtualization Overview	5
2.1	Virtualization Concepts and Classes	5
2.2	Virtual System Components and Scoping Guidance	7
3	Risks for Virtualized Environments	10
3.1	Vulnerabilities in the Physical Environment Apply in a Virtual Environment	10
3.2	Hypervisor Creates New Attack Surface	10
3.3	Increased Complexity of Virtualized Systems and Networks	11
3.4	More Than One Function per Physical System	11
3.5	Mixing VMs of Different Trust Levels	11
3.6	Lack of Separation of Duties	12
3.7	Dormant Virtual Machines	12
3.8	VM Images and Snapshots	13
3.9	Immaturity of Monitoring Solutions	13
3.10	Information Leakage between Virtual Network Segments	13
3.11	Information Leakage between Virtual Components	14
4	Recommendations	15
4.1	General Recommendations	15
4.2	Recommendations for Mixed-Mode Environments	20
4.3	Recommendations for Cloud Computing Environments	22
4.4	Guidance for Assessing Risks in Virtual Environments	25
5	Conclusion	27
6	Acknowledgments	28
	About the PCI Security Standards Council	28
7	Appendix – Virtualization Considerations for PCI DSS	29

Key Security Processes

- Configuration and Asset Management
- Security Architecture
- Secure Build Process
- Hardening Process
- Security Bulletin Monitoring Process
- Patch Management Process
- Privilege Management
- Vulnerability Management Process



NIST SP800-125 - Guide to Security for Full Virtualization Technologies

- Virtualization Security Overview
 - Guest OS Isolation
 - Guest OS Monitoring
 - Image and Snapshot Management
- Security Recommendations for Virtualization Components
 - Hypervisor Security
 - Guest OS Security
 - Virtualized Infrastructure Security
 - Desktop Virtualization Security
- Secure Virtualization Planning and Deployment



NIST 800-125-A Draft: Security Recommendations for Hypervisor Deployment

- Threats Areas:
 - HY-BF1 - Execution Isolation for Virtual Machines
 - HY-BF2 Devices Emulation & Access Control – such as Network and Storage (block) devices
 - HY-BF3 Execution of Privileged Operations for Guest VMs by the Hypervisor
 - HY-BF4 Management of VMs
 - HY-BF5 Administration of Hypervisor Host & Hypervisor Software
- Recommendations for hypervisor security baseline functions (vendor-neutral)



NIST SP800-125B

Secure Virtual Network Configuration for Virtual Machine (VM) Protection

- Network Segmentation
Configurations for VM Protection
- Network Path Redundancy
Configurations for VM Protection
- VM Protection through Traffic Control
Using Firewalls
- VM Traffic Monitoring



vSphere 5.5 / 6

- Security Guide
- Hardening Guide



VM Hardening Steps

- Secure Configuration (Hardening)
- Security Patch Management
- Example Standards:
 - STIG
 - <http://iase.disa.mil/stigs/stig/index.html>
 - CIS Benchmark
 - <http://cisecurity.org>
 - VMware Best Practice Guides



ESXi Server 5.5 – Coverage



CIS VMware ESXi 5.5 Benchmark

v1.0.0 - 08-04-2014

- 1 Install.....
- 2 Communication
- 3 Logging
- 4 Access
- 5 Console
- 6 Storage.....
- 7 vNetwork
- 8 Virtual Machines
- 8.1 Communication.....
- 8.2 Devices
- 8.3 Guest.....
- 8.4 Monitor.....
- 8.5 Resources
- 8.6 Storage.....
- 8.7 Tools.....

STIG Guidelines

DISA STIG Viewer : 2.3

File Export Checklist Options Help

STIG Explorer

▼ STIGs

CK	Name	Vul ID	Rule Name
<input type="checkbox"/>	VMware vSphere ESXi 6.0 Security Technical Implementation G...	V-63147	SRG-OS-000027-VMM-000080
<input type="checkbox"/>	VMware vSphere vCenter Server Version 6 Security Technical Im...	V-63173	SRG-OS-000480-VMM-002000
<input type="checkbox"/>	VMware vSphere Virtual Machine Version 6 Security Technical I...	V-63175	SRG-OS-000480-VMM-002000
		V-63177	SRG-OS-000032-VMM-000130
		V-63179	SRG-OS-000021-VMM-000050
		V-63181	SRG-OS-000329-VMM-001180
		V-63183	SRG-OS-000023-VMM-000060
		V-63185	SRG-OS-000023-VMM-000060
		V-63187	SRG-OS-000023-VMM-000060
		V-63189	SRG-OS-000033-VMM-000140
		V-63191	SRG-OS-000033-VMM-000140
		V-63193	SRG-OS-000107-VMM-000530
		V-63195	SRG-OS-000480-VMM-002000
		V-63197	SRG-OS-000480-VMM-002000
		V-63199	SRG-OS-000480-VMM-002000
		V-63201	SRG-OS-000480-VMM-002000
		V-63203	SRG-OS-000480-VMM-002000
		V-63205	SRG-OS-000480-VMM-002000
		V-63207	SRG-OS-000480-VMM-002000
		V-63209	SRG-OS-000480-VMM-002000
		V-63211	SRG-OS-000480-VMM-002000
		V-63213	SRG-OS-000480-VMM-002000
		V-63215	SRG-OS-000480-VMM-002000
		V-63217	SRG-OS-000480-VMM-002000
		V-63219	SRG-OS-000480-VMM-002000

Profile: No Profile

▼ Filter Options

CAT I CAT II CAT III

Enter filter keyword

Inclusive Filter Exclusive Filter

Showing rule 1 out of 195

▼ General Information

VMware vSphere ESXi 6.0 Security Technical Implementation Guide :: Release: 2 Benchmark Date: 22 Jul 2016

Rule Title: The VMM must limit the number of concurrent

▼ Discussion

Enabling lockdown mode disables direct access to an ESXi host requiring the host be managed remotely from vCenter Server. This is done to ensure the roles and access controls implemented in vCenter are always enforced and users cannot bypass them by logging into a host directly. By forcing all interaction to occur through vCenter

▼ Check Content

From the vSphere Web Client select the ESXi Host and go to Manage >> Settings >> System >> Security Profile. Scroll down to "Lockdown Mode" and verify it is set to Enabled (Normal or Strict).

or

▼ Fix Text

From the vSphere Web Client select the ESXi Host and go to Manage >> Settings >> System >> Security Profile. Click edit on "Lockdown Mode" and set to Enabled (Normal or Strict).

or

▼ CCI

CCI: CCI-000054
The information system limits the number of concurrent sessions for each organization-defined account and/or account type to an organization-defined number of sessions.
NIST SP 800-53 - AC-10

VMware Best Practice Guides

- VMware vSphere Hardening Guide
 - Virtual Machines
 - ESXi Hosts
 - Virtual Network
 - vCenter Server
 - vCenter Components



Storage Security

- NAS
- SAN
- Protocols
 - NFS
 - CIFS / SMB

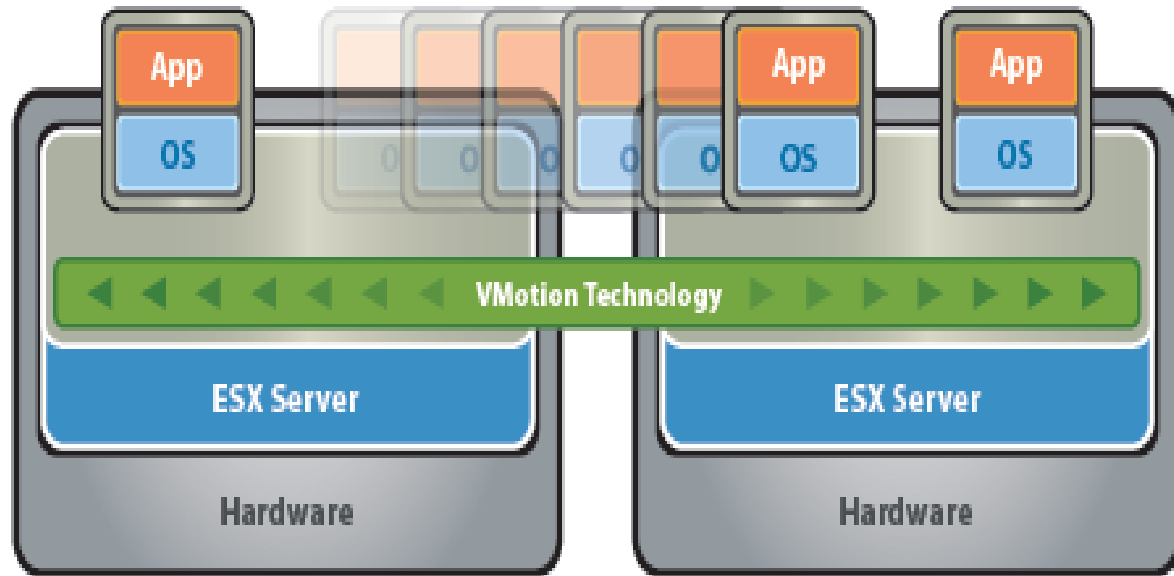


Network and Firewall Security

- Minimize TCP/IP Services
 - Host and Guest VM's
- Firewall and VLAN security
- Vswitch configuration
- Distributed Switches



Vmotion / Cloud Bursting



Source – VMware

Cloud Security Benchmarks



CIS Amazon Linux 2014.09 Benchmark

v1.0.0 - 01-06-2015

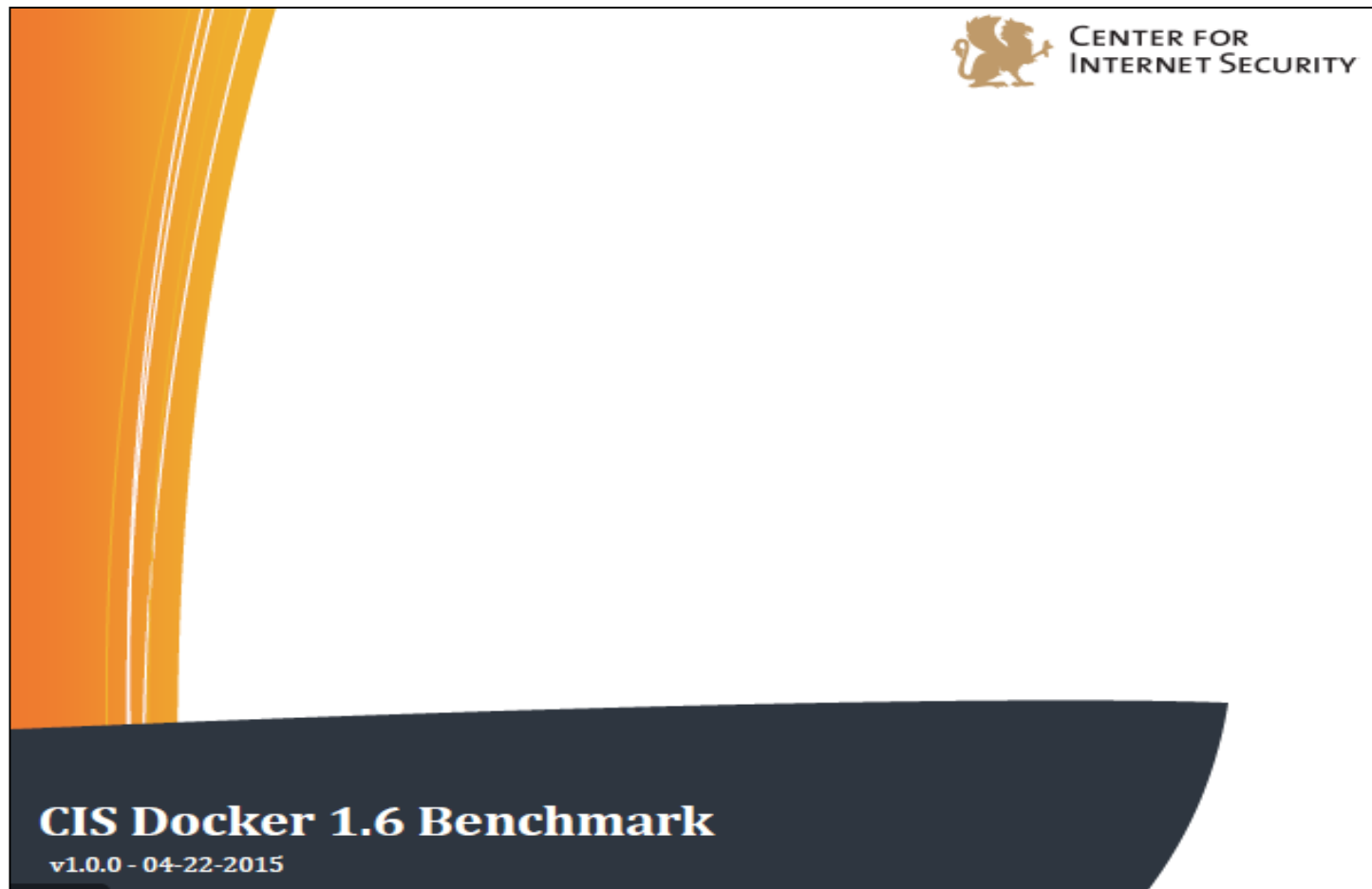
8.50 x 11.00 in

Other Audit Areas to Consider

- Software Defined Data Centre (SDDC)
- Micro segmentation
- Software Defined Networking (SDN)
- Hyper-convergence
- Containers



CIS – Docker Benchmark



ISACA VMWare Audit Program

- Planning and Scoping the Audit
- Governance of the virtualized environment
- Pre Fieldwork Preparation
- VMware virtualized environment
- Compliance
- *Control & Audit Objectives*



Session Summary

- Use of Virtualization technology within Organization
- Understand key risks
- Understand technology and key controls
 - vCenter Security (Management)
 - ESXi Security (Hypervisors)
 - VM Security (Guest VM)
- Service and Cloud Provider Environments

