Virtualization Security & Audit

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

ISACA®
Trust in, and value from, information systems
South Africa Chapter

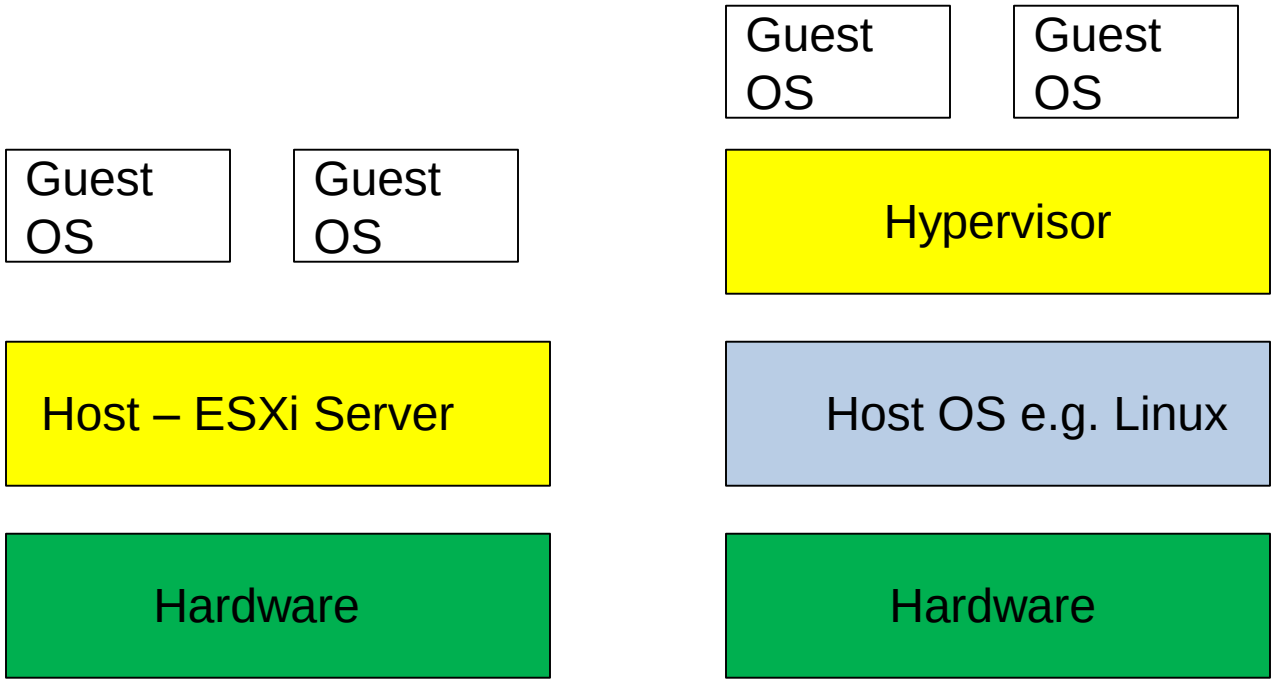
ISACA
Trust in, and value from, information systems
South Africa Chapter

Session Overview

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

ISACA
Trust in, and value from, information systems
South Africa Chapter

Virtualization Concepts



Type1:
Bare Metal Hypervisor

Type 2:
OS-Based Hypervisor

#isacazaconf

ISACAZA @ISACAZA ISACA South Africa

ISACA
Trust in, and value from, information systems
South Africa Chapter

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)

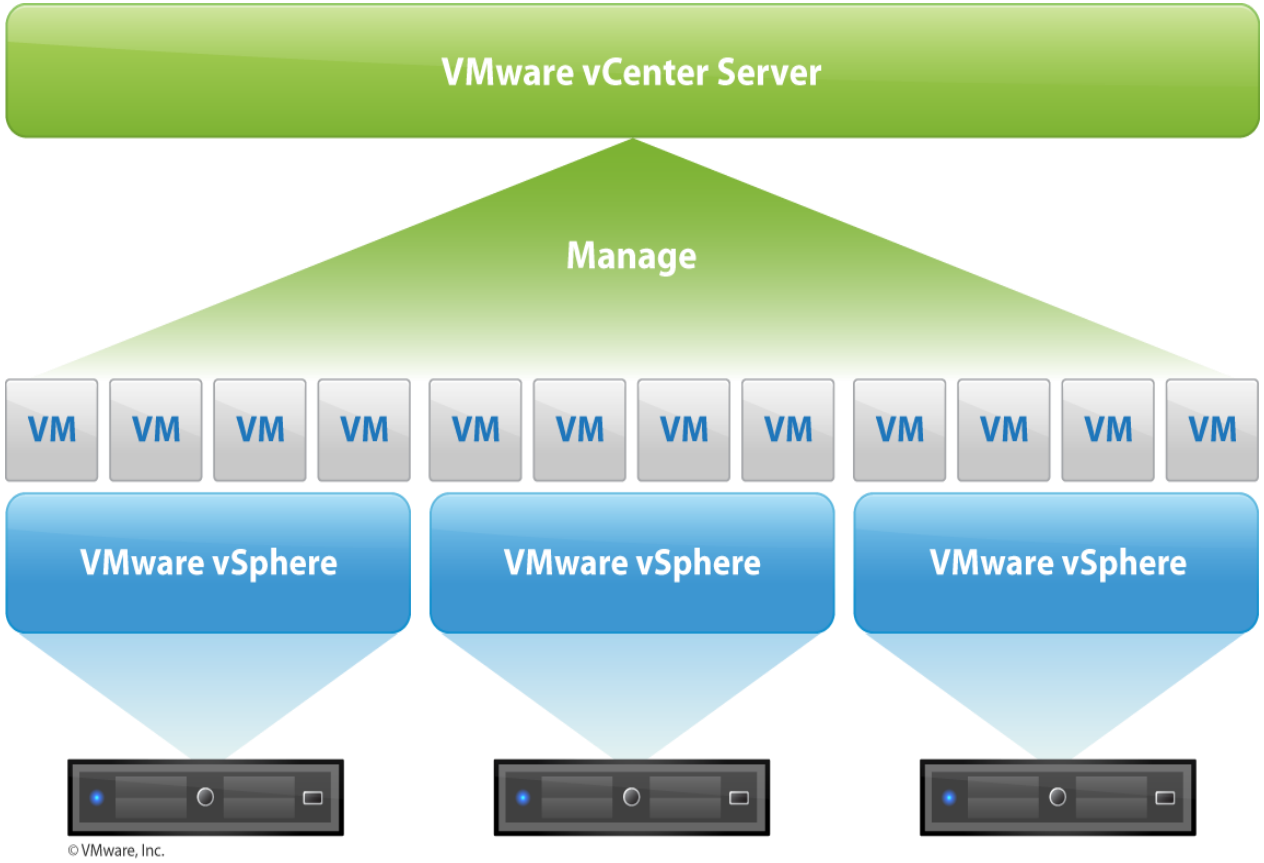
ISACA
Trust in, and value from, information systems
South Africa Chapter

Virtualization Technologies

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

ISACA
Trust in, and value from, information systems
South Africa Chapter

vSphere



Source – VMware

#isacazaconf

ISACAZA @ISACAZA ISACA South Africa

ISACA
Trust in, and value from, information systems
South Africa Chapter

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

ISACA
Trust in, and value from, information systems
South Africa Chapter

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)

ISACA
Trust in, and value from, information systems
South Africa Chapter

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

ISACA
Trust in, and value from, information systems
South Africa Chapter

Defcon 20 - VASTO

#isacazaconf

ISACAZA @ISACAZA ISACA South Africa

ISACA
Trust in, and value from, information systems
South Africa Chapter

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

ISACA
Trust in, and value from, information systems
South Africa Chapter

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

ISACA
Trust in, and value from, information systems
South Africa Chapter

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**

ISACA
Trust in, and value from, information systems
South Africa Chapter

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

#isacazaconf

ISACAZA @ISACAZA ISACA South Africa

ISACA
Trust in, and value from, information systems
South Africa Chapter

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

ISACA
Trust in, and value from, information systems
South Africa Chapter

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

#isacazaconf

ISACAZA @ISACAZA ISACA South Africa

ISACA
Trust in, and value from, information systems
South Africa Chapter

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

ISACA
Trust in, and value from, information systems
South Africa Chapter

vSphere 5.5 / 6

- Security Guide
- Hardening Guide

ISACA
Trust in, and value from, information systems
South Africa Chapter

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

#isacazaconf

ISACAZA @ISACAZA ISACA South Africa

ISACA
Trust in, and value from, information systems
South Africa Chapter

ESXi Server 5.5 – Coverage

CIS VMware ESXi 5.5 Benchmark

v1.0.0 - 08-04-2014

#isacazaconf

ISACAZA @ISACAZA ISACA South Africa

ISACA
Trust in, and value from, information systems
South Africa Chapter

STIG Guidelines

DISA STIG Viewer : 2.3

File Export Checklist Options Help

STIG Explorer

STIGs

CK	Name
	VMware vSphere ESXi 6.0 Security Technical Implementation G...
	VMware vSphere vCenter Server Version 6 Security Technical Im...
	VMware vSphere Virtual Machine Version 6 Security Technical I...

Profile: No Profile

Filter Options

CAT I CAT II CAT III

Enter filter keyword Add

Inclusive Filter Exclusive Filter

Remove Filter Remove All Filters

Vul ID	Rule Name
V-63147	SRG-OS-000027-VMM-000080
V-63173	SRG-OS-000480-VMM-002000
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

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

#isacazaconf

ISACAZA @ISACAZA ISACA South Africa

ISACA
Trust in, and value from, information systems
South Africa Chapter

VMware Best Practice Guides

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

ISACA
Trust in, and value from, information systems
South Africa Chapter

Storage Security

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

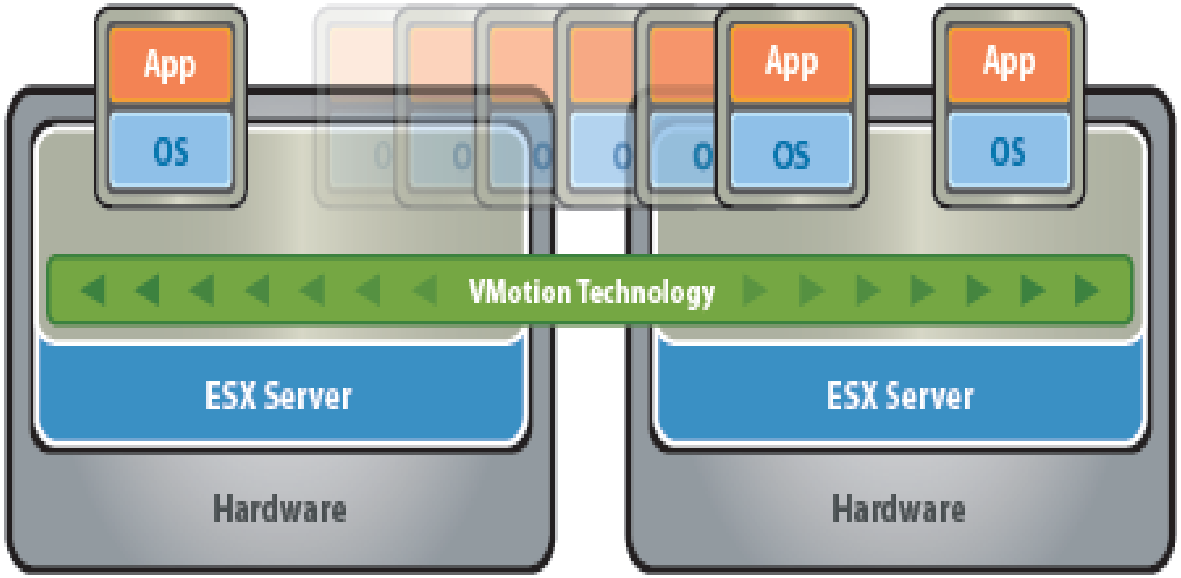
ISACA
Trust in, and value from, information systems
South Africa Chapter

Network and Firewall Security

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

ISACA
Trust in, and value from, information systems
South Africa Chapter

Vmotion / Cloud Bursting



Source – VMware

ISACA
Trust in, and value from, information systems
South Africa Chapter

Cloud Security Benchmarks

#isacazaconf

ISACAZA @ISACAZA ISACA South Africa

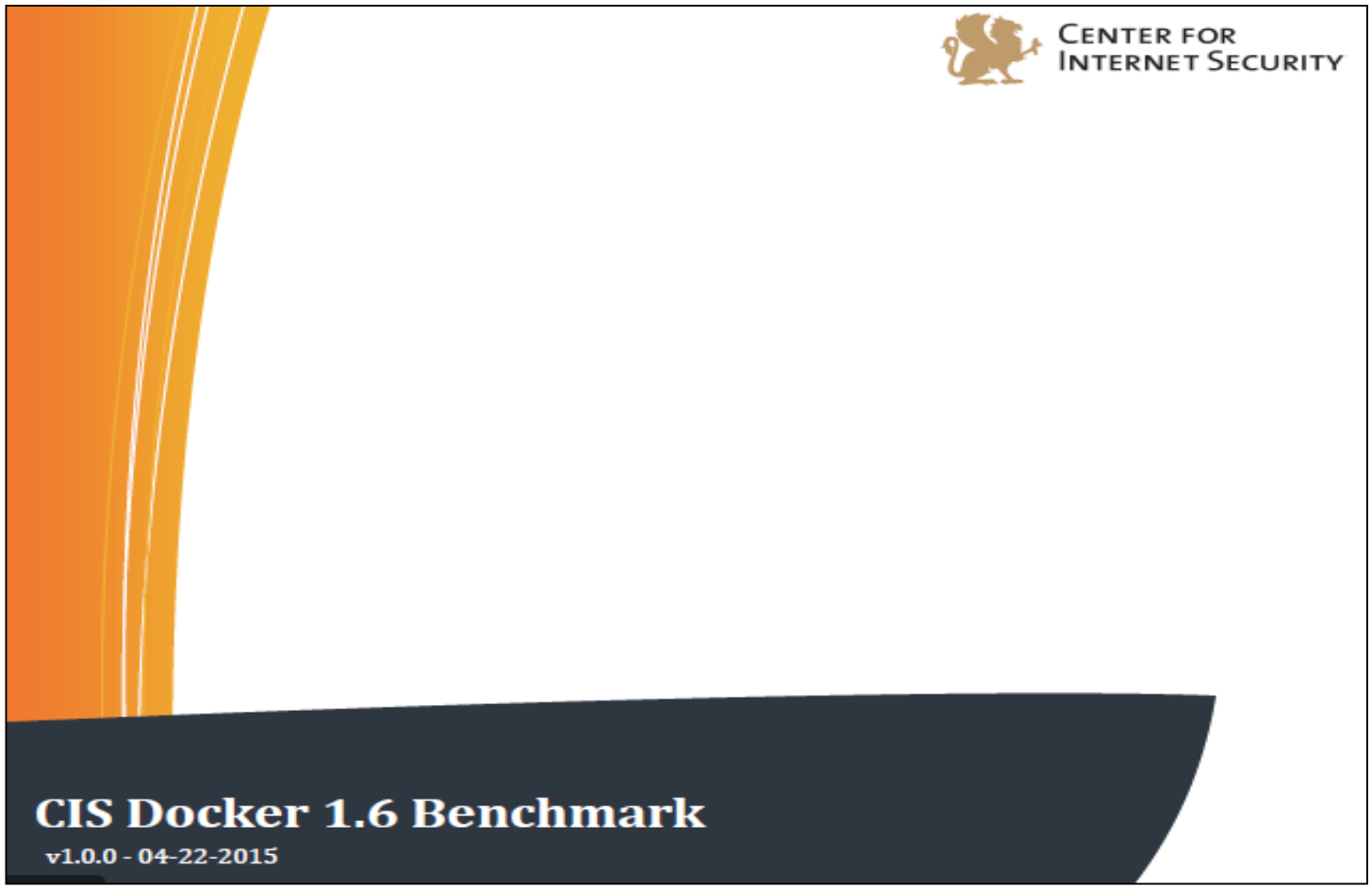
ISACA
Trust in, and value from, information systems
South Africa Chapter

Other Audit Areas to Consider

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

ISACA
Trust in, and value from, information systems
South Africa Chapter

CIS – Docker Benchmark



#isacazaconf

ISACAZA @ISACAZA ISACA South Africa

ISACA
Trust in, and value from, information systems
South Africa Chapter

ISACA VMWare Audit Program

- Planning and Scoping the Audit
- Governance of the virtualized environment
- Pre Fieldwork Preparation
- VMware virtualized environment
- Compliance

- *Control & Audit Objectives*

#isacazaconf

ISACAZA @ISACAZA ISACA South Africa

ISACA
Trust in, and value from, information systems
South Africa Chapter

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

#isacazaconf

ISACAZA @ISACAZA ISACA South Africa