Presentation for ISACA Chapter NL

Auditing Virtual Servers

VMware: Security and Operations

Gert-Jan Timmer
3. September, 2012

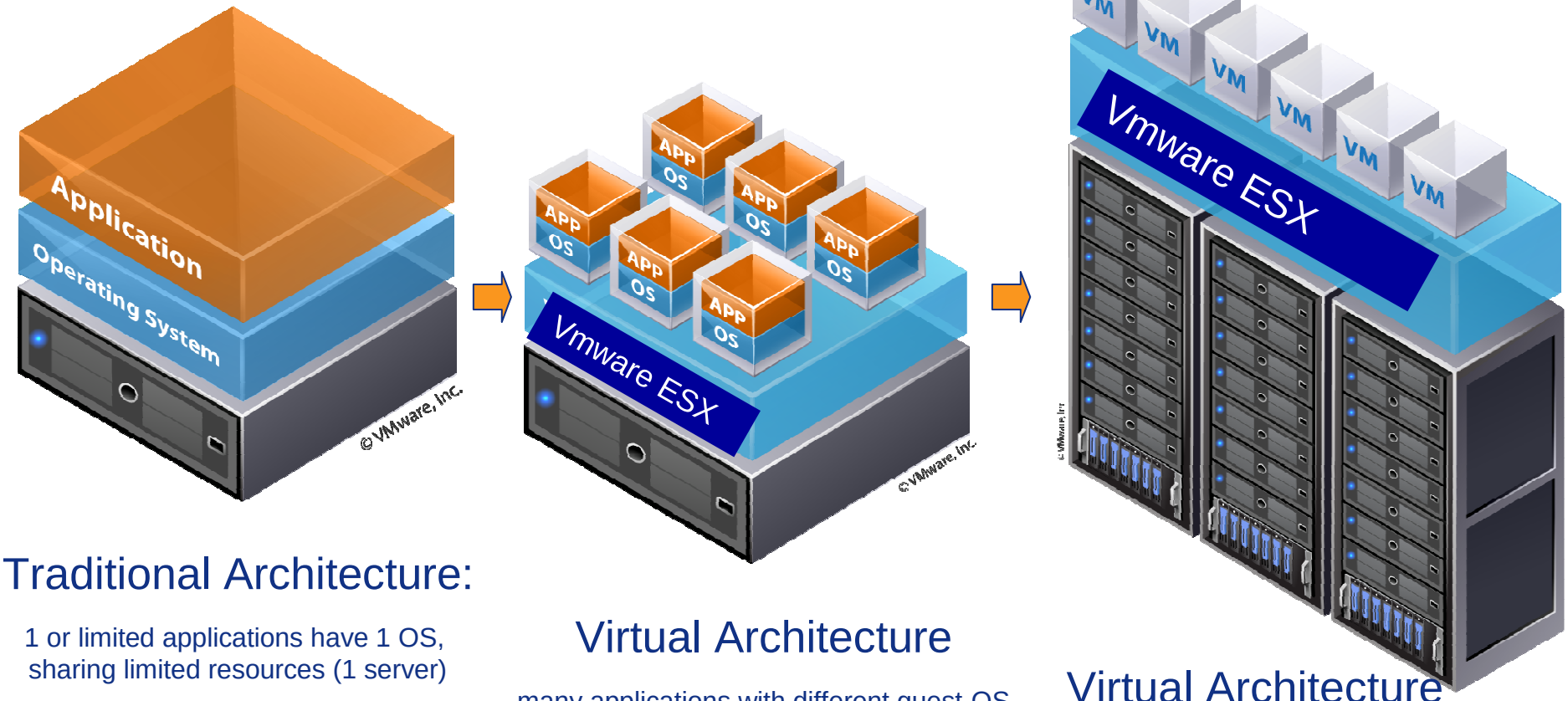
redefining / standards

Auditing Virtual Servers:
Vmware: Security and Operations

Presentation today:

- (Very) Short introduction in Virtualisation
- Auditing Virtual Servers:
  - **Step 1: „Understand the virtual server environment“:**
  - **Step 2: Define the scope of the audit**
  - **Step 3: Make an Audit program for security risks**
  - **Step 4: Make an Audit program for operational risks**

Short introduction in Virtualisation (1/4)



Traditional Architecture:

1 or limited applications have 1 OS,
sharing limited resources (1 server)

Virtual Architecture

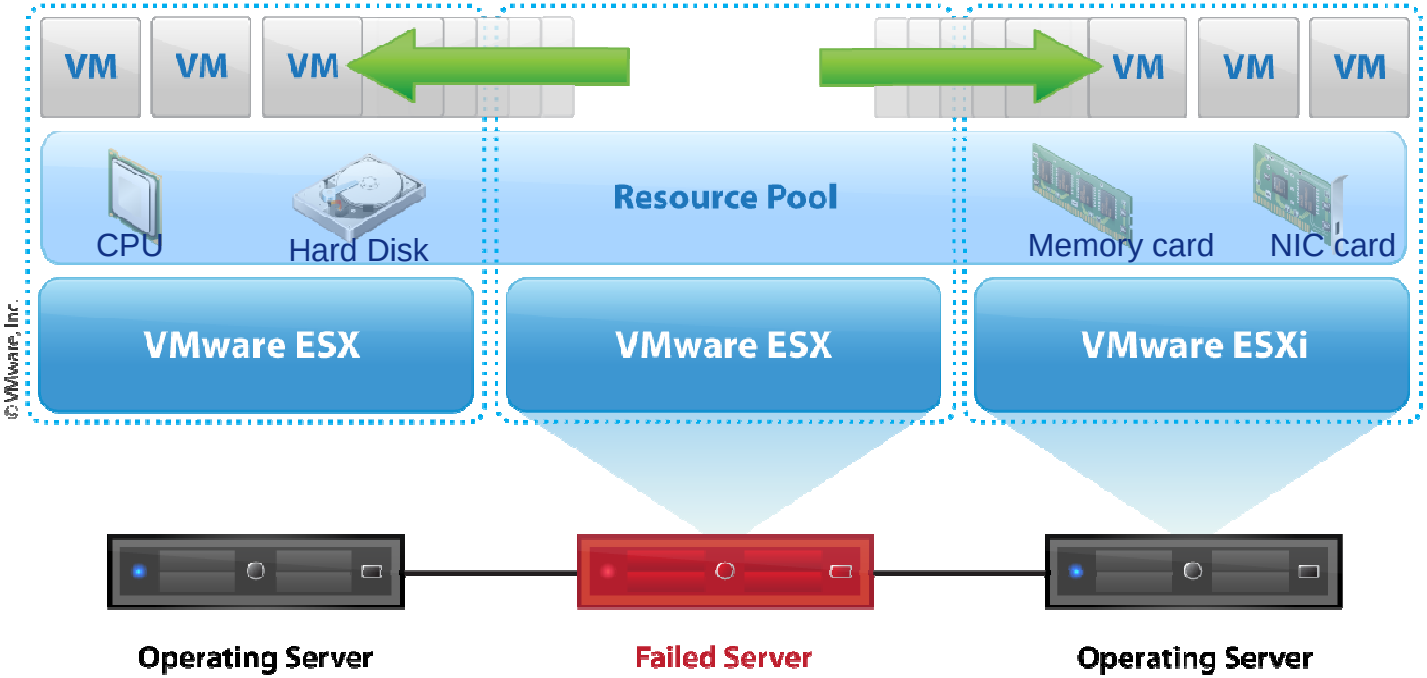
many applications with different guest-OS
share limited resources (1 server)

Virtual Architecture

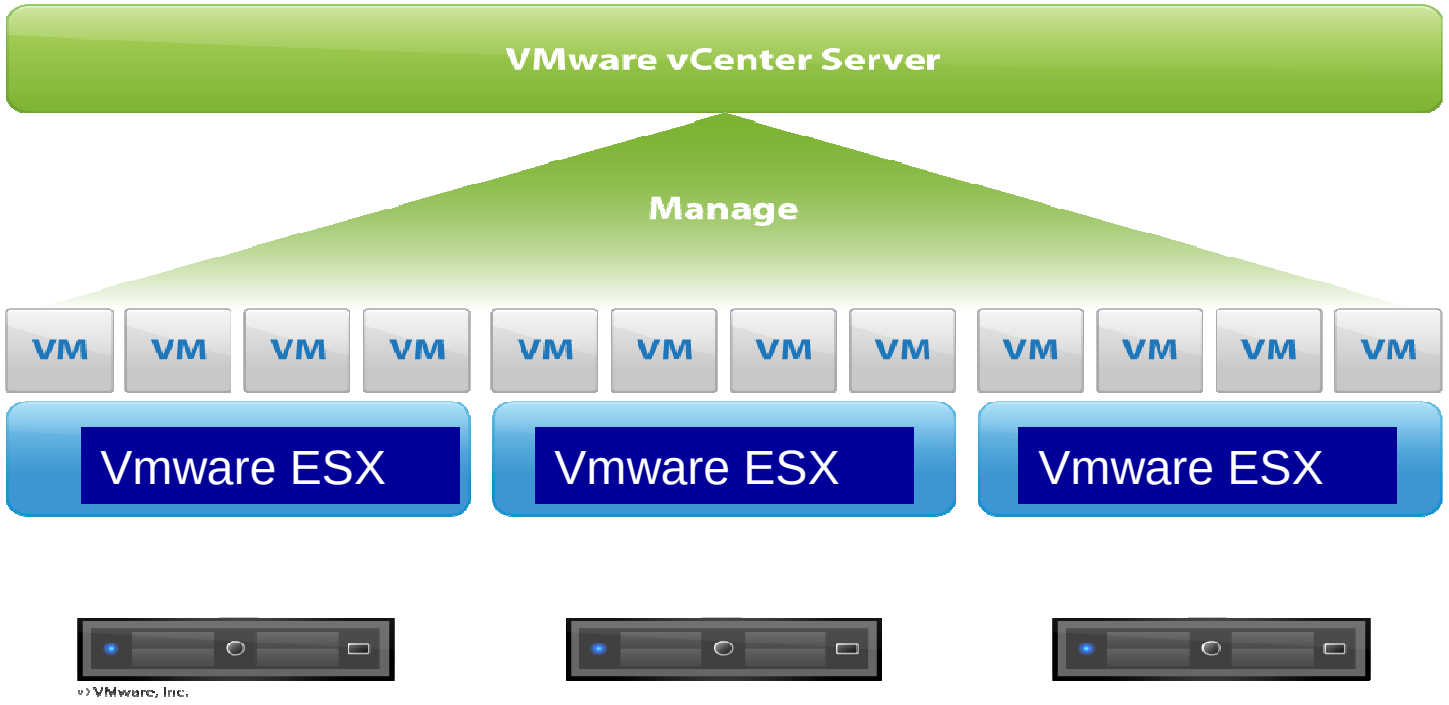
many VMs share many resources

(cluster of servers)

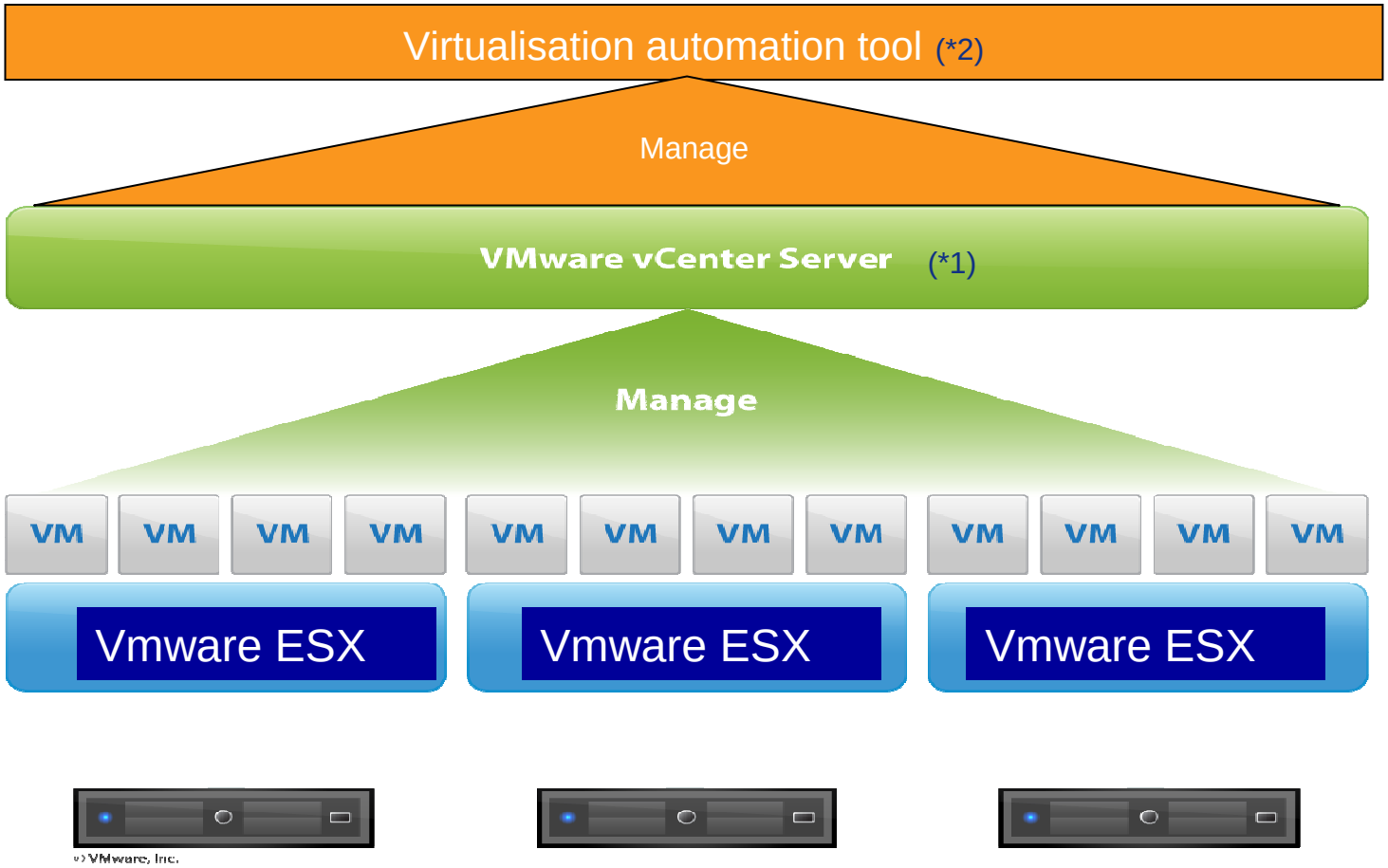
Short introduction in Virtualisation (2/4)



Short introduction in Virtualisation (3/4)



Short introduction in Virtualisation (3/4)



*1 VMware VCenter = tool for managing the virtual environment
*2 Virtualisation Automation tool = tool for automating virtual environments

Auditing Virtual Servers, step 1

- Step 1: „Understand the virtual server environment“:
  - **Internet**: Information about Auditing in virtual environments, e.g.:
    ISACA Audit Assurance Program, ISACA Cloud Computing Management Audit / Assurance Program, SANS Institute, Cloud Security Alliance Guidelines, Scripties VU, etc.
  - **Supplier documentation** e.g.:
    - VMware vSphere 4.1 Hardening Guidelines,
    - VMware security advisory / knowledge base
  - **Visit a seminar** to get basic or detailed knowledge e.g.: Virtualization & Cloud Audit Professional or Auditing VMware & Cloud Computing
  - **Information about the virtual environment in the organisation:**
    - Overview of virtual servers, software versions, security policies, responsibilities, risk or technical assessments, etc.
    - Order read-only rights for the Virtual Center.

Auditing Virtual Servers, step 2 (1/2)

- Step 2: Define the scope of the audit

- 2a. Which potential security risks exist?

  - Potential risks: inadequate security in the virtual environment could negatively impact the confidentiality, integrity and availability of the data processing used in business processes.
  - Question to be answered: Which security risks are not adequately covered?
  - In Scope of the audit concerning security risks, e.g.:
    - **Logical security / user rights**
    - **ESX Server security**
    - **Network security**
    - **Automated security processes for virtual environments**
    - **VM files settings**
    - **Loggings management**

    Out-of-scope e.g. physical security, (virtual) Storage

Auditing Virtual Servers, step 2 (2/2)

- 2b. Which potential operational risks exist?

  - Potential risks: inadequate operational management of the virtual environment can negatively impact the continuity of the data processing for business processes.
  - Question to be answered: Which operational risks are not adequately covered?
  - In Scope of the audit concerning operational risks, e.g.:
    - **Capacity management,**
    - **Asset and configuration management,**
    - **Backup & Recovery,**
    - **High availability solutions, Disaster Recovery,**
    - **License management,**
    - **Use of (new) VMware Tools,**

    Out-of-scope, e.g.: development / staging of virtual applications into production

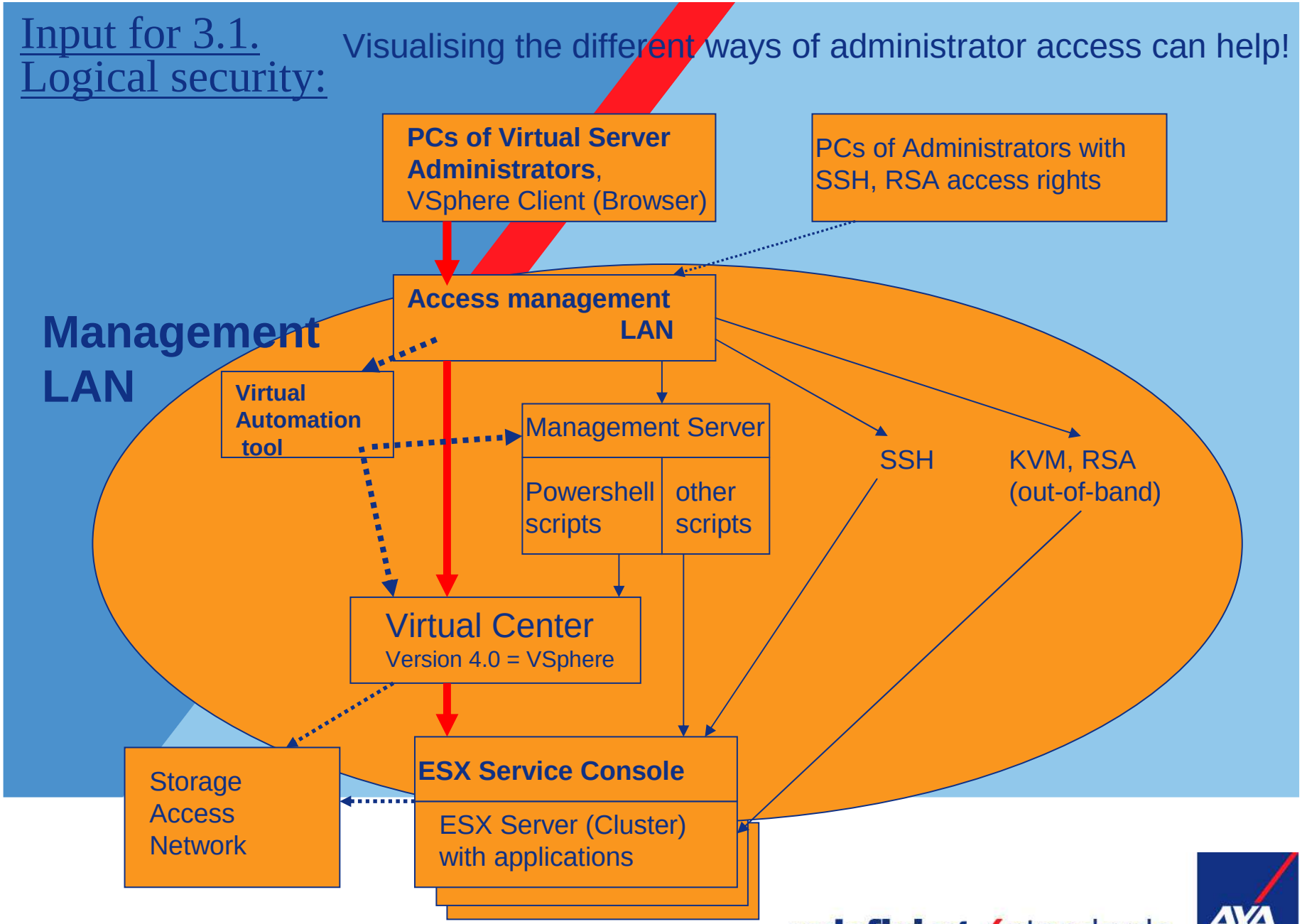
Auditing Virtual Servers, step 3 (1/7)

Step 3: Make an Audit program for security risks,
the following areas could be included:

- **3.1 Logical security / access rights**
- **3.2 ESX Server Security**
- **3.3 Network security on the ESX Server**
- **3.4 Automated security processes for virtual environments**
- **3.5 VM files settings**
- **3.6 Loggings management**

Input for 3.1. Logical security:

Visualising the different ways of administrator access can help!



redefining / standards

Auditing Virtual Servers, step 3 (3/7)

Attention points for security risks:

- **3.1 Logical security / access rights for:**
  - Virtual Center Security: e.g. Windows 2003/2008 or Linux
  - Virtual Center Database (alarm/event data, HA/DRS data, etc)
  - Managed Object Browser (potential unauthorised access to VCenter; not logged)
  - Virtual Center: (Administrator) Roles
    - Inaktive roles; „read-only“
    - Seggregation of duties / limit activities with „No access“
    - Change Management of roles and Logging
    - Update Manager database user: use least privilege
  - User rights management proces:
    - Use of autorisation and authentication server: LDAP / Active Directory
    - SOX Controls, Re-Certification
  - (Remote) Access of ESX Server
  - Service Console of ESX Server and Logging
  - Plugins and Scripts
  - Automation tool for access to functions in the automation layer above VCenter

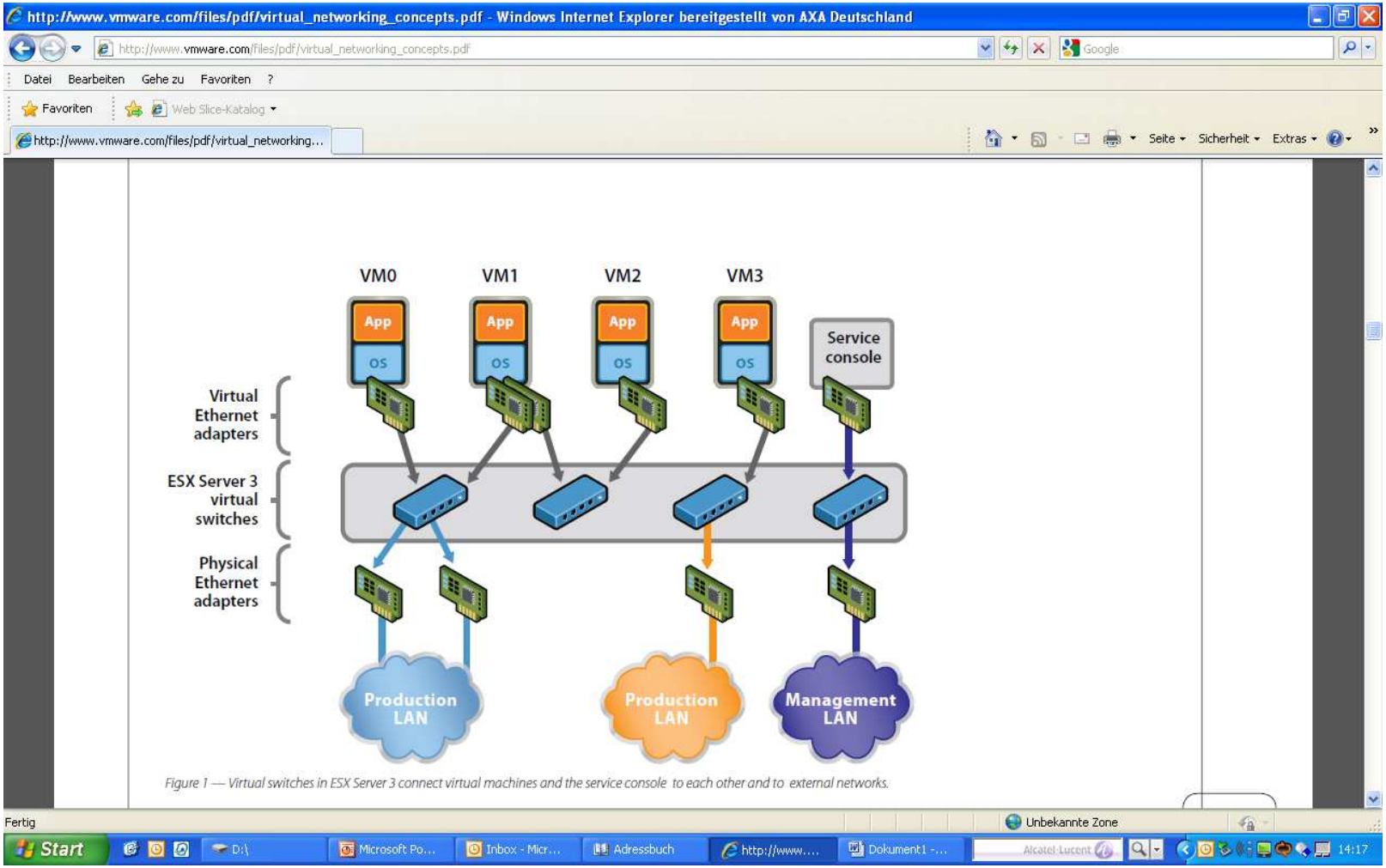
Auditing Virtual Servers, step 3 (4/7)

- **3.2 ESX Server Security:**
  - Security policies („hardening baselines“)
  - Software Version VMware ESX (or ESXi Version?)
  - Security configuration of the Service Console (Linux)e,g, free Tool: AZscan
  - If an authorised person can get to the ESX console, (s)he can list (LS-command) all possible commands to (mis)use. Esx.conf file is important.
  - Security breaches of VMware (> 110 reported!)
  - Anti-virus solutions for VMware (VDI, guest OS)
  - Integrity of installation files (checksum)
  - Test Management
  - Templates and Change Management of templates
  - Transparent Page Sharing (physical memory deduplication)
  - Patch Management (ESX Server; Service Consoles)
  - (New) VMware functionalities like:
    - Vshield zones (virtuelle Firewalls),
    - third party security appliances (Trendmicro, Symantec, ..) to control the security of the VMs

Auditing Virtual Servers, step 3 (5/7)

- **3.3 Network security on the ESX Server:**
  - Network Architecture Policy for ESX Server
  - Secure communication to the VCenter and VCenter Database?
  - Virtual LAN (VLAN, Private VLAN):
    - Separation of development and production applications?
    - Compliance / Laws: Bank applications?
    - Isolation of security critical applications with the help of PVLANs? e.g. in Tier 1 for Internet server.
  - Via which ports can the user / administrators connect with an ESX Server, are these connections secure?
  - Exchange of data between ESX Server / Cluster (VMotion): over a secure and seperate Netwerk connection / VLAN
  - Virtual (distributed) Switches (Vswitches):
    - Trunking risk
    - Isolation of data traffic: use port groups for connecting data traffic over NICs and switches to connect VMs
    - Compliance / Laws (who can access which VMs over Virtual switches)

Auditing Virtual Servers, step 3 (6/7)



Auditing Virtual Servers, step 3 (7/7)

3.4 Automated security processes for virtual environments

- The design, implementation and security controls in automated processes, like e.g. server provisioning, patch management and security compliance processes are relevant to audit.

3.5 VM files (parameter) settings

- Hardening VCenter application (guest operating system).
- The VM configuration file (VMX) sets the rules for behaviour,
  - e.g. for guest operating system (Linux, Windows, ..) commands
  - non-administrators can shrink disk capacity
  - when Vmsafe = true, the security virtual appliance can control the security of the VM
  - VM storage profile (category/classification of files; certain configuration files must be stored on certain discs.
- Application interfaces (APIs), VM Communication Interface (vmmci-interface)
- VM isolation can be violated

3.6 Loggings Management

- Logging for changed roles in VCenter, Automation tool, security related events, guest Operating System (incl. in the VM)
- Write logs directly to a dedicated server
- Security log analyse process
- Set up forensic audit trails (if needed). Set logging on „verbose“. This captures more information in case of forensics

Auditing Virtual Servers, step 4 (1/5)

Step 4: Make an Audit program for operational risks,
the following areas could be included:

- **4.1 Capacity management**
- **4.2 Asset and Configurationsmanagement (CMDB)**
- **4.3 Backup & Recovery**
- **4.4 High availability solutions, Disaster Recovery (DR)**
- **4.5 License management**
- **4.6 Analyse and use of (new) VMware Tools**

Auditing Virtual Servers, step 4 (2/5)

Attention points for operational risks:

- **4.1 Capacity management:**
  - Balance of virtual applications (VMs) utilisation over (a cluster of) ESX Servers:
    - A. Policy for the max. number of VMs and max. degree of server utilisation, B. Detailed capacity management with estimated high degree of capacity utilisation per application
  - Monitoring of capacity
  - Ressourcepool (Prioritising of applications / Distrib.Resource Scheduler Tool)
  - Clustering of ESX Servers („Fail-Over“)
  - Compliance-Aspekte: Which VMs on which ESX Servers?

- **4.2 Asset and Configurationsmanagement (CMDB):**
  - Compliance-Aspekte: Place of applications and data processing? Dynamically!

Auditing Virtual Servers, step 4 (3/5)

- **4.3 Backup & Recovery:**
  - Backup requirements
  - Backup policies: Use and dependencies between VMware Consolidated Backup (VCB), VM Snapshots, Tape Backup
  - Different elements: Virtual applications (VMs), ESX Operating System, Virtual Center Software
  - Secure communication from backup agents to datastores?
  - In Scope of the audit? Separate audit?

- **4.4 High availability solutions, Disaster Recovery (DR):**
  - High availability policy
  - Where are the applications in case of a DR?
  - Use of VMware SRM Tool for standardising of DR steps

Auditing Virtual Servers, step 4 (4/5)

4.5 License management

- Compare existing licenses (the number can change rapidly!) in the Virtual Center) with supplier contracts
- License optimisation policy (great differences between Vmware license models Vsphere V4 (powered on VMs), V5 (use of RAM). In V5, you could limit the RAM of the resource pool in a cluster to set a max. for test VMs.

4.6 Analyse and use of (new) VMware Tools:

- Evaluating process for new functionalities, like:
  - Vshield zones (virtuelle Firewalls),
  - Distributed switch / Private Virtual LAN (PVLAN),
  - Fault tolerance,
  - VM Converter,
  - Linked mode für Virtual Center,
  - Guided consolidation
  - etc.

Auditing Virtual Servers, step 4 (5/5)

- **Out of scope of the audit?:**
  - Development, test and staging into production of virtual applications (VMs):
    - Change and Test Management of VMs (requests, approval, versioning)
    - Use of standard VM templates
    - VMware Vcenter Stage Manager
    - VMs storage
    - In scope of the audit? Separate audit?

Questions / Discussion

gert-jan.timmer@axa-tech.com

Gert-Jan Timmer RE CIA CISA

Past:

- Studied Business Informatics
- Post-Academic studies: IT-Auditing at the Erasmus University in Rotterdam and at the Vrije University in Amsterdam (AO)
- Work experience since 1992: PwC, KPN, ACS, Achmea and AXA in several functions (financial, operational and especially in IT-Auditing and consulting)
- Teacher IT-Auditing study for post-graduates
- Member of the German IIA working group E-Commerce

Currently:

- Manager Internal Audit North-Europe in AXA Technology Services
- Leader of the German ISACA working group CobiT-CMMi
- Member of the German ISACA working group Cloud Computing
- Member of the German ISACA working group Academic Education: setting up and teaching the first master study IT Auditing in Germany