Virtualisation Security for Regulated Environments

AusCERT2011, Gold Coast, Australia

Conference Release, May 2011

Compliance, Protection & Business Confidence

Sense of Security Pty Ltd

Sydney
Level 8, 66 King Street
Sydney, NSW 2000,
Australia

Melbourne
Level 8, 350 Collins Street
Melbourne, Victoria 3000,
Australia

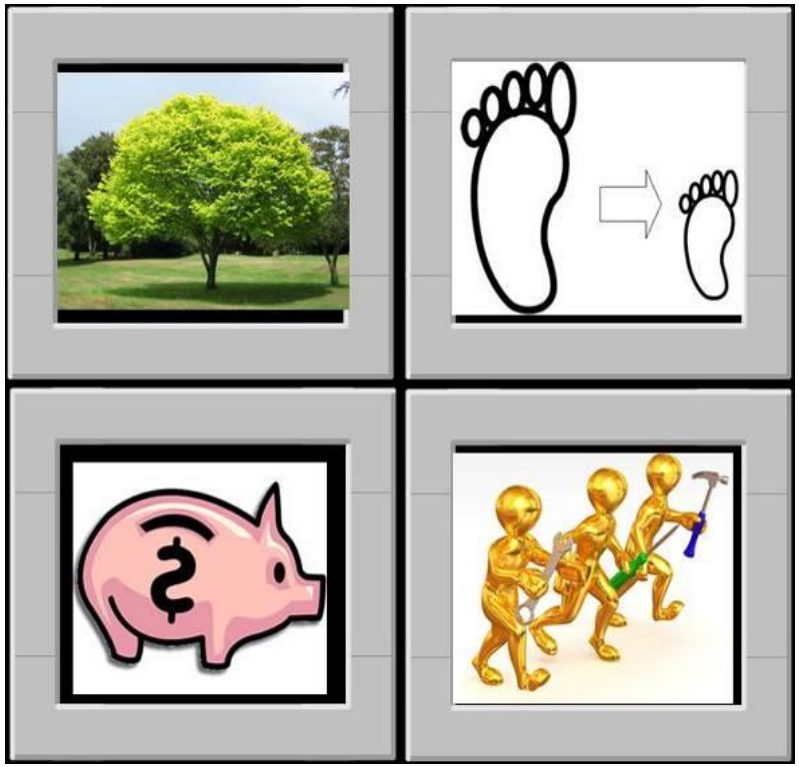
T: 1300 922 923
T: +61 (0) 2 9290 4444
F: +61 (0) 2 9290 4455

info@senseofsecurity.com.au
www.senseofsecurity.com.au
ABN: 14 098 237 908

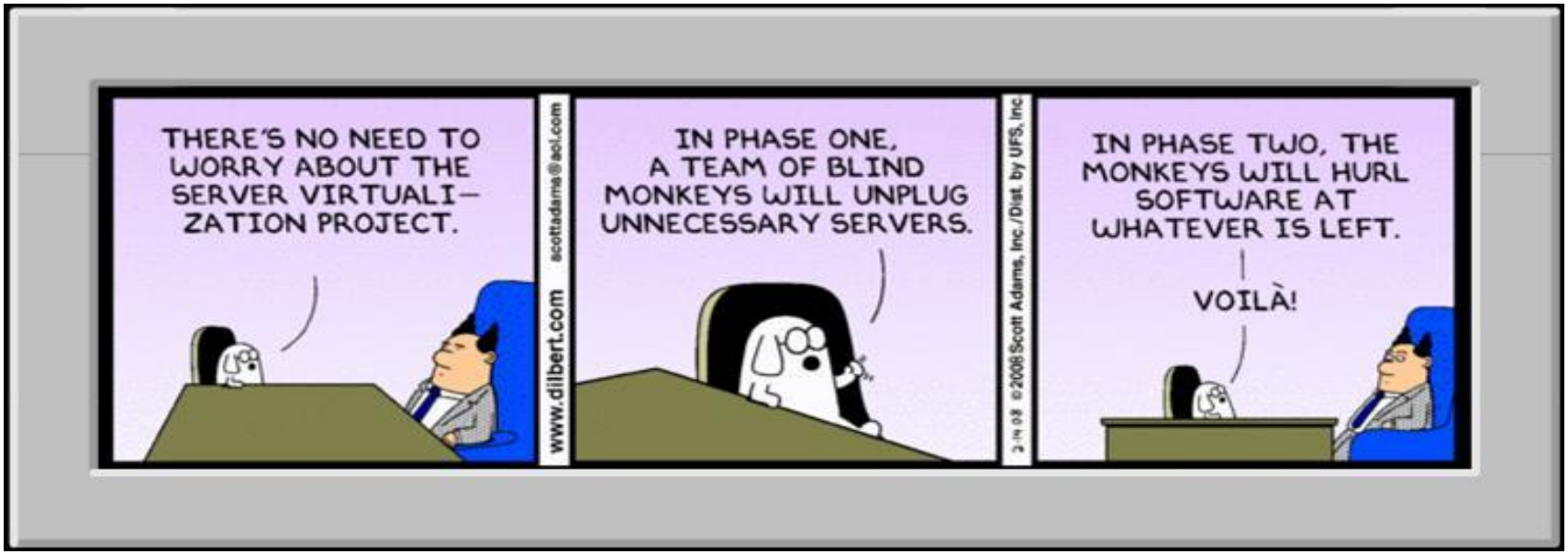
Agenda

- Introduction to Regulations
- Virtualisation Security Challenges
- Implications for Regulated Environments
- Be Prepared
- Conclusion

Virtualisation Benefits

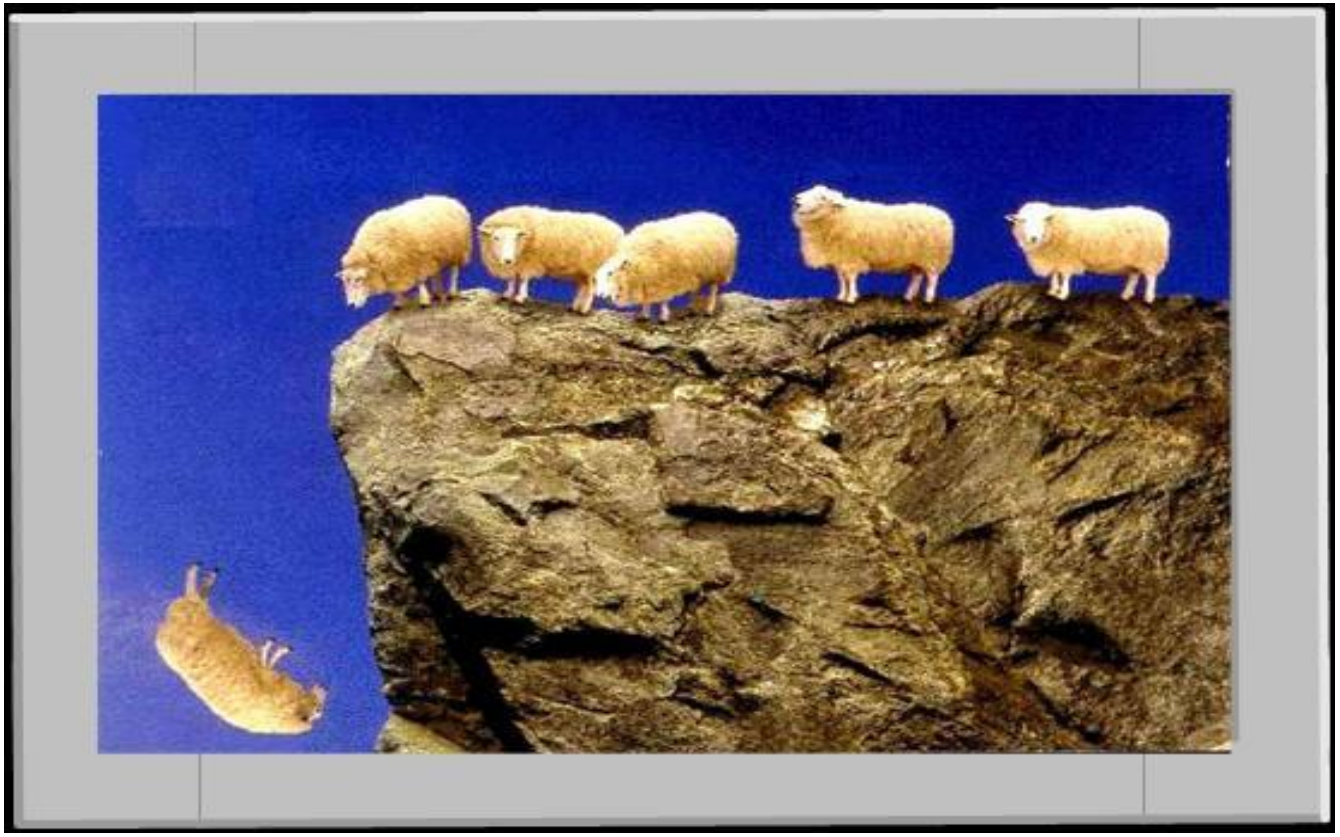


Even Dilbert's boss is onto this!



Licensed

It’s so easy, follow me



Virtualisation, Regulation & Guidance

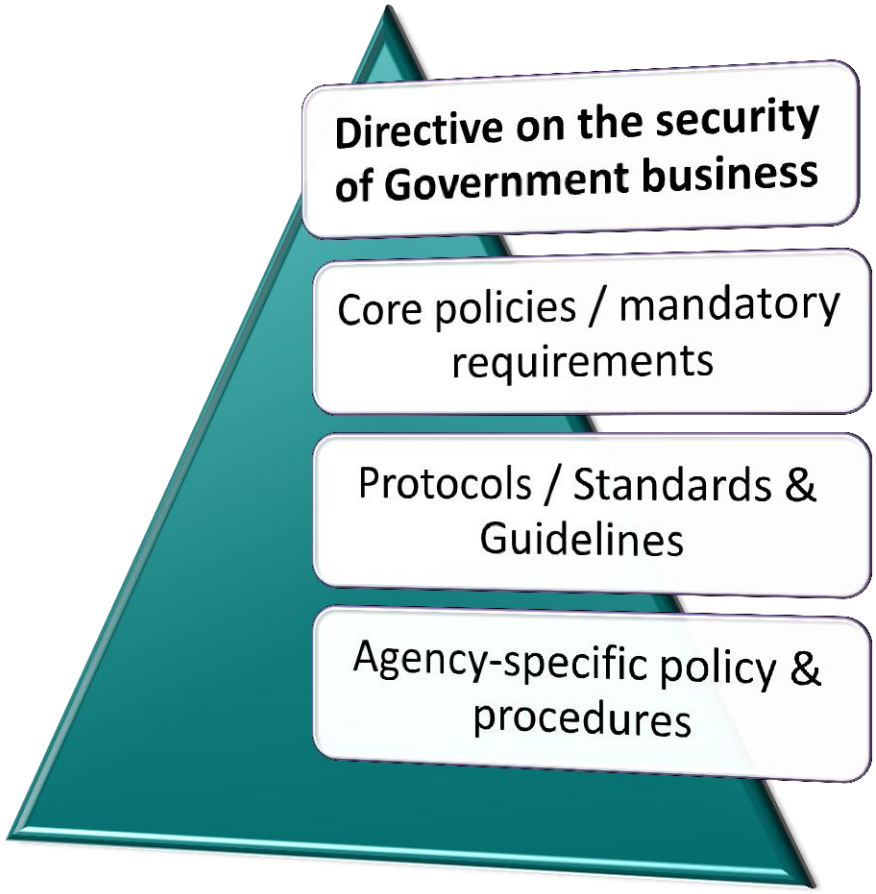
- Payment Industry
  - PCI DSS (2.0), Virtualization Special Interest Group (Info Supp and mapping tool due soon)
- Australian Government
  - ISM, PSPF, Cloud Computing Guidance (AGD, Dept of Finance, DSD)
- US Government
  - National Institute of Standards and Technology (NIST)
  - Federal Risk and Authorization Management Program (FedRAMP)
  - Defense Information Systems Agency (DISA)
- UK
  - CabinetOffice, G-Cloud
- Europe
  - FP7 – Seventh Framework Programme
  - European Network and Information Security Agency (ENISA)
- Other Guidance
  - Cloud Computing Alliance (useful mapping tools)

Cloud and Regulation – AU Govt

- Australian Government Cloud Computing Strategic Direction Paper [1]
  - WoG policy position on Cloud Computing: "Agencies may choose cloud-based service where they demonstrate value for money and adequate security*"
  - *adequate security requires meeting the mandatory requirements outlined in Protective Security Policy Framework (PSPF) [2]
  - Must ensure cloud service providers and their service offerings meet the requirements of the PSPF, the Australian Government Information Security Manual (ISM) and the Privacy Act 1988; and
  - With cloud computing, an agency may have limited ability to prescribe the protective security of the cloud environment. Yet agencies will remain ultimately responsible for the information that is stored and/or processed in the cloud. Management must maintain assurance that the security of the cloud service provider is in accordance with the PSPF.

[Ref: Australian Government Cloud Computing Strategic Direction Paper, Dept of Finance, April 2011 Version 1.] [1]

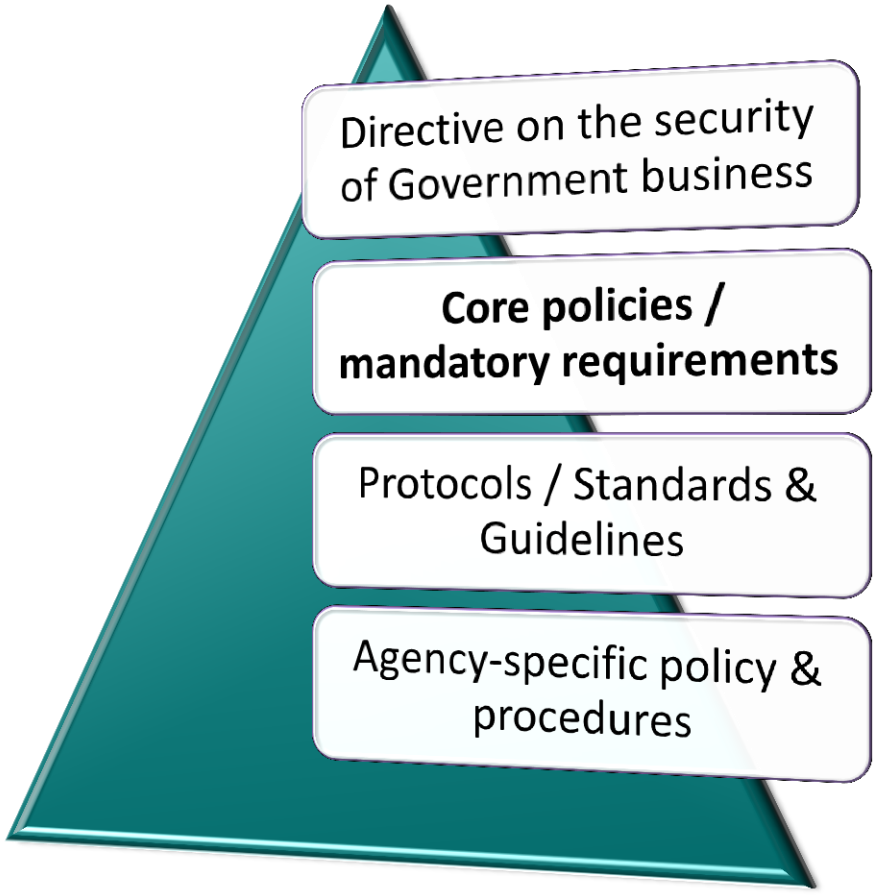
Cloud and Regulation – AU Govt



Protective Security Policy Framework [3]

Keystone: Articulates the Government's requirements for protective security to be a business enabler that allows agencies to work together securely in an environment of trust and confidence.

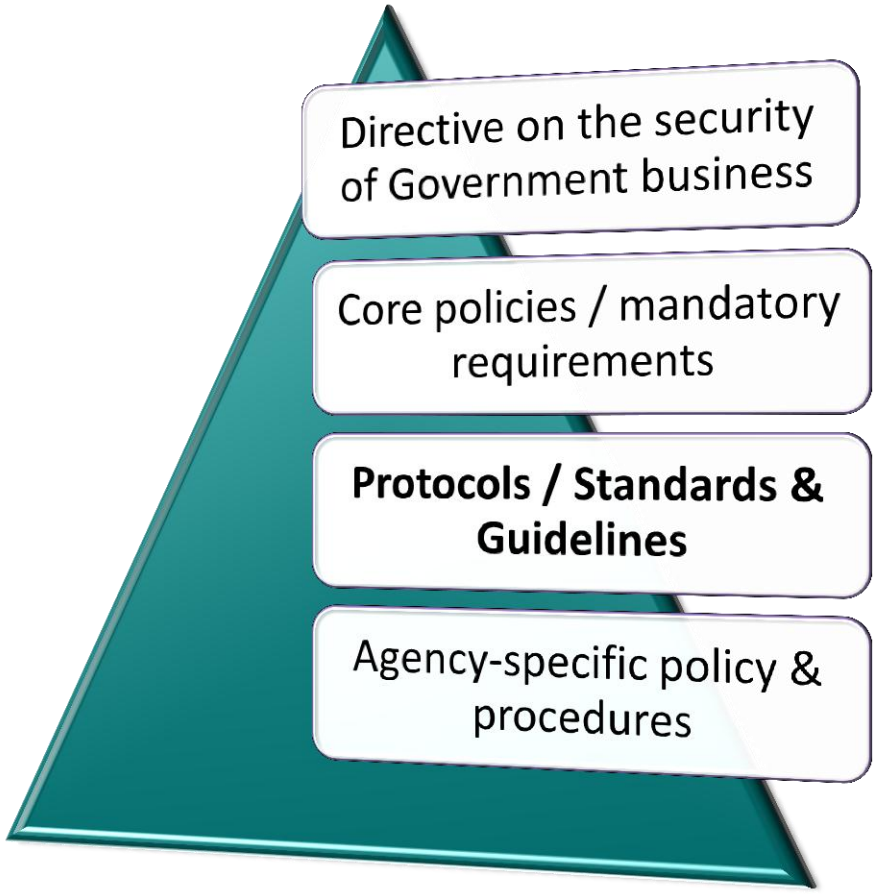
Cloud and Regulation – AU Govt



The core policy documents in the Framework describe the higher level mandatory requirements. All applicable agencies are to comply with the **mandatory** requirements. These requirements cover **Governance**, Personnel Security, **Information Security**, and Physical Security.

Protective Security Policy Framework [3]

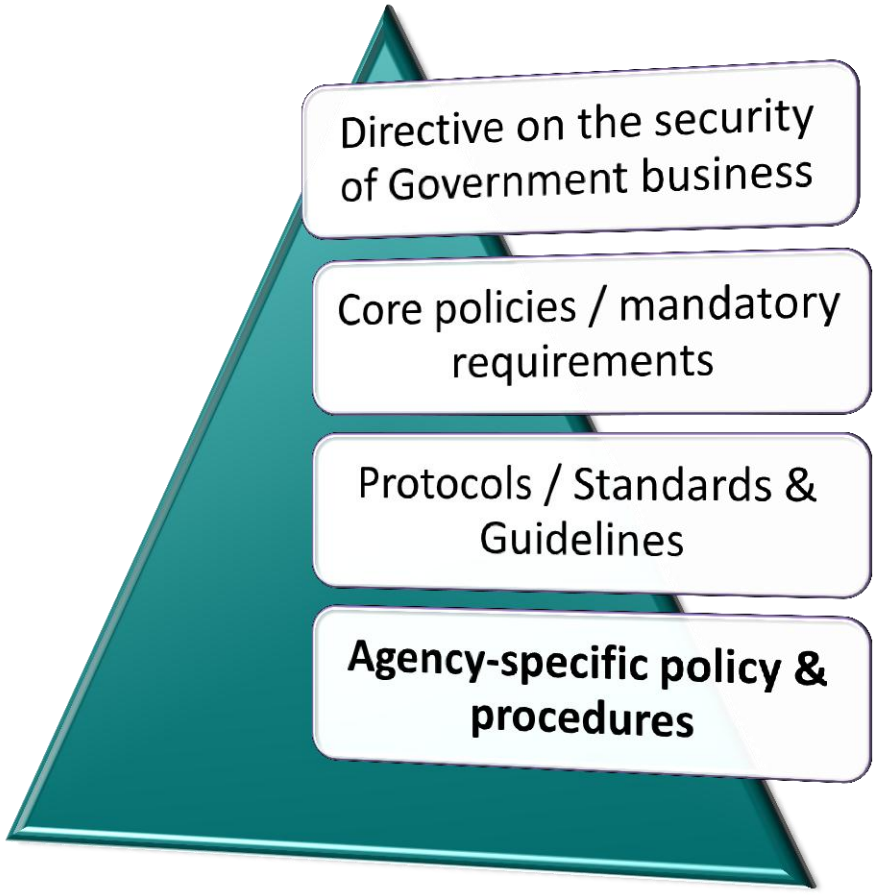
Cloud and Regulation – AU Govt



Protective Security Policy Framework [3]

…contain the key practice documents including:
the **information classification policy**, protocols for the conduct of Government specific protective security activities to meet the mandatory requirements

Cloud and Regulation – AU Govt



Protective Security Policy Framework [3]

…Agencies are to develop specific protective security policies

….. are to take into account the risks created by the agency for others, as **well as the risks inherited from business partners**.

Cloud and Regulation – AU Govt

- **3. Applicability of the Protective Security Policy [3]**

3.1 As a policy of the Australian Government, the following agencies must apply the Protective Security Policy to the extent that their enabling legislation allows:

- agencies subject to the *Financial Management and Accountability Act 1997*

bodies that are:

- subject to the *Commonwealth Authorities and Companies Act 1997*, and
- have received Ministerial direction to apply the general policies of the Australian Government
- other bodies established for a public purpose under a law of the Commonwealth and other Australian Government agencies, where the body or agency has received a notice from the relevant Minister that the Framework applies to them.

3.2 The Australian Government requires non-government organisations that access national security classified information to enter into a Deed of Agreement to apply the Protective Security Policy.

3.3 The Commonwealth expects state and territory government agencies that hold or access national security classified information to apply the PSP.

[Ref: Securing Government Business. Protective Security Guidance for Executives, AGD] [3]

Cloud and Regulation – AU Govt

- Sample of Mandatory Reqs [2]:
  - document requirements for information security when entering into outsourcing contracts …
  - specifying the necessary protective security requirements in the terms and conditions of any contractual documentation, and
  - undertaking assessments visits to verify that the contracted service provider complies with the terms and conditions of any contractual documentation.
  - put in place comprehensive systems maintenance processes and procedures including operator and audit/fault logs and information backup procedures
  - take all reasonable steps to monitor, review and audit agency information security effectiveness, including assigning appropriate security roles and engaging internal and/or external auditors and specialist organisations where required
  - identify and implement access controls including access restrictions and segregation/isolation of ICT systems into all infrastructures, business and user developed applications.
  - The policy and procedures are to …. identify protective security roles and responsibilities

[Ref: Australian Government Protective Security Policy Framework, AGD, Jan 2011, V1.2] [2]

Tactical Application of Cloud by Govt

Layer	Example	Data Centre with Adv. Virtualisation	Private Cloud	Hybrid cloud	Community Cloud (Incl. G-Cloud)	Public Cloud
Information and Services layers						
Citizen-facing services	Citizen-driven (joined-up) service delivery (lines of business)	Now-5 years	Now-5 years	Now-5 years	Now-5 years	3- 5 years
Business Processes	Consolidated or shared business processes, for example, Financial, HR, Budgeting, Procurement, content management, case management	Now-5 years	Now-5 years	Now-5 years	Now-5 years	3-5 years
Applications	Custom applications/Packaged applications/external services	Now-5 years	Now-5 years	Now-5 years	Now-5 years	3-5 years
Citizen Information	Concerns individual citizens, covered by privacy and data protection (security)	1-2 years	1-2 years	3-5 years	3-5 years	6-10 years
Public Information	Open government data / mashups Collaborative tools, e.g. blogs, wikis, data.gov.au					Now
Technology layer						
Channels (online)	Government websites and portals Web2.0 technologies (e.g. gmail) Discovery tools, for example Google Search			Now		Now
Technology (Infrastructure)	IT and telecommunication infrastructure – utility model	Now	Now	Now	Now	Now
Technology (process / storage capability)	Process and analyse large datasets Use as a storage platform	Now	Now	Now	Now	Now

Tactical Application and Use of Cloud by Government at the Information and technology layers [2]

Cloud and Regulation – AU Govt

- Cloud Computing Security Considerations, DSD [4]

Risk Management,

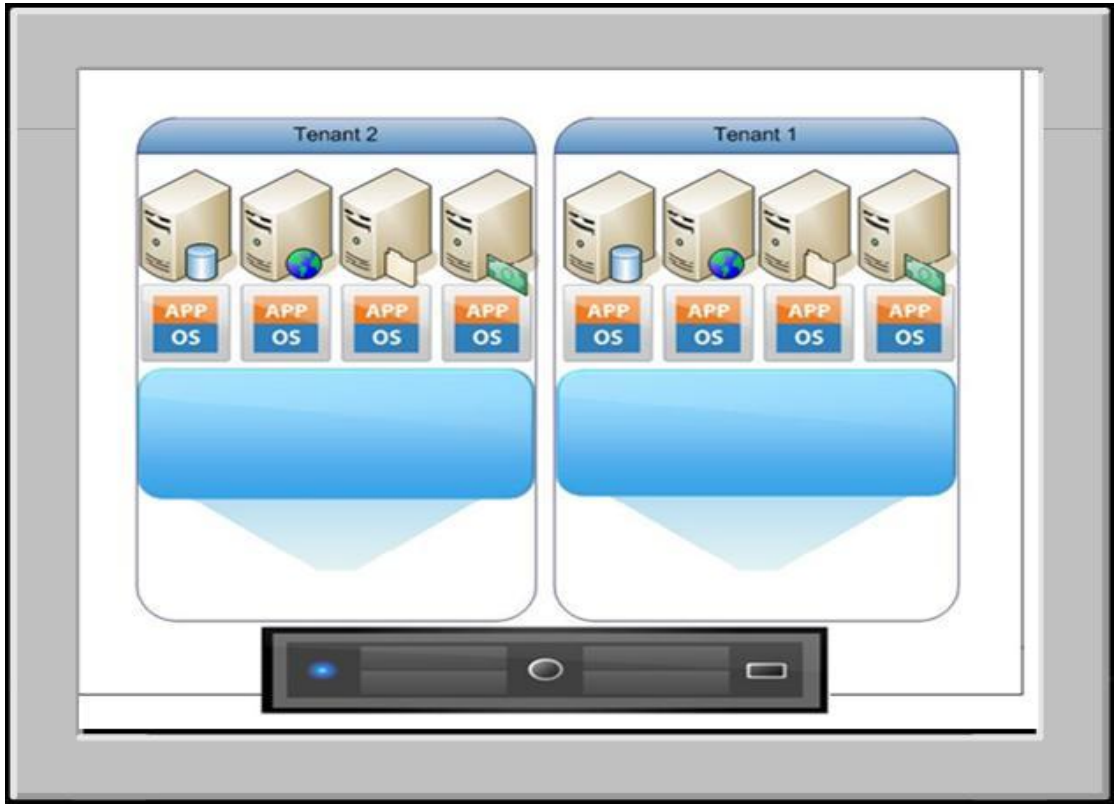
"15. The contract between a vendor and their customer must address mitigations to governance and security risks, and cover who has access to the customer's data and the security measures used to protect the customer's data. Vendor's responses to important security considerations must be captured in the Service Level Agreement or other contract, otherwise the customer only has vendor promises and marketing claims that can be hard to verify and may be unenforceable."

"16. In some cases it may be impractical or impossible for a customer to personally verify whether the vendor is adhering to the contract, requiring the customer to rely on third party audits including certifications instead of simply putting blind faith in the vendor."

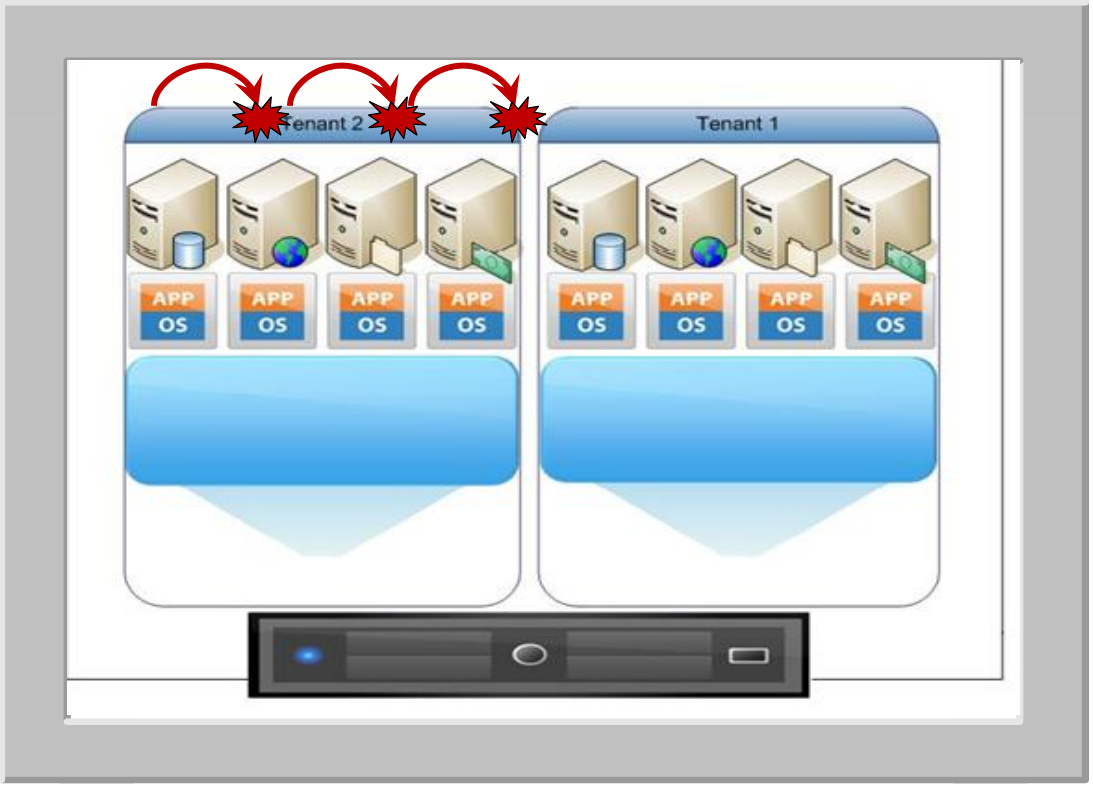
Review the checklist in this document for security considerations.

[Ref: Cloud Computing Considerations. DSD, April 2011] [4]

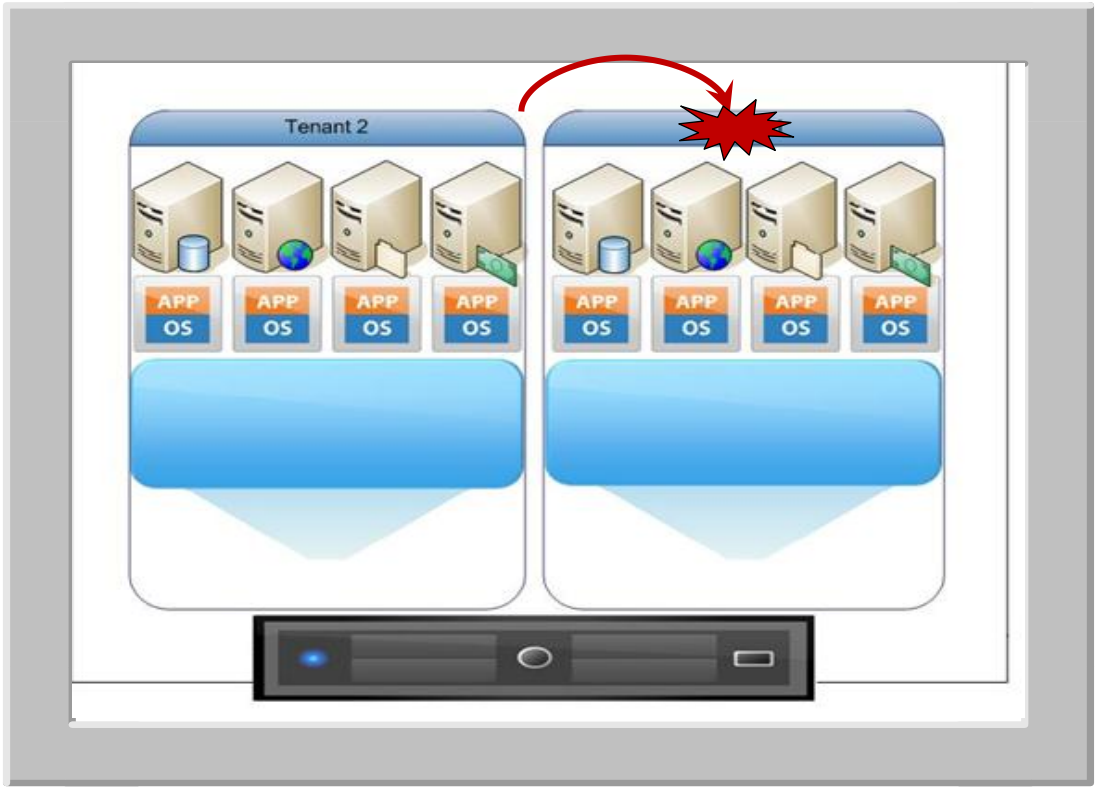
Sample Scenario – Multitenant or Internal



Guest to Guest Compromise



Guest to Guest - Inter-tenancy Compromise

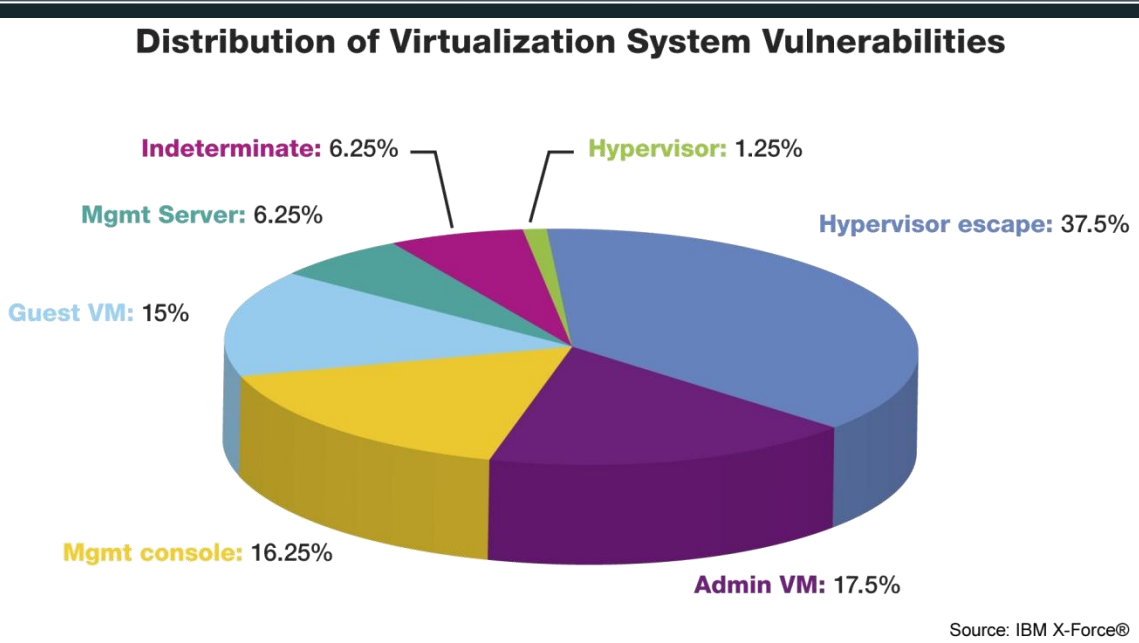


Guest to Host (HV) - Worst Case

How does it happen?

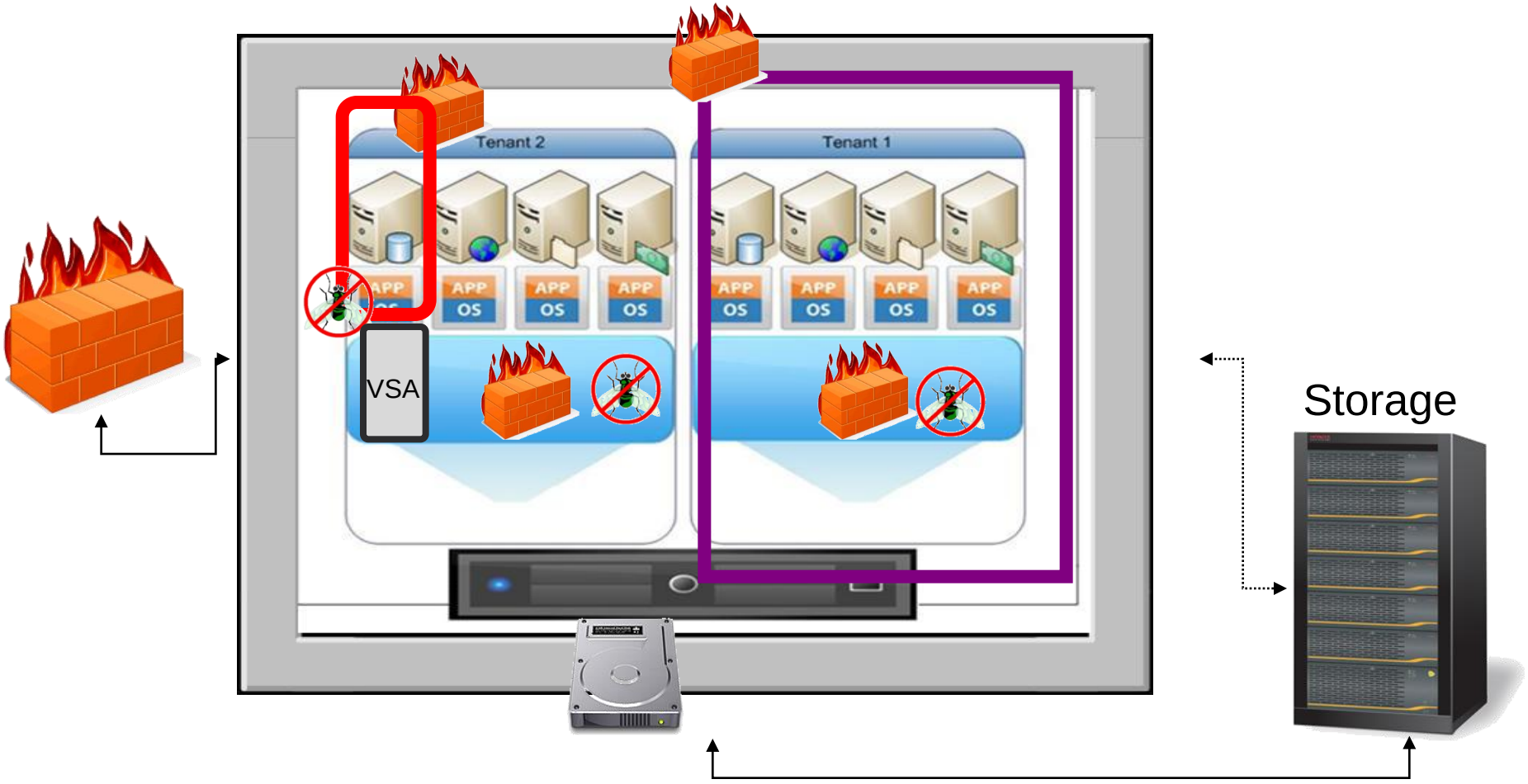
- Hypervisor should prevent guest-to-guest or guest-to-host compromise
- However, if mis-configured isolation may not be effective
  - Poor setup of virtual networking
  - Optional features such as drag-and-drop, clipboard sharing etc. may break isolation
  - No secured management VLAN
  - Hypervisor & guest itself not secured
  - Ineffective controls to protect Hypervisor & guest (patch mgt, access control, auth)
  - Root Hypervisor Vulnerability

Vulnerabilities & public exploits



"Of particular note here are the first two classes of vulnerabilities. **The most common class of vulnerabilities in server class virtualization products, hypervisor escape vulnerabilities, generally represents the most serious risk to virtualization systems as these vulnerabilities violate the principal of isolation of virtual machines**. The next largest class of vulnerabilities, administrative VM vulnerabilities, also present serious risk, as these can provide control over the configuration of the entire virtualization system."
[IBM XForce 2010 Trends Report] [5]

Where is the protection applied?



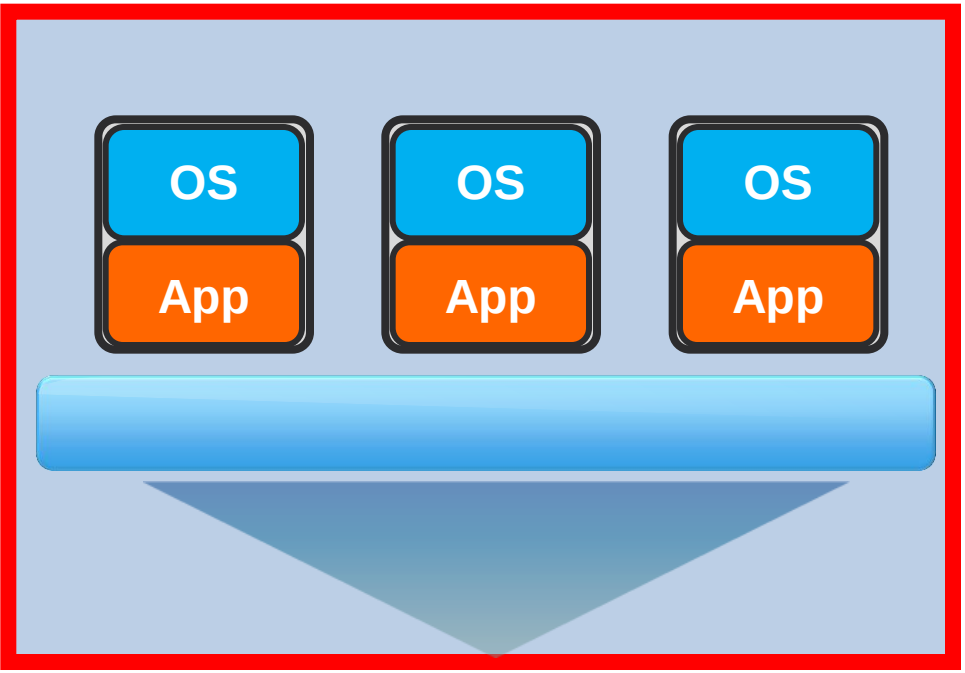
The Solution?

- Physically isolate zones of trust (CDE and non CDE for PCI DSS)?
- Co-hosted but isolated? Separate Virtual Switches?
- Risk Assessment (ISM Control: 0750; PSPF Gov-6, NIST, PCI DSS Req 12.1.2 and defined in VSIG guidance)
- In the case of virtualised "mixed mode" implementations, the risk assessment must demonstrate the segmentation has been achieved at a level that meets or exceeds PCI Reqs.

Mixed Mode - Multitenant

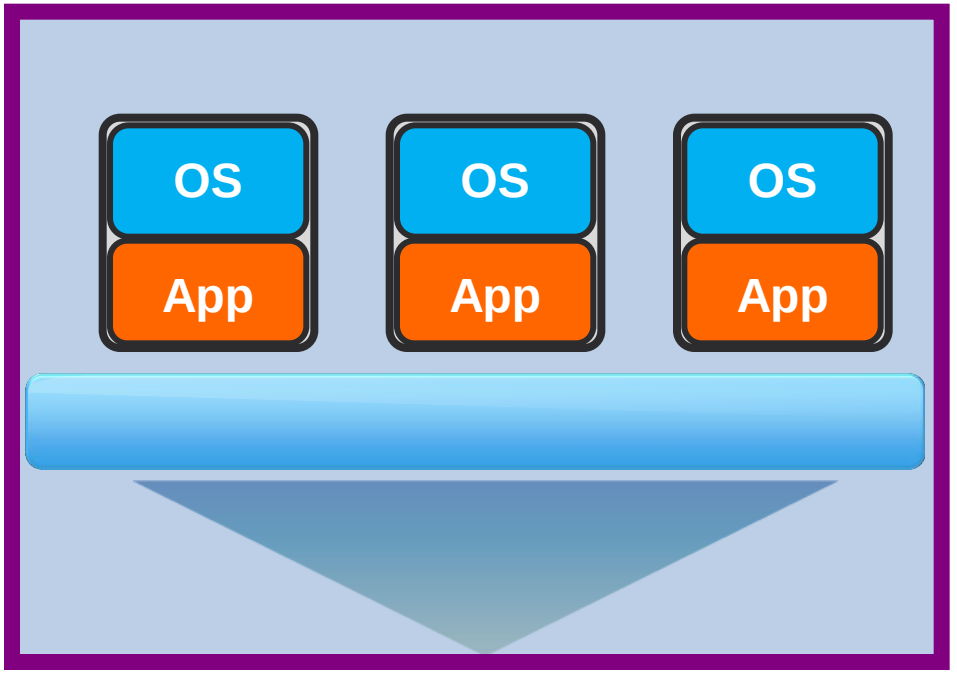
Cardholder Data Environment

Tenant 1



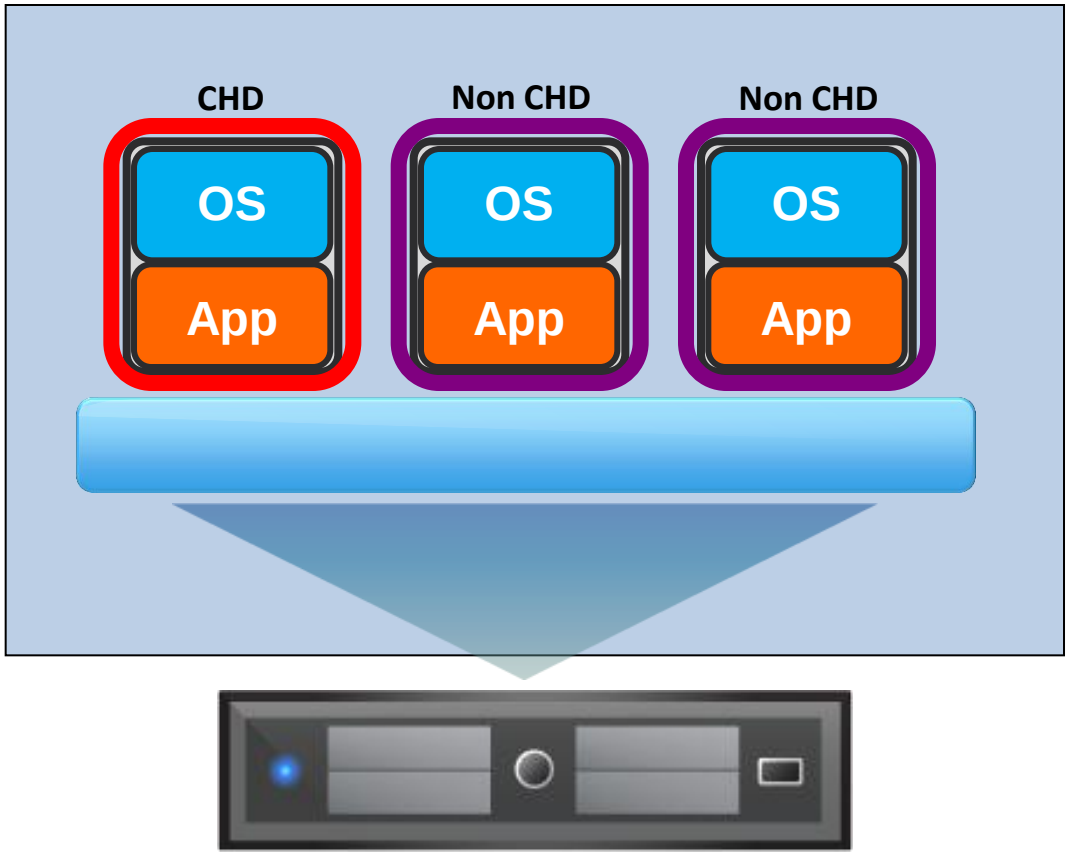
Non Cardholder Data Environment

Tenant 2

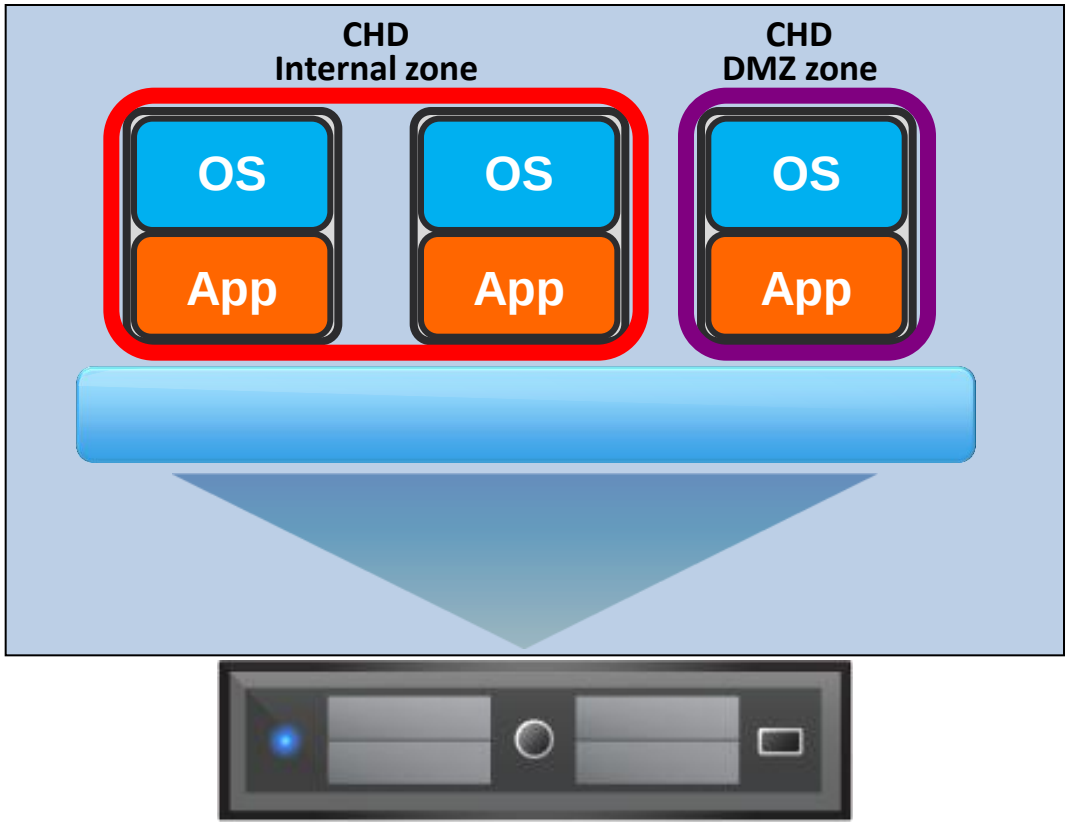


Mixed Mode Single Tenant

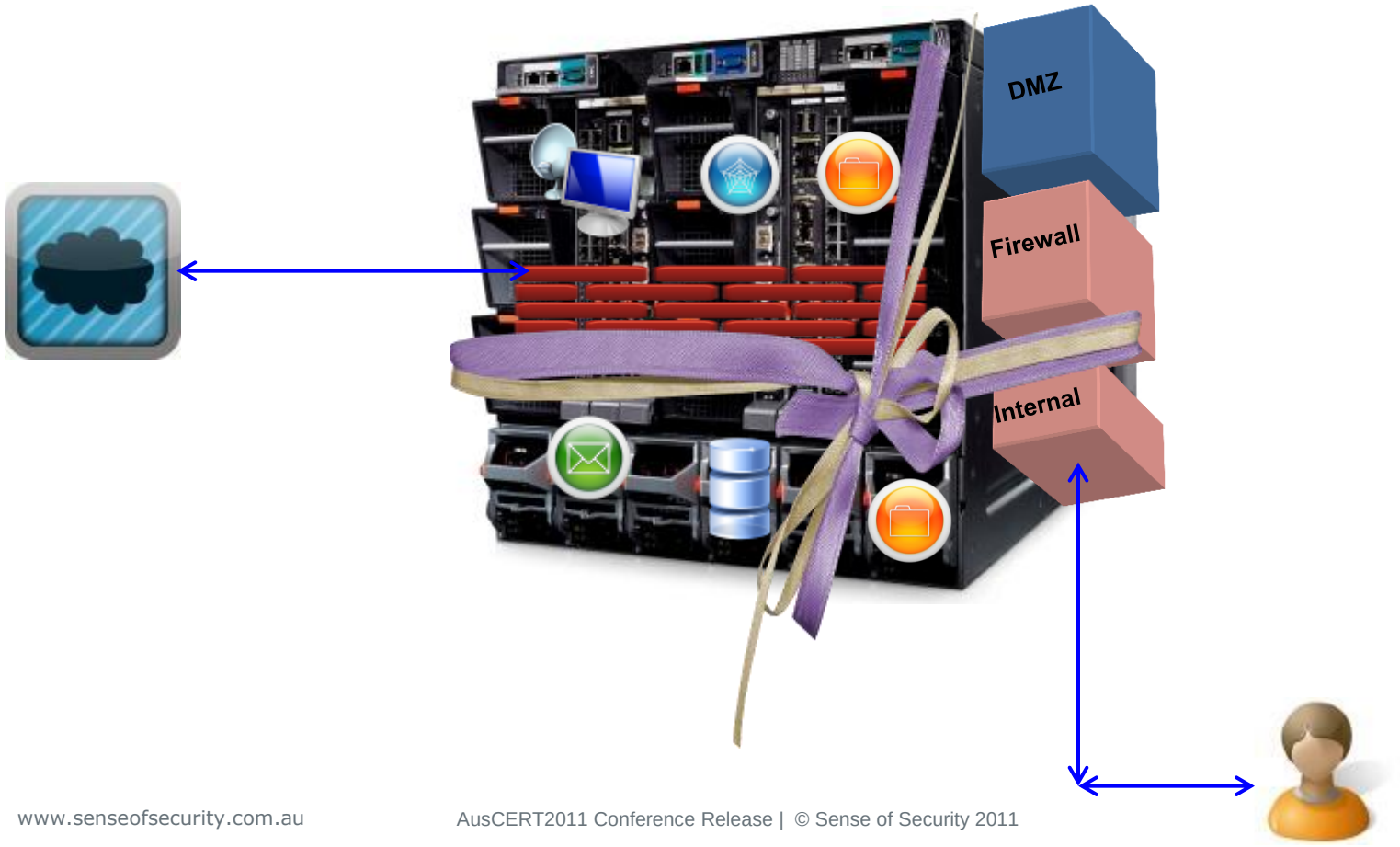
Tenant 1



Mixed Mode CHD Environment



Company in a box



Is it getting crowded in there?

NIST Requirements

However, there can be substantial security risks in consolidating multiple services within a single hypervisor. For example, a critical service is usually placed on its own dedicated host so that the host can be secured specifically for that service and so that a compromise of any other service would not impact the critical service. By placing a critical service on a host with other services, both of those goals are impacted. It is particularly risky to place multiple services on a host if they have significantly different security needs. For example, suppose that one service is considered critical and is secured very strongly, while another service on the same host is considered low-impact and is secured relatively weakly. An attacker wanting to compromise the critical service could compromise the low-impact service and use the fact that it is local on the virtual network to attempt to access the critical service or to compromise the hypervisor and thus gain access to the critical service. Organizations that have policies relating to allocation of computer resources should consider virtualization in such policies.

[REF NIST - Guide to Security for Full Virtualization Technologies SP 800-125] [6]

NIST Requirements

Organizations should be aware of how their use of virtualization may affect the security categorization of the physical system. The security categories associated with Federal information system based on three security objectives: confidentiality, integrity and availability. These security categories are described in NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems.* The security categorization of a particular information system depends on the potential impact associated with a loss of confidentiality, integrity or availability. If a system hosts guest OSs with different impact levels, the system should be secured in accordance with the highest of those levels. The organization's virtualization security policy should define how combining multiple guest OSs on a single system affects the system's security requirements, both positively and negatively, and which combinations of guest OSs are permitted or prohibited. Organizations may also choose to reduce risk by prohibiting combinations that include resources accessing particular types of information, such as highly sensitive personally identifiable information (PII).[3]

[REF NIST - Guide to Security for Full Virtualization Technologies SP 800-125] [6]

ISM Requirements

Functional separation between servers

Control: 0385; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Where high value servers have connectivity to unsecured public networks, agencies should:

- maintain effective functional separation between servers allowing them to operate independently
- minimise communications between servers at both the network and file system level as appropriate
- limit system users and programs to the minimum access needed to perform their duties.

Control: 0953; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended

It is recommended agencies ensure that functional separation between servers is achieved either:

- physically, using single dedicated machines for each function
- using virtualisation technology to create separate virtual machines for each function in the same security domain.

[REF: Australian Government Information Security Manual - November 2010] [7]

ISM Requirements

Using virtualisation for functional separation between servers

Control: 0841; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should not

Virtualisation technology should not be used for functional separation between servers in different security domains at the same classification.

Control: 0842; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must not

- Virtualisation technology must not be used for functional separation between servers of different classifications.

[REF: Australian Government Information Security Manual - November 2010] [7]

Stealing a Physical Machine

VERY DIFFICULT

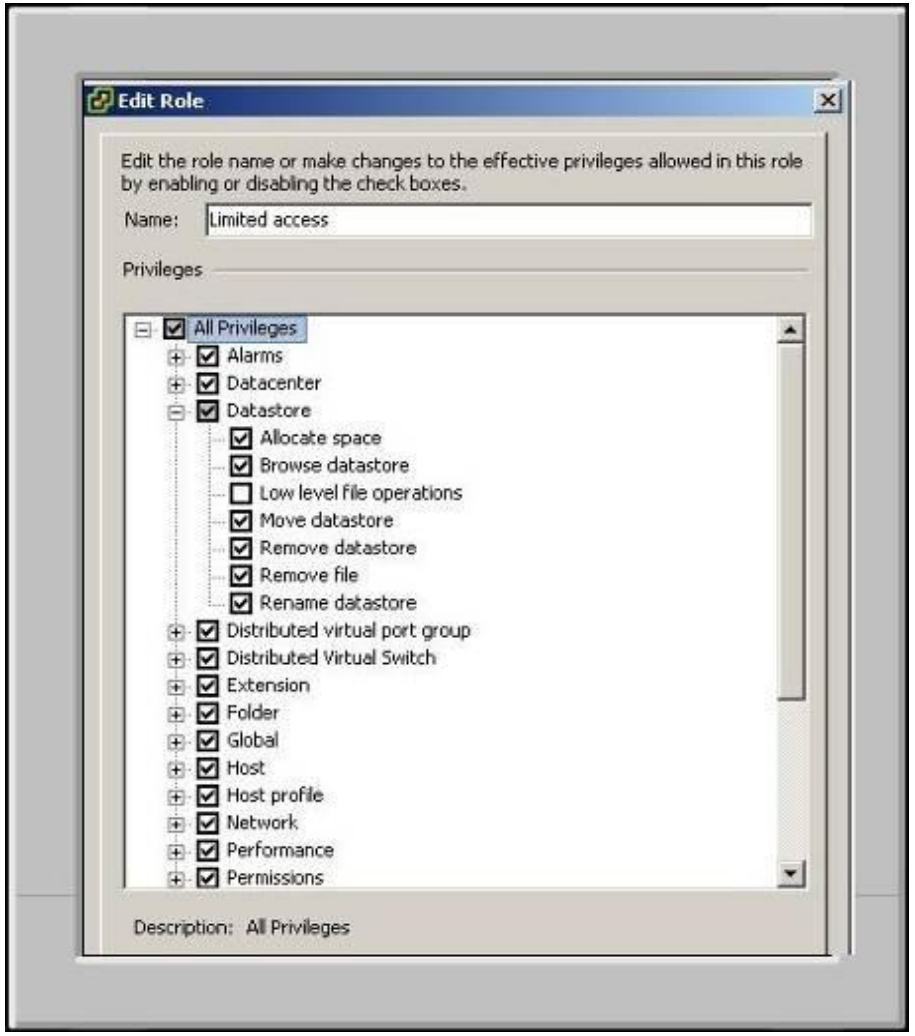
Stealing a Virtual Machine

- Take a snapshot of the machine
- After snapshot virtual disk is unlocked
- Copy to removable media
- Mount VM, access to virtual disk
- If credentials are not known - boot using recovery tool; change admin password
- If credentials are known - power on with player

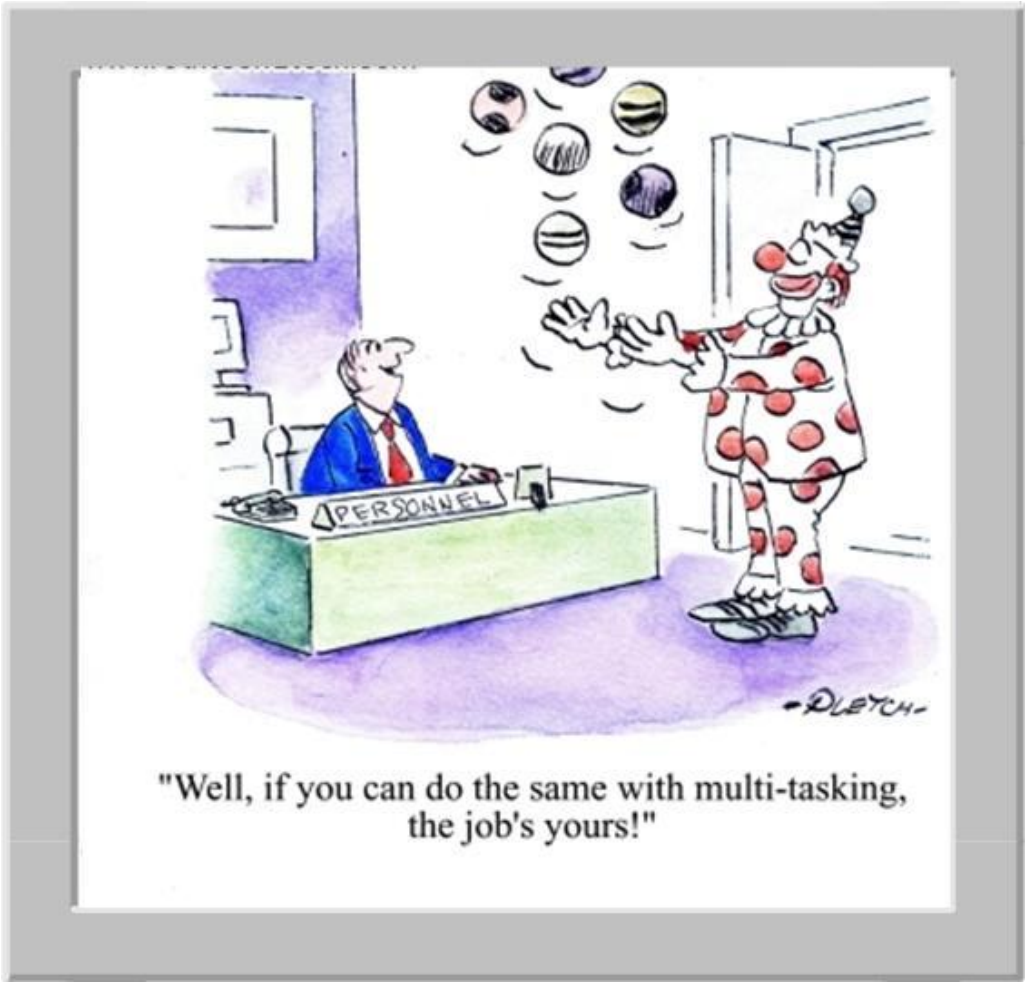
See video at: http://www.senseofsecurity.com.au/consulting/virtualisation-security

Protection

- Encrypt Data
- Improve RBAC – restrict access to low level file ops
- Restrict access to Service Console
- Implement controls for access, accountability, and visibility



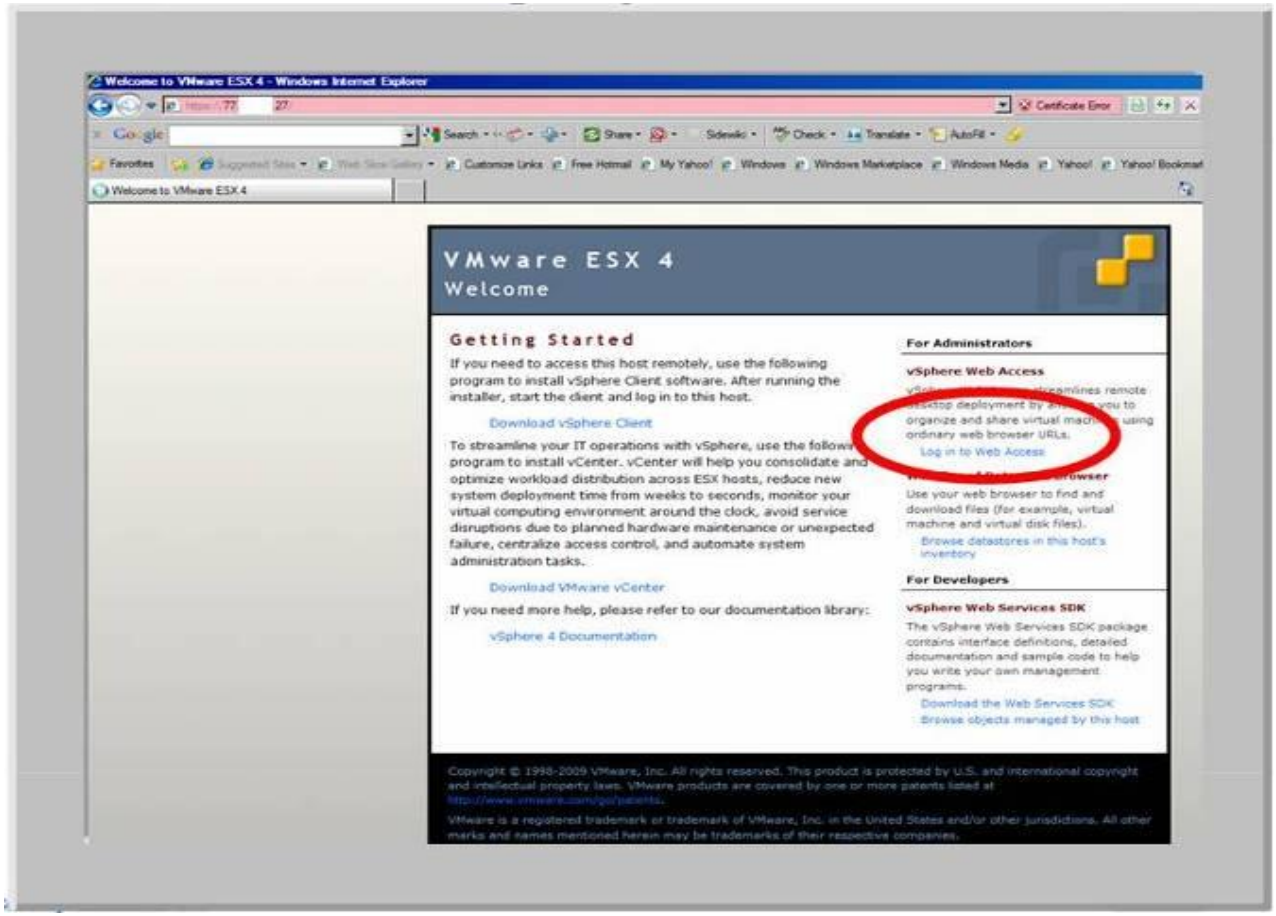
Who manages the system?



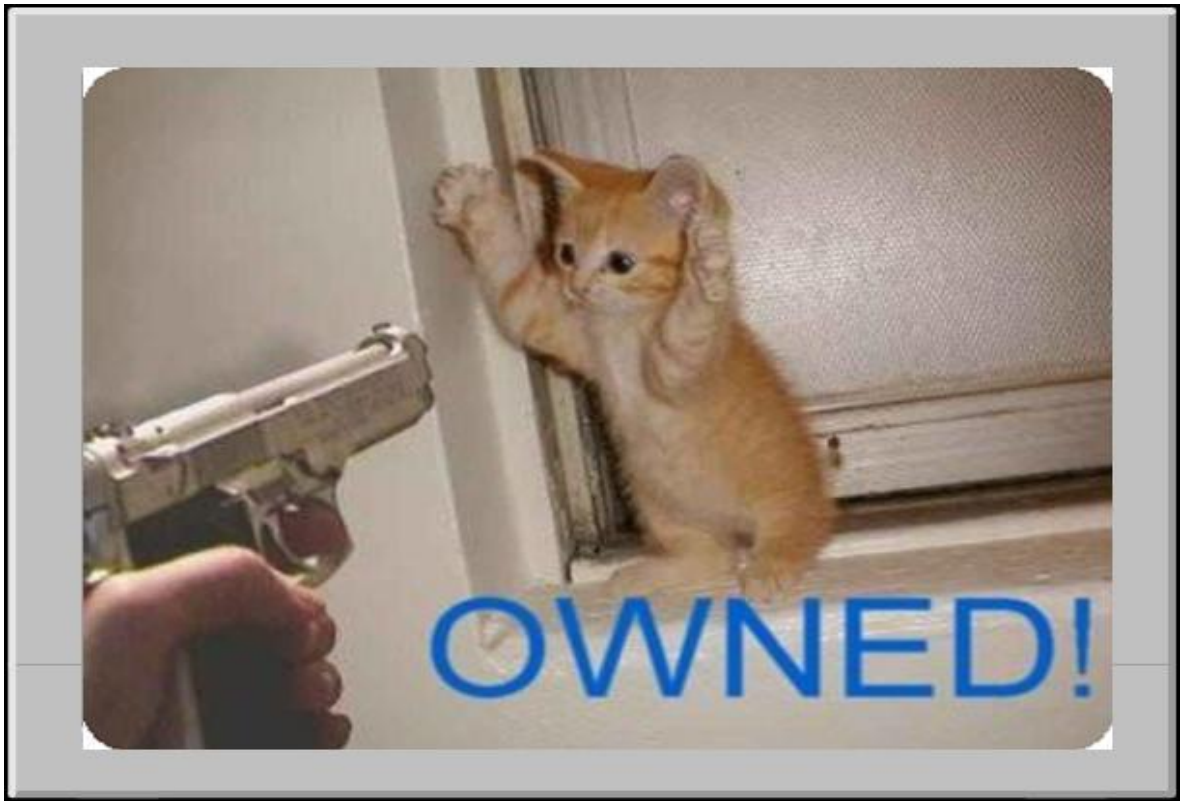
Segregation of Duties

- Server, storage, network, and security duties are collapsed
- Critical considerations:
  - Role-mapping within IT
  - RBAC capabilities of virtualisation platform
  - Layered controls (prevent, detect, respond)
  - Must enforce least privilege
- Roles and Responsibilities
  - Review of discrete responsibilities assigned to roles

Too Accessible?



This is a good start to getting ….



System Components

- The PCI DSS security requirements apply to all system components that are included in or connected to the cardholder data environment.
- For virtualised environments this should include:
  - ANY Virtual Machine
    - Network Component (Vswitch; router)
    - Server (One Primary Function per VM)
    - Application
  - Virtual Appliance
    - Servicing CDE
    - Hooks into hypervisor
    - Security Appliances (Firewall, IPS, AV etc)
  - Hypervisor
  - Third Party Components
  - Virtual Applications (e.g. for Point of Sales)

Hypervisor Protection

- Choice of Hypervisor
  - See industry radar at http://virtualization.info/en/radar/

- References to PCI DSS Requirements
  - Secure Configuration (Hardening, Disable unnecessary services etc) (2.2.X)
  - Encryption of non-console administrative traffic (2.3)
  - Anti Virus (5.1)
  - Patch Management, HV is a new dimension (6.1)
  - Identify new vulnerabilities (6.2)
  - Restrictive access (7)
  - Effective user authentication (8.5)
  - Audit trails for all changes (10)

Other Virtualisation Considerations

- Dormant VM's
  - Audit trails required for access to all dormant machines (10)
  - May include Cardholder Data, encryption keys (3)
  - How do you address retention and destruction? (9.10)

- Virtual Media
  - SAN/NAS? Management Networks?
  - If NAS will require additional isolation and controls
  - VM's are just files on disks
  - Access controls apply (7)
    - Master images, images with CHD
  - Physical controls apply (9)

Other Virtualisation Considerations

- Change Management
  - VMSprawl must be managed particularly for VM's with CHD
  - Movement from Dev to Test to Production must be controlled
  - Snapshot and rollback may inadvertently re-instate and non-compliant image
  - Enrolment & retirement must be controlled

Other Virtualisation Considerations

- Audit and Logging
  - The entire environment should be auditable
  - All activity should be logged and monitored
  - Administrators/Auditors should be able to produce compliance reports at any point in time
  - Native and Commercial tools can be used

Audit Items

- Risk Assessment
- Network, LAN, WAN controls
- Infrastructure Readiness & Scope: Dev, UAT, Prod
- System Level & Data Classification
- Documentation: Applicability in policies, standards, procedures
- Specific Controls: Standard specific, deviation management
- Administrative Access; Remote Access
- Logical Access Controls, RBAC
- Intersystem connectivity
- Auditing and Logging
- Backups
- Integrity Monitoring (VM's and VMM)
- Vulnerability Management, Patch Management

[Ref Auditing Security Risks in Virtual IT Systems, ISACA Journal] [8]

Summary of Issues

- Effectiveness of Technical Controls
- Effectiveness of Governance and Risk Management
- Trust & Ownership
- Hypervisors
- Disclosure & Visibility
- Audit, Reporting, Compliance

References

- References:

[1] Australian Government Cloud Computing Strategic Direction Paper, Dept of Finance, April 2011 Version 1.
http://www.finance.gov.au/e-government/strategy-and-governance/docs/final_cloud_computing_strategy_version_1.pdf

[2] Australian Government Protective Security Policy Framework, AGD, Jan 2011, V1.2
http://www.ema.gov.au/www/agd/agd.nsf/Page/ProtectiveSecurityPolicyFramework_Contents

[3] Securing Government Business. Protective Security Guidance for Executives, AGD, June 2010
http://www.ag.gov.au/www/agd/agd.nsf/Page/ProtectiveSecurityPolicyFramework_ProtectiveSecurityPolicyFrameworkDownloads

[4] Cloud Computing Considerations. DSD, April 2011
http://www.dsd.gov.au/publications/Cloud_Computing_Security_Considerations.pdf

[5] IBM XForce 2010 Trends Report, March 2011
http://xforce.iss.net/

[6] Guide to Security for Full Virtualization Technologies SP 800-12, NIST, Jan 2011
http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf

[7] Australian Government Information Security Manual - November 2010]
http://www.dsd.gov.au/publications/Information_Security_Manual_2010.pdf

[8] Auditing Security Risks in Virtual IT Systems, ISACA Journal Vol 1, 2011

Thank you

The latest version of this presentation should be downloaded from
http://www.senseofsecurity.com.au/research/presentations

Murray Goldschmidt
Chief Operating Officer
Sense of Security
murrayg@senseofsecurity.com.au
+61 2 9290 4444

Recognised as Australia's fastest growing information security and risk management consulting firm through the Deloitte Technology Fast 50 & BRW Fast 100 programs

T: 1300 922 923
T: +61 (0) 2 9290 4444
F: +61 (0) 2 9290 4455
info@senseofsecurity.com.au
www.senseofsecurity.com.au