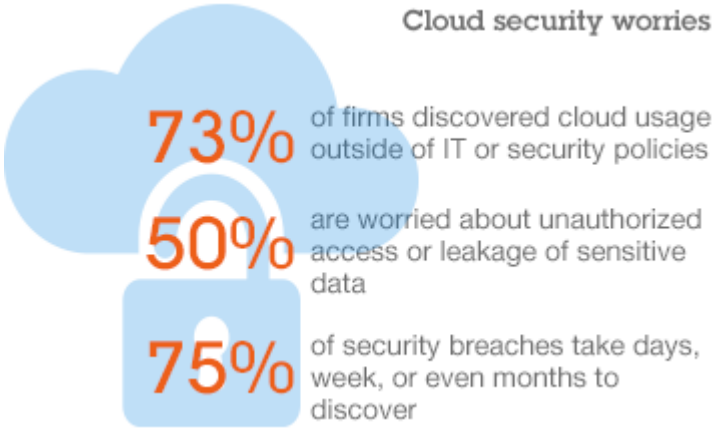
"The cloud is an opportunity to rethink security."

–Raj Nagaratnam

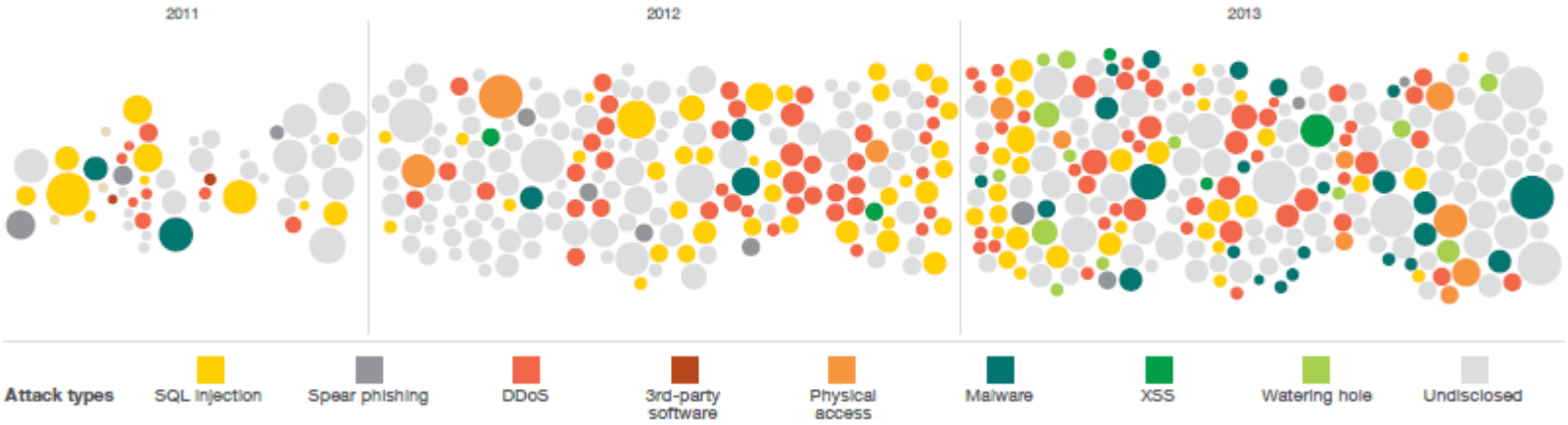
Cloud Security

Agenda

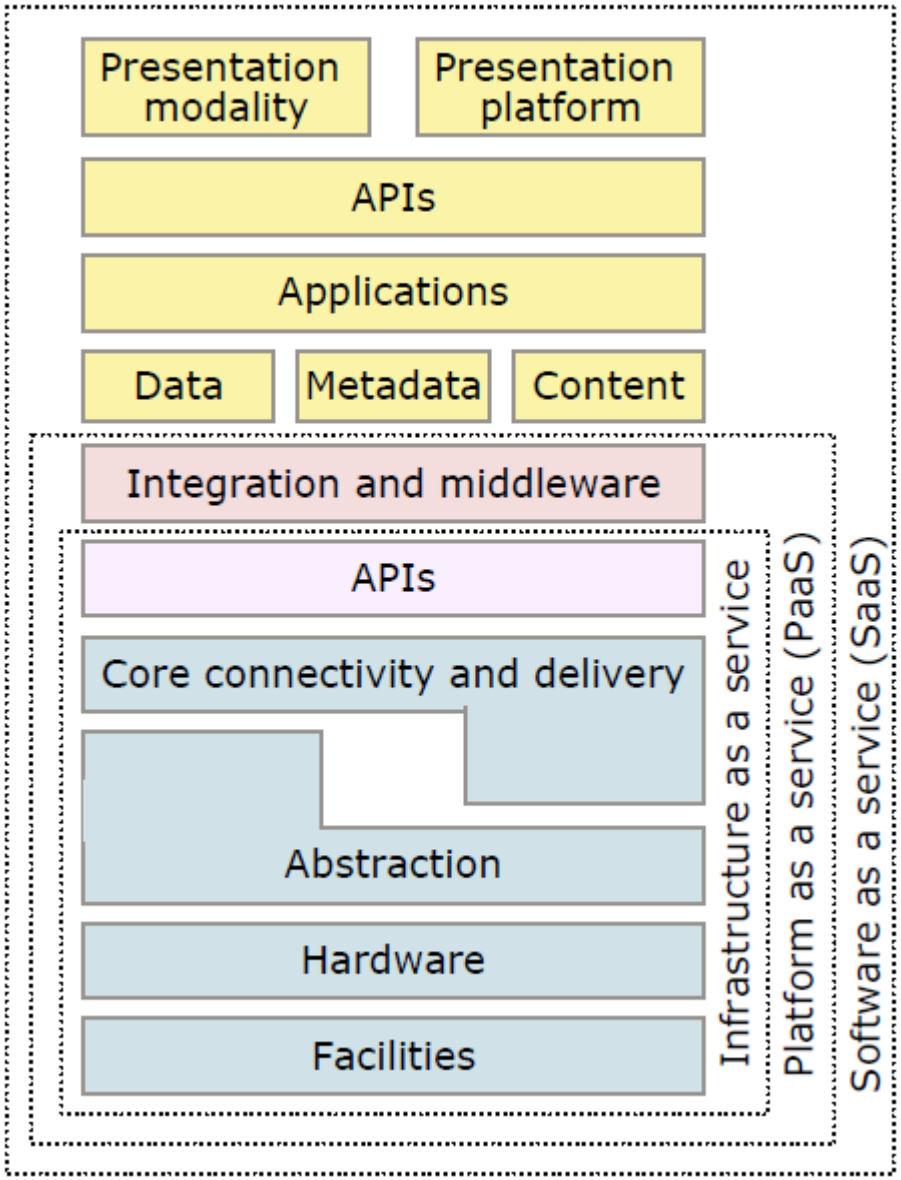
- Cloud security – inheritance
- Security responsibility – private vs public
- General areas of concerns
- Key security dangers to cloud computing
- Cloud Security framework / standards
- Cloud Security Implementation
- Data privacy
- Security concerns – examples & quiz



A historical look at security incidents by attack type, time and impact, 2011 to 2013



Cloud security: inheritance



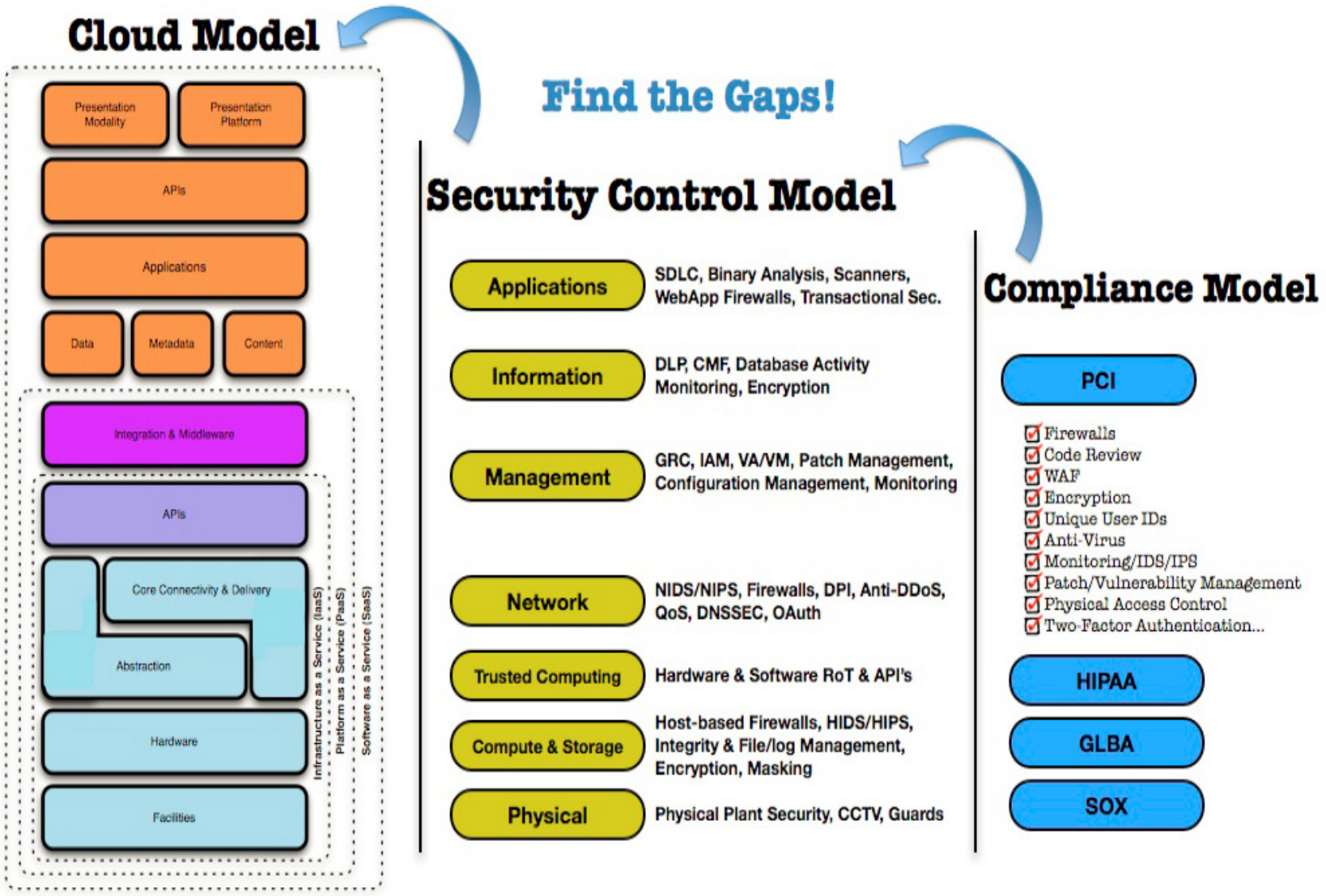


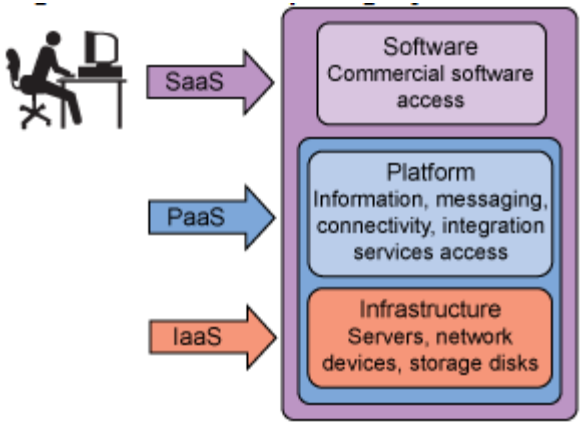
Figure 5—Mapping the Cloud Model to the Security Control & Compliance

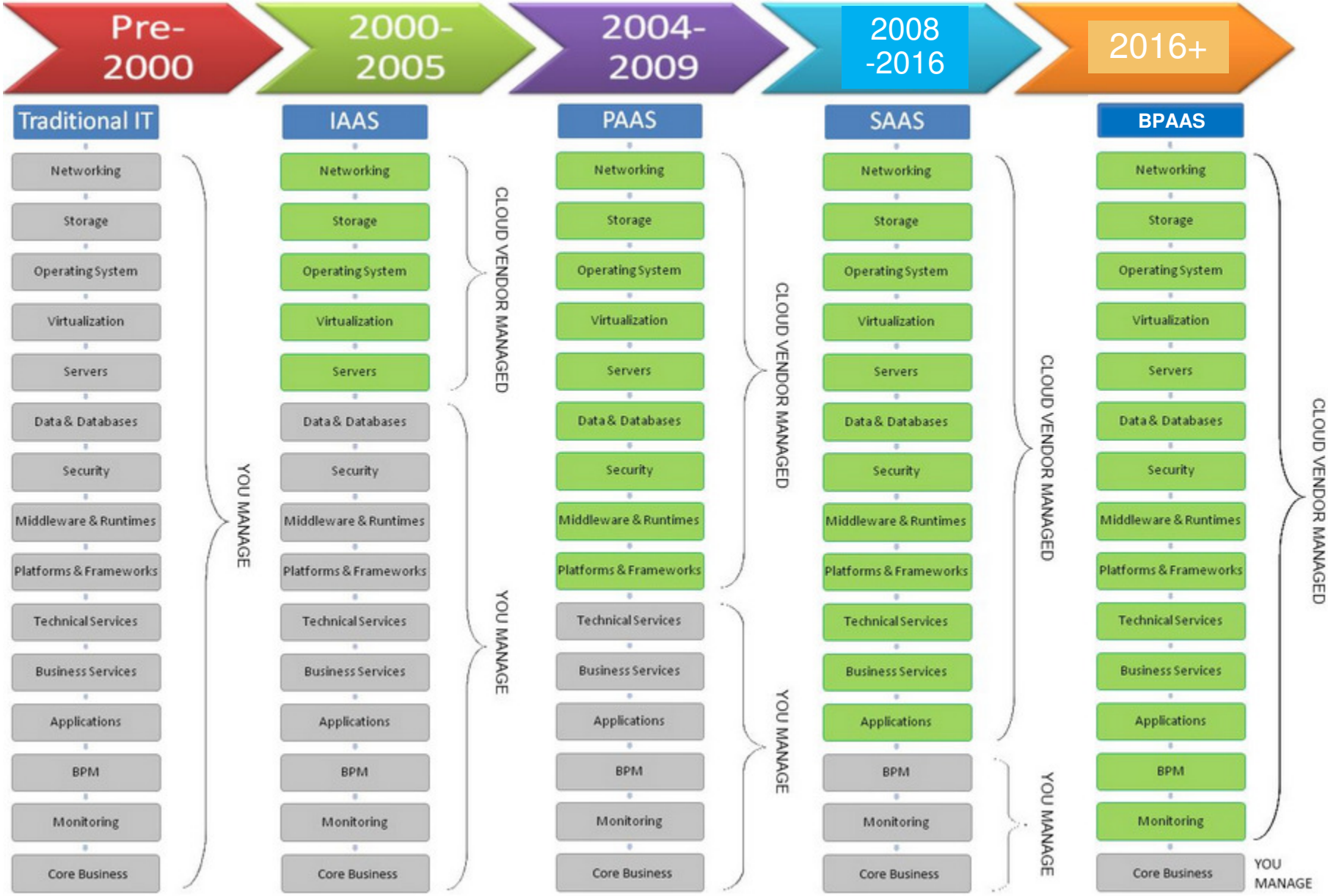
Security responsibility – differences for SaaS, PaaS, IaaS

• *Software as a Service (SaaS) model, most of the responsibility for security* management lies with the cloud provider. SaaS provides a number of ways to control access to the Web portal, such as the management of user identities, application level configuration, and the ability to restrict access to specific IP address ranges or geographies.

• *Platform as a Service allow clients to assume more responsibilities for* managing the configuration and security for the middleware, database software, and application runtime environments.

• *Infrastructure as a Service (IaaS) model transfers* even more control, and responsibility for security, from the cloud provider to the client. In this model, access is available to the operating system that supports virtual images, networking, and storage.




Pre-2000
2000-2005
2004-2009
2008-2016
2016+
Traditional IT
IAAS
PAAS
SAAS
BPAAS
Networking
Storage
Operating System
Virtualization
Servers
Data & Databases
Security
Middleware & Runtimes
Platforms & Frameworks
Technical Services
Business Services
Applications
BPM
Monitoring
Core Business
YOU MANAGE
CLOUD VENDOR MANAGED

Security responsibility – differences between private and public cloud

Area	Public	Private owned
Data ownership	Physically cloud provider (legally you)	You have full control / ownership
Security standards	You get what you are being offered	Customization is possible – responsibility on security lies with you
Security exposure	Can be higher than in private cloud (in case private provider would not have knowledge or finances) but is more exposed to attacks	Can be higher than in public cloud but requires expertise to establish all security aspects (with particular knowledge)
Governance	Lies with provider	Lies with provider
Design flexibility	Minimum flexibility	Do whatever you want

Table 1—Cloud Computing Deployment Models

	Infrastructure Managed By[1]	Infrastructure Owned By[2]	Infrastructure Located[3]	Accessible and Consumed By[4]
Public	Third Party Provider	Third Party Provider	Off-Premise	Untrusted
Private/ Community	Or Organization / Third Party Provider	Organization / Third Party Provider	On-Premise / Off-Premise	Trusted
Hybrid	Both Organization & Third Party Provider	Both Organization & Third Party Provider	Both On-Premise & Off-Premise	Trusted & Untrusted

[1] *Management includes: governance, operations, security, compliance, etc…*
[2] *Infrastructure implies physical infrastructure such as facilities, compute, network & storage equipment*
[3] *Infrastructure Location is both physical and relative to an Organization's management umbrella and speaks to ownership versus control*
[4] *Trusted consumers of service are those who are considered part of an organization's legal/contractual/ policy umbrella including employees, contractors, & business partners. Untrusted consumers are those that may be authorized to consume some/all services but are not logical extensions of the organization.*

Cloud security – general areas of concern

1. Governance and Enterprise Risk Management
2. Legal Issues: Contracts and Electronic Discovery
3. Compliance and Audit
4. Information Management and Data Security
5. Portability and Interoperability
6. Traditional Security, Business Continuity and Disaster Recovery

Security Guidance for Critical Areas of Focus in Cloud - https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/csaguide.v3.0.pdf

Cloud security – general areas of concern

7. Data Center Operations
8. Incident Response, Notification and Remediation
9. Application Security
10. Encryption and Key Management
11. Identity and Access Management
12. Virtualization
13. Security as a Service

Security Guidance for Critical Areas of Focus in Cloud - https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/csaguide.v3.0.pdf

Key security dangers to cloud security

- Virtualization and multitenancy
- Nonstandard and vulnerable APIs
- Internal security breaches
- Data corruption or loss
- User account and service hijacking

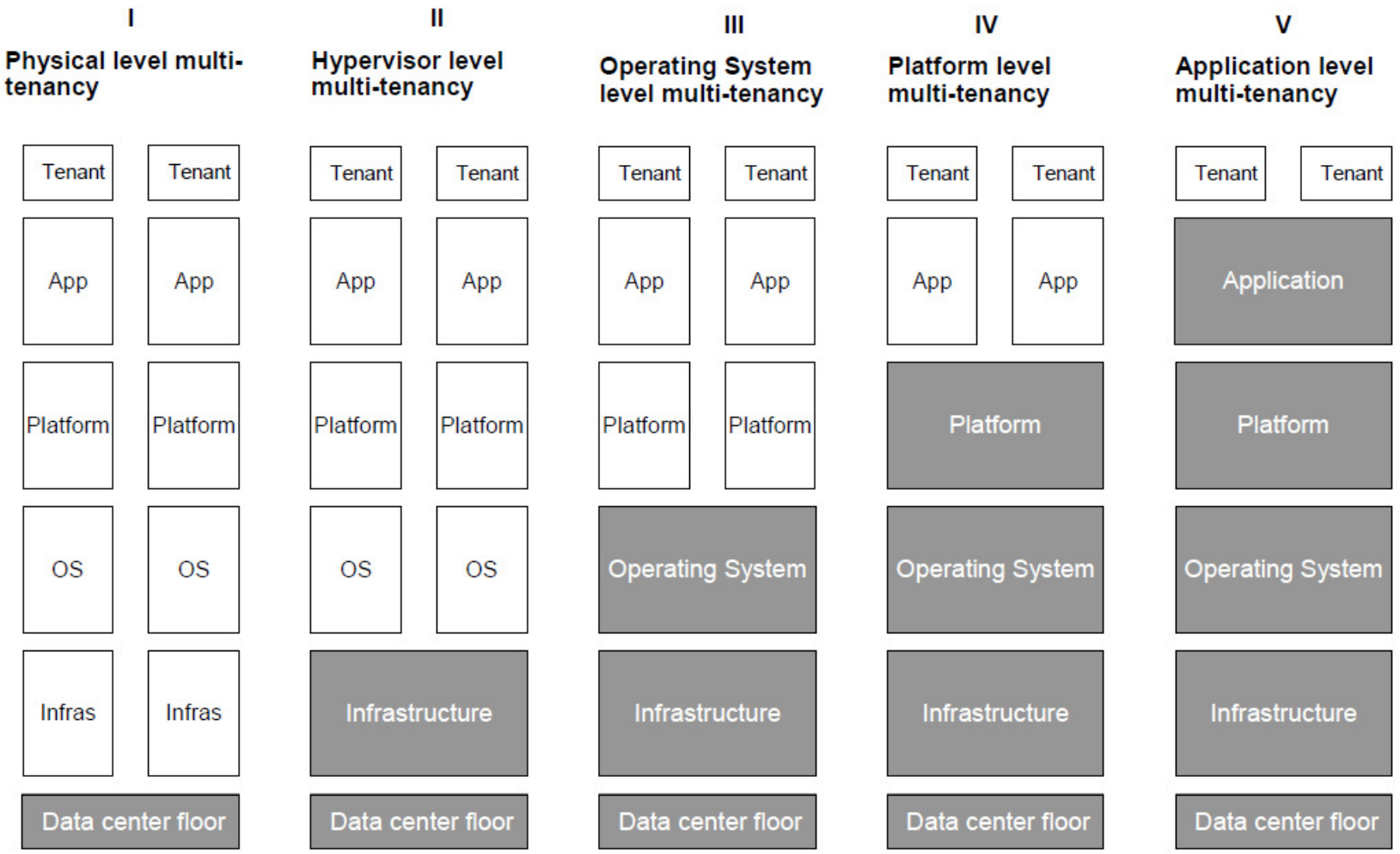
Listed challenges are typically addressed via series of tools and practices – e.g.

- Host-based intrusion protection systems (HIPS)
- Network-based intrusion protection systems (NIPS)
- Security best practices

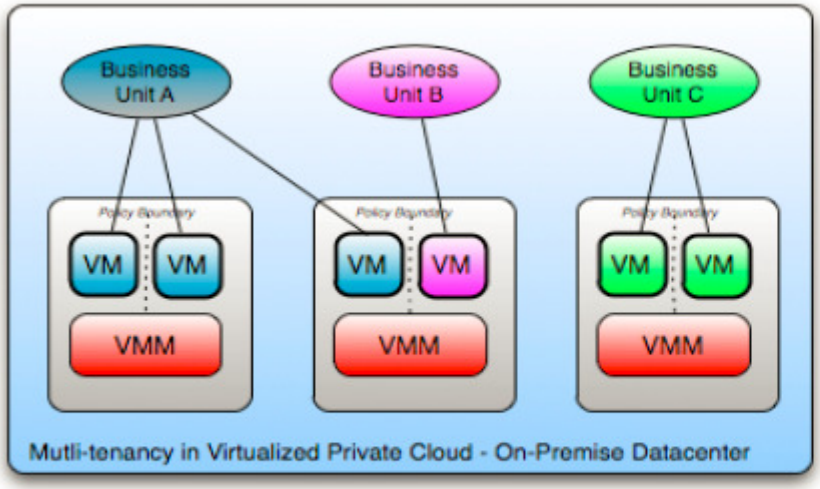
Key security dangers to cloud security

- **Virtualization and multitenancy**
  - Limited isolation in place – hypervisor extend security risk and expose operational system. Attacker can expose not only hypervisor but can get access into data and internal application.
  - As mitigation - security (operation system or application) best practices are recommended – e.g. patch management, Authentication, authorization, auditing

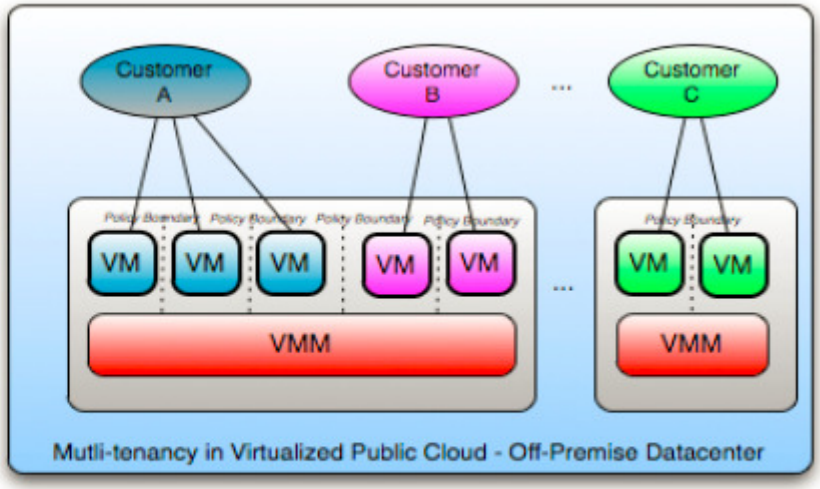
Multi-tenancy



Multi-tenancy



Private Cloud of Company XYZ with 3 business units, each with different security, SLA, governance and chargeback policies on shared infrastructure

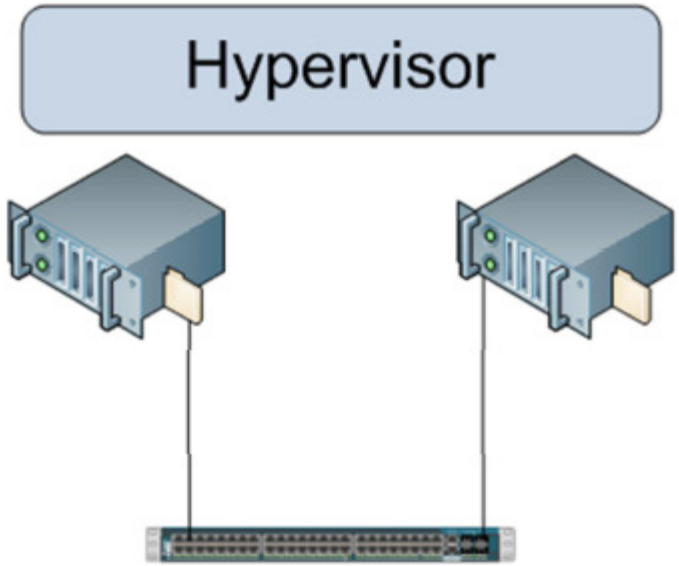


Public Cloud Provider with 3 business customers, each with different security, SLA, governance and billing policies on shared infrastructure

Security Guidance for Critical Areas of Focus in Cloud - https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/csaguide.v3.0.pdf

Example – security concern

The lack of an Air Gap



Key security dangers to cloud security

- **Nonstandard and vulnerable APIs**
  - Cloud API are not standardize yet – weak interface (API) can expose system into intruders
  - As mitigation - security (API) best practices are recommended – e.g. Authentication, authorization, auditing + review cloud provider's security model used for API (e.g. API trusted chain)

Key security dangers to cloud security

- **Internal security breaches**
  - In IT area – over 70% of security breaches is caused by internal factors / employees
  - To reduce risk consider following
    a) Transparency in information and internal management practices
    b) Understand the human resources requirements
    c) Have a clear level of escalation and notification of a breach

Key security dangers to cloud security

- **Data corruption or loss – 1/2**
  - Data corruption or loss is amplified since the cloud provider is the source for a companies data, not the company itself
  - As mitigation steps you might consider
    a) Implement application systems security best practices, such as authentication, authorization, and auditing
    b) Implement strong encryption, SSL, digital signatures and certificate practices
    c) Ensure that strong disaster recovery processes exist and are tested on a periodic basis
    d) Require that the persistent medium used to store your data is erased prior to releasing it back into the pool

Key security dangers to cloud security

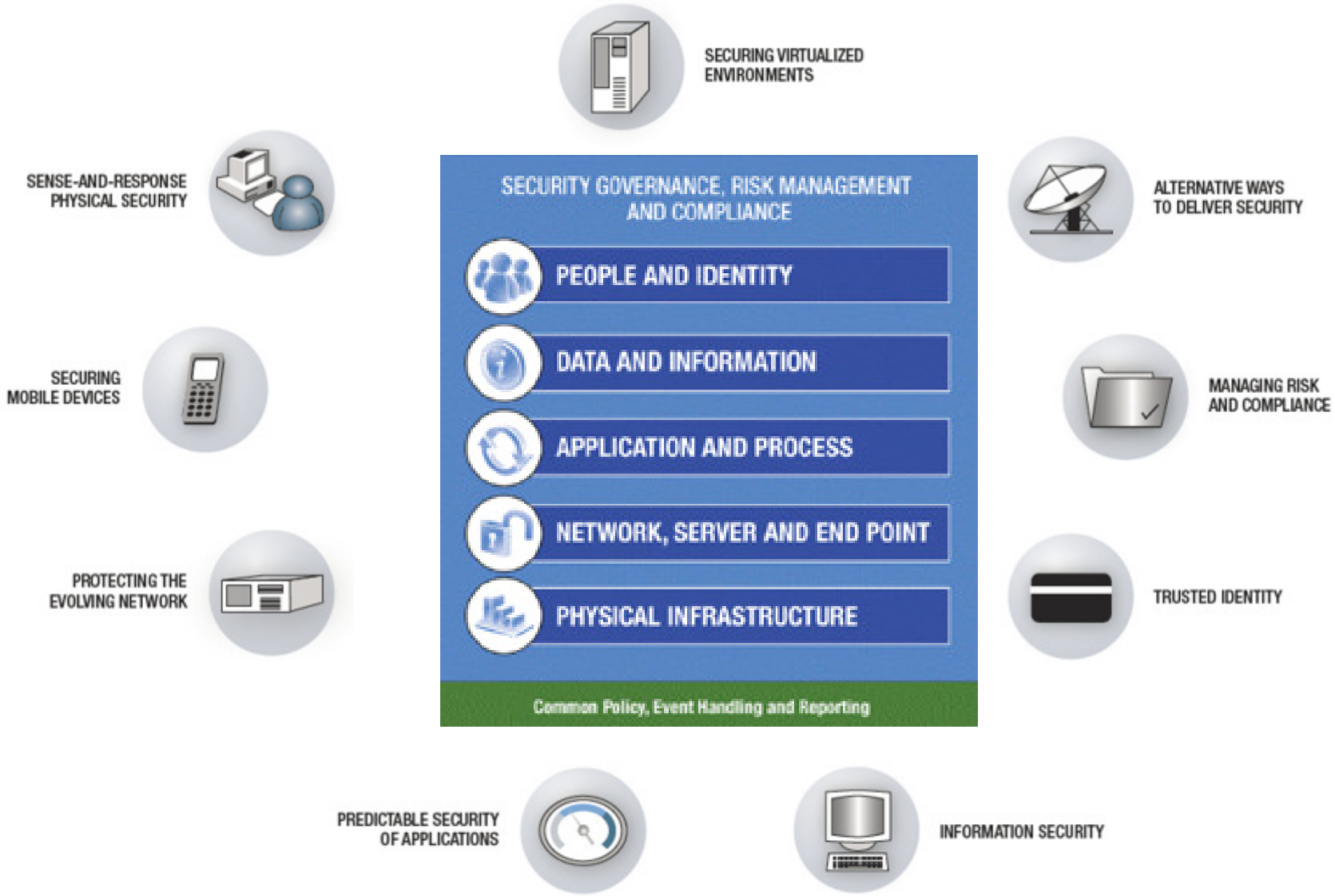
- **Data corruption or loss – 2/2**
  - **Multi-tenancy challenge**
    - implies use of same resources or application by multiple consumers that may belong to same organization or different organization.
    - The impact of multi-tenancy is visibility of residual data or trace of operations by other user or tenant.
    - implies a need for policy-driven enforcement, segmentation, isolation, governance, service levels, and chargeback/billing models for different consumer constituencies
    - offers benefits of scaling but could present security risk

Security Guidance for Critical Areas of Focus in Cloud - https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/csaguide.v3.0.pdf

Key security dangers to cloud security

- **User account and service hijacking**
  - User account and service hijacking occurs when a attacker obtains your cloud services information and uses it to take over your cloud access
  - If attackers gain access to a cloud user's credentials, they can eavesdrop on activities and transactions, manipulate or steal data, return falsified data, and redirect clients to illegitimate sites
  - To mitigate this risk following approaches are recommended
    a) Implement security best practices, including human processes, such as strong passwords, two-factor authentication, and prohibiting the sharing of users' credentials
    b) Implement application systems security best practices, such as AAA (authentication, authorization, and auditing)
    c) Implement strong encryption, SSL, digital signatures, and certificate practices
    d) Ensure that auditing and logging is being used to monitor activities

Security Framework should cover at least following



Security and control frameworks

COBIT

Control Objectives for Information and related Technology1 (CobiT), the International Organization for Standardization 27002:20052 (ISO/IEC 27002:2005), and the Information Technology Infrastructure Library3 (ITIL) have emerged worldwide as the most respected frameworks for IT governance and compliance.

Cobit - is a set of best practices (framework) for IT management created by the Information Systems, Audit and Control Association (ISACA) and the IT Governance Institute (ITGI) in 1996. It is an internationally accepted framework for IT governance and control.

ISO 27002

The ISO 27002 standard provides guidance for the implementation of an Information Security Management System. It is exhaustive. Therefore, every organization that relies on this preferred practice should select the controls that are applicable for their information system or environment.

A step-by-step manner of approaching ISO/IEC 27002:2005 is best. The best starting point is usually an assessment of the current position or situation, followed by an identification of the changes needed for ISO/IEC 27002:2005 compliance. From here, planning and implementing must be rigidly undertaken

ISO 27017

"P*rovide guidance on the information security elements of cloud computing, recommending and assisting with the implementation of cloud-specific information security controls supplementing the guidance in ISO/IEC 27002 and indeed other ISO27k standards including ISO/IEC 27018 on the privacy aspects of cloud computing, ISO/IEC 27031 on business continuity, and ISO/IEC 27036-4 on relationship management, as well as all the other ISO27k standards*" (source: http://www.iso27001security.com/html/27017.html)

ISO 27017

New Controls specific for cloud

- Shared roles and responsibilities within a cloud computing environment
- Removal of cloud service customer assets
- Segregation in virtual computing environments
- Virtual machine hardening
- Administrator's operational security
- Monitoring of cloud services
- Alignment of security management for virtual and physical networks

Source : http://advisera.com/27001academy/blog/2015/11/30/iso-27001-vs-iso-27017-information-security-controls-for-cloud-services/

Cloud Control Matrix

Microsoft Excel
Worksheet

Cloud Security alliance - https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/

"The cloud is an opportunity to rethink security."

–Raj Nagaratnam

Cloud Security

Cloud Security implementation

Implementation of security

The following security measures represent general best practice implementations for cloud security. At the same time, they are not intended to be interpreted as a guarantee of success.

1. Implement and maintain a security program.
2. Build and maintain a secure cloud infrastructure.
3. Ensure confidential data protection.
4. Implement strong access and identity management.
5. Establish application and environment provisioning.
6. Implement a governance and audit management program.
7. Implement a vulnerability and intrusion management program.
8. Maintain environment testing and validation.

Cloud Security Summary

Security domains	Today	Security gaps	Tomorrow: Security intelligence	
People	Manage identities per application		Employ role-based dashboard and privileged user management	Apply advanced correlation and deep analytics
Data	Deploy access control and encryption		Monitor usage and control leakage	
Applications	Scan for vulnerabilities		Build securely from day one	
Infrastructure	Block unwanted network access and viruses		Execute real-time advanced threat detection and forensics	

Reactive → ***Proactive***

Source: IBM analysis.

Figure 3: A balanced approach is needed to manage physical, technological and human assets.

Security intelligence	People	Data	Applications	Infrastructure
Optimized	• Governance, risk and compliance • Advanced correlation and deep analytics			
	• Role-based analytics • Privileged user controls	• Data flow analytics • Data governance	• Secure application development • Fraud detection	• Advanced network monitoring/forensics • Secure systems
Proficient	• Identity management • Strong authentication	• Activity monitoring • Data loss prevention	• Application firewall • Source code scanning	• Asset management • Endpoint/network security management
Basic	• Passwords and user IDs	• Encryption • Access control	• Vulnerability scanning	• Perimeter security • Anti-virus

Source: IBM analysis.

Figure 6: Using analytics to proactively highlight risks and identify, monitor and address threats.

Cloud – data privacy, law

"*If you look at the legislation landscape of Financial Services sector in North America, it is full of very specific requirements about how and where certain records and information must be retained. Unfortunately, there is no single set of rules to follow.*"

Australia

- Anti–Money Laundering and Counter-Terrorism Financing Act 2006
- Australian Prudential Regulation Authority Act 1998
- Corporate Law Economic Reform
- Program (CLERP 9)/ Corporations Act
- Part VA of the Trade Practices Act 1974 (CTH)
- Privacy Amendment (Enhancing Privacy Protection) Act 2012

United Kingdom

- Financial Services Authority (FSA): Companies Act and Tax Legislation
- eDisclosure (U.K. eDiscovery), Legal Records, and BSI PD 008
- Electronic Communications Act 2000

Germany

- Telecommunications Data Retention Law
- Tax Mandates § 62(2) Implementing Regulation of the Turnover Tax Law (UstDV)

France

- Financial Security Law of France (LSF or Loi de Sécurité Financière).
- Freedom of Information Act (Loi n° 78-753)
- Délibération n° 2009-474
- Ordinance 2004-178 (National Patrimony)

Source: https://www-304.ibm.com/connections/blogs/bcde08b8-816c-42a8-aa37-5f1ce02470a9/entry/legal_regulations_and_compliance_on_records_management?lang=cs

Cloud – data privacy, law

There are existing security challenges, experienced in other computing environments, and there are new elements which are necessary to consider.

The challenges include:

- Governance
- Data
- Architecture
- Application
- Assurance

Security is often related to compliance & local laws or regulations – **typical questions are below.**

1. Jurisdiction and regulatory requirements (could data be hosted in private / public / hybrid cloud?)

2. Complying with Export/Import controls (is data center located in approved country?)

3. Compliance of the infrastructure (is cloud provider uses standards to adhere GREEN compliance posture?)

4. Audit and reporting

5. Data location and segregation

6. Data footprints

Cloud – data privacy, law, policy

"**SafeHarbor** is the name of a **policy agreement** established between the United States Department of Commerce and the European Union (E.U.) in November 2000 to regulate the way that U.S. companies export and handle the personal data (such as names and addresses) of European citizens.

The agreement is a policy compromise set up in response to a European directive that differed from traditional business procedures for U.S. companies dealing with the E.U"

Adobe Acrobat Document

Source: http://trade.gov/media/publications/pdf/safeharbor-selfcert2009.pdf

Cloud – Safe Harbor principles

How does an organization join?

The decision by U.S. organizations to enter the U.S.-EU Safe Harbor program is entirely voluntary. Organizations that decide to participate in the U.S.-EU Safe Harbor program must comply with the U.S.-EU Safe Harbor Framework and publicly declare that they do so

What do the Safe Harbor principles require?

1. Notice
2. Choice
3. Onward Transfer (Transfers to Third Parties)
4. Access
5. Security
6. Data integrity
7. Enforcement

Source: http://trade.gov/media/publications/pdf/safeharbor-selfcert2009.pdf

Cloud – Safe Harbor future

Safe Harbour is being replaced by **“Privacy Shield**” agreement that should address certain legal issues (from EU perspective) (July 2016)

It’s expected that even this agreement may not be final and European Court of justice may / likely will terminate its validity once real law case is presented to this institution.

ISO/IEC 27018:2014 – privacy standard

- **establishes** commonly accepted control objectives, **controls and guidelines for implementing measures to protect Personally Identifiable Information** (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.

- **specifies guidelines** based on ISO/IEC 27002, taking into consideration the regulatory requirements **for the protection of PII which might be applicable within the context of the information security risk environment(s) of a provider of public cloud services.**

- **is applicable to all types and sizes of organizations**, including public and private companies, government entities, and not-for-profit organizations, which provide information processing services as PII processors via cloud computing under contract to other organizations.

Source: ISO

ISO/IEC 27018:2014 – privacy standard

Examples of additional controls and policies

- Rights of the customer to access and delete the data
- Not using the data for marketing and advertising
- Notification to the customer in case of a request for data disclosure
- Procedure for data restoration
- Encrypting data that is transmitted over public networks
- Specifying the minimum security controls in contracts with customers and subcontractors
- Ensuring the data reaches the destination
- Notification to the customer in case of a data breach

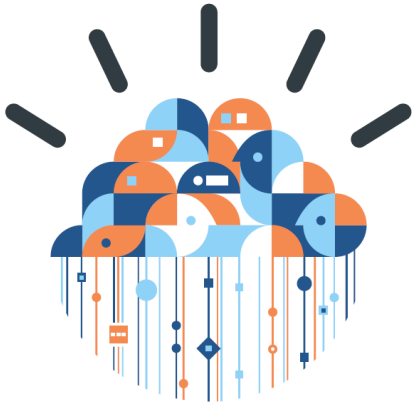
Source: www.adviser.com

Information security and privacy standard examples

Financial	Government	Healthcare	Media and Entertainment	Cross industry
Payment Card Industry Data Security Standard (PCI DSS)	Advertising Standards Authority (ASA)	Health Insurance Portability and Accountability Act (HIPAA)	Personal Information Protection and Electronics Document Act (PIPEDA)	Control Objectives for Information and Related Technologies (COBIT)
Gramm - Leach - Bliley Act (GLBA)	The Department of Defense Architecture Framework (DoDAF)	HITRUST Common Security Framework (CSF)		International Organization for Standardization (ISO 27002:20XX)
Federal Information Processing Standard (FIPS)	National Institute of Standards and Technology standards (NIST)			Information Technology Infrastructure Library (ITIL)
Bank for International Settlements (Basel III)	Family Educational Rights and Privacy Act (FERPA)			Open Group Architecture Framework (TOGAF)
Sarbanes - Oxley Act (SOX)				IBM Unified Method Framework (UMF)
Financial Sector Implementation Assistance (FISAP)				Open Enterprise Security Architecture (O-ESA)
European Union Data Protection Directive (EUDPD)				Sherwood Applied Business Security Architecture Framework (SABSA)
				Trusted Cloud Initiative Reference Architecture (TCI)

"The cloud is an opportunity to rethink security."

–Raj Nagaratnam



Cloud Security

Security examples & concerns that might affect cloud adoption

Example – security concern

"***Microsoft's U.K. head admitted in June 2011 that no cloud data is safe from the Patriot Act, and the company can be forced to hand EU-stored data over to U.S. authorities.***"

"While it has been suspected for some time, this is the first time Microsoft, or any other company, has given this answer.

Any data which is housed, stored or processed by a company, which is a U.S. based company or is wholly owned by a U.S. parent company, is vulnerable to interception and inspection by U.S. authorities." source: ZDLINK

Response from European parliament

"*The European Commission should quickly make it clear that European businesses and citizens are under European privacy laws.* ***European citizens and businesses need to be confident that EU institutions enforce their own laws.***

Keen to stress that though EU subsidiaries of U.S. parent companies are breaking European law by handing over data back to the United States under a Patriot Act request, that while these subsidiaries are operating within Europe, ***EU law must take precedent****.*

"The European Commission should urgently contact the U.S. government and make clear that we do not accept." source: ZDLINK

Example – security concern & quiz

”*Safe Harbour is a agreement set up 16 years ago to create a way for US businesses to transfer EU citizens’ personal data to the US even though American data protection laws are not up to the European standard. Following the revelations by Edward Snowden that US businesses were being compelled to hand over personal data under the Prism programme, Austrian law student Schrems complained to the Irish data protection commissioner - Facebook’s EU operations are head-quartered in Ireland – that his privacy rights were being violated.*

The Irish data protection authority (DPA) refused to act on the grounds that the social network is signed up to Safe Harbour/Harbor - a voluntary scheme whereby companies promise to protect EU personal data.

Undeterred, Schrems took his case to the Irish High Court which referred it to the European Court of Justice (ECJ).

*the ECJ says that national DPAs cannot use Safe Harbour as a reason for not investigating suspected mishandling of data The challenge of the matter is that although companies may respect the Safe Harbour guidelines, “**United States public authorities are not themselves subject to it***
The register.cu.uk

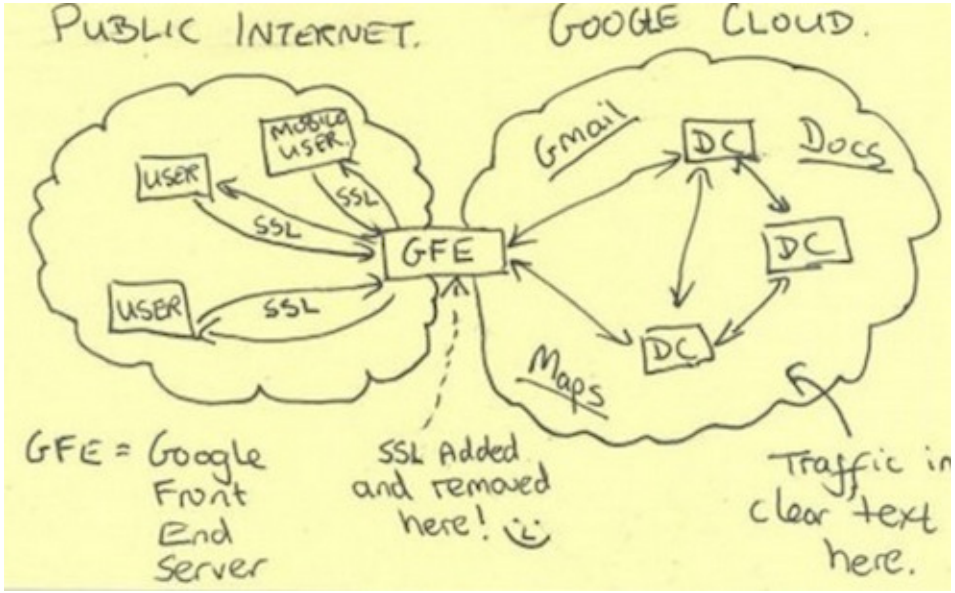
Quiz: How facebook could respond for a ban on data transfer?
a. No need to worry as Facebook is US company and they don’t need to follow EU rules / law
b. Move data to EU
c. Have all EU data encrypted (on side of US servers)
d. Stop providing a service for users from EU

Example – security assurance (encryption)

"*Microsoft is looking to follow its global cloud partners, Google and Yahoo, in encrypting the traffic flowing between its worldwide datacenter locations, fearing the U.S. government's ability to tap into customer data."* source: ZDLINK

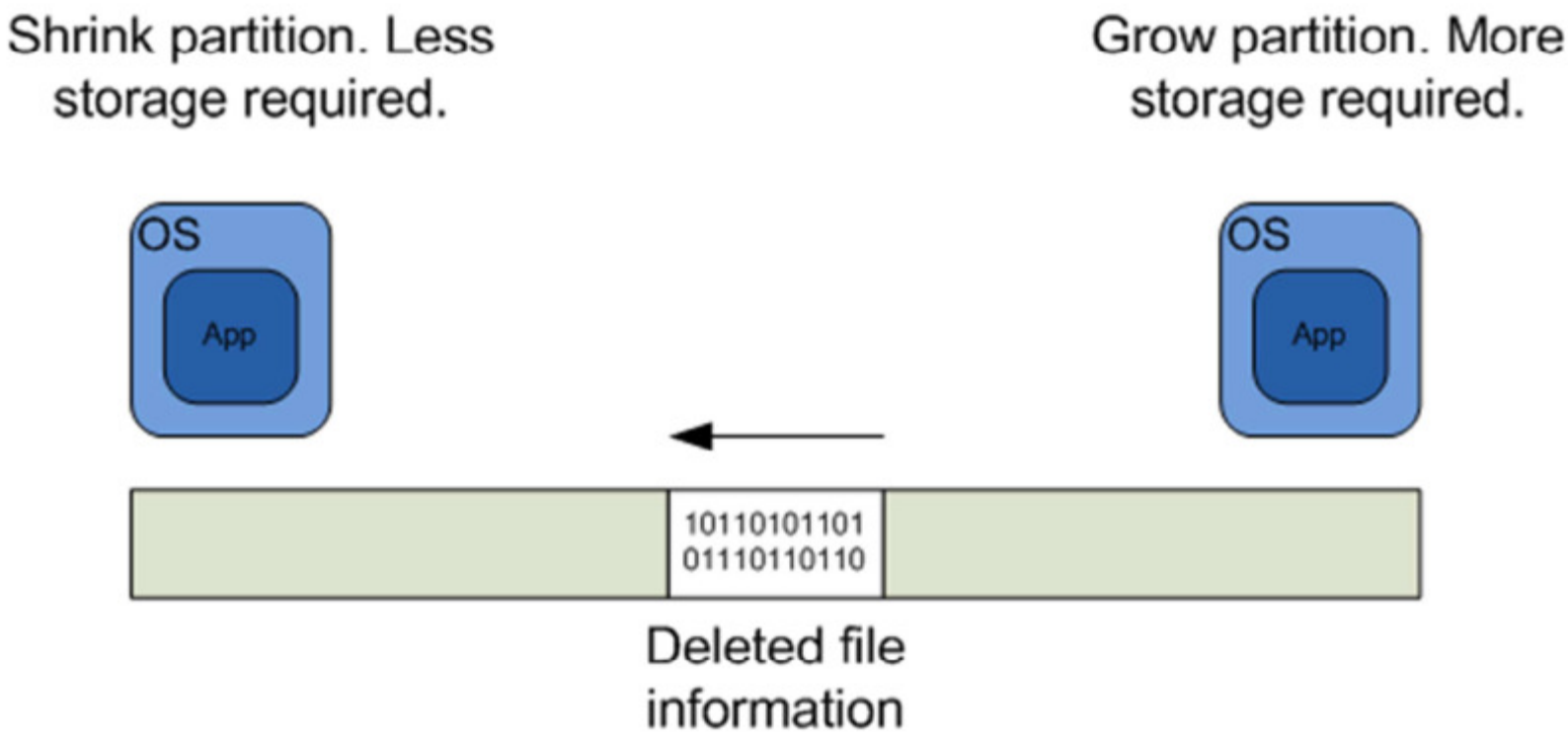
"*Though Google and other companies spend vast amounts on leasing fiber optic cables from companies in order to keep their data off the "public" Internet, the NSA and GCHQ still reportedly tap these cables at major Internet hubs around the world, including in the U.K.*"

"*Unless Microsoft takes immediate action to rectify this situation,* ***any business or individual using their services to store or transmit sensitive data will have been fundamentally let down by a brand that suggested it was worthy of trust***."



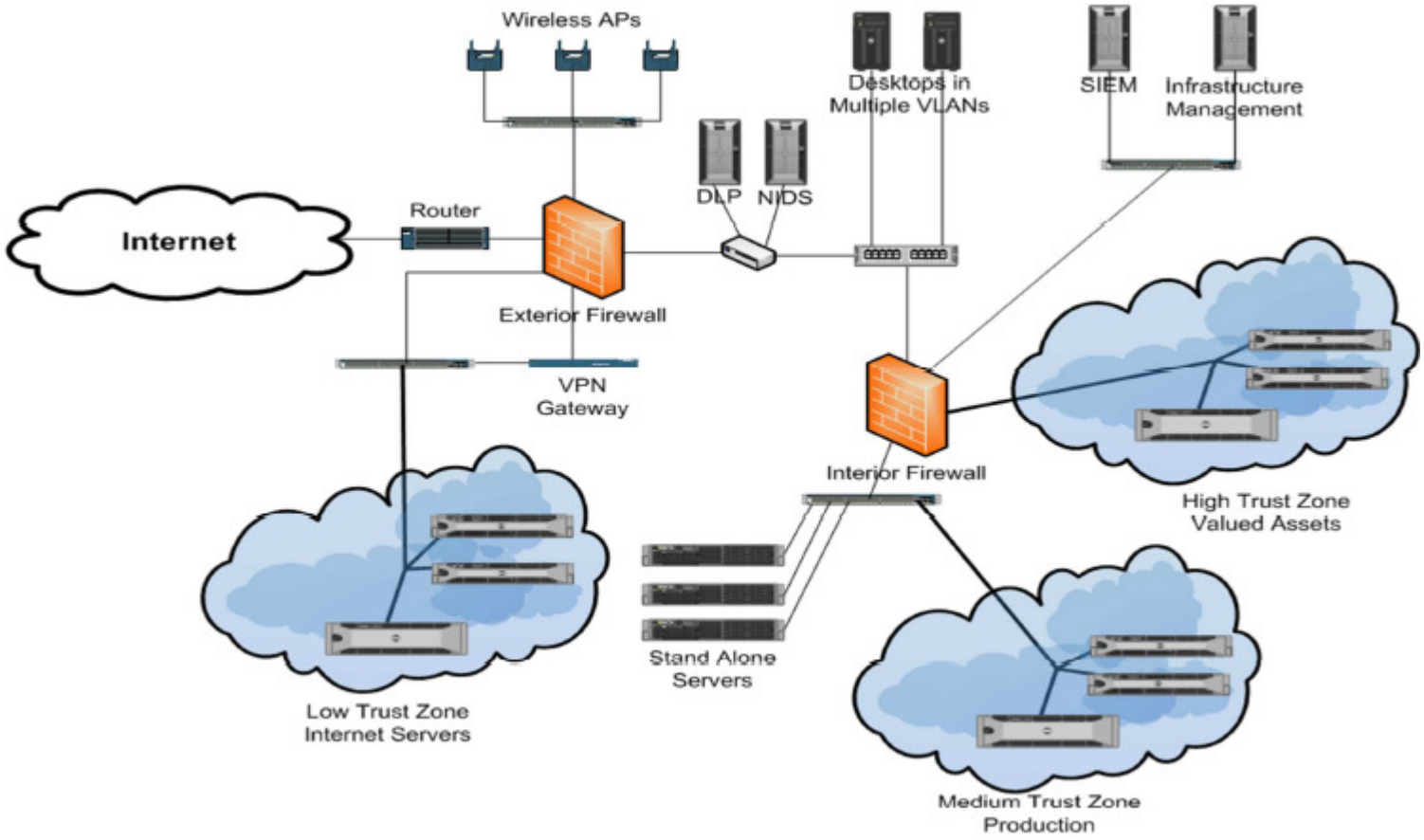
Example – security concern

Potential data misplacement



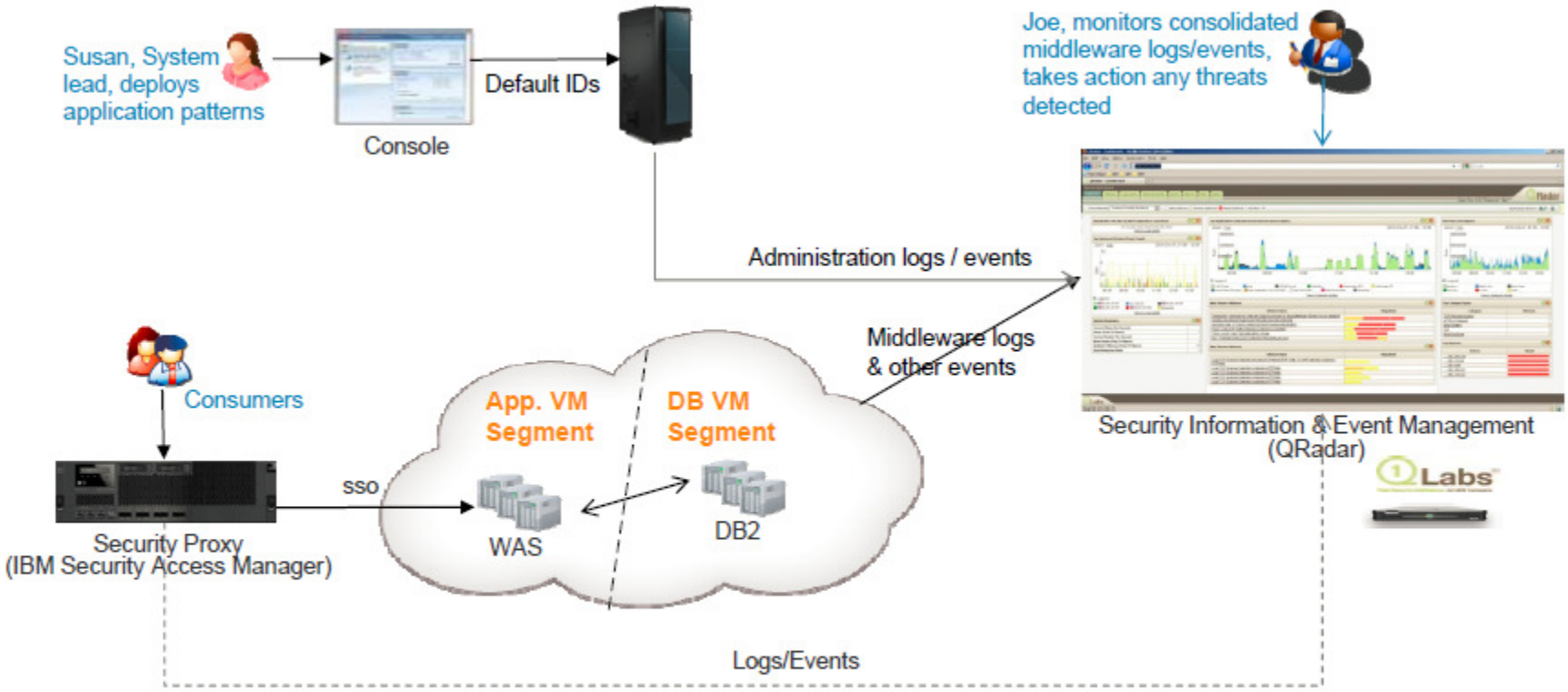
Example – security concern

Layers with virtualization



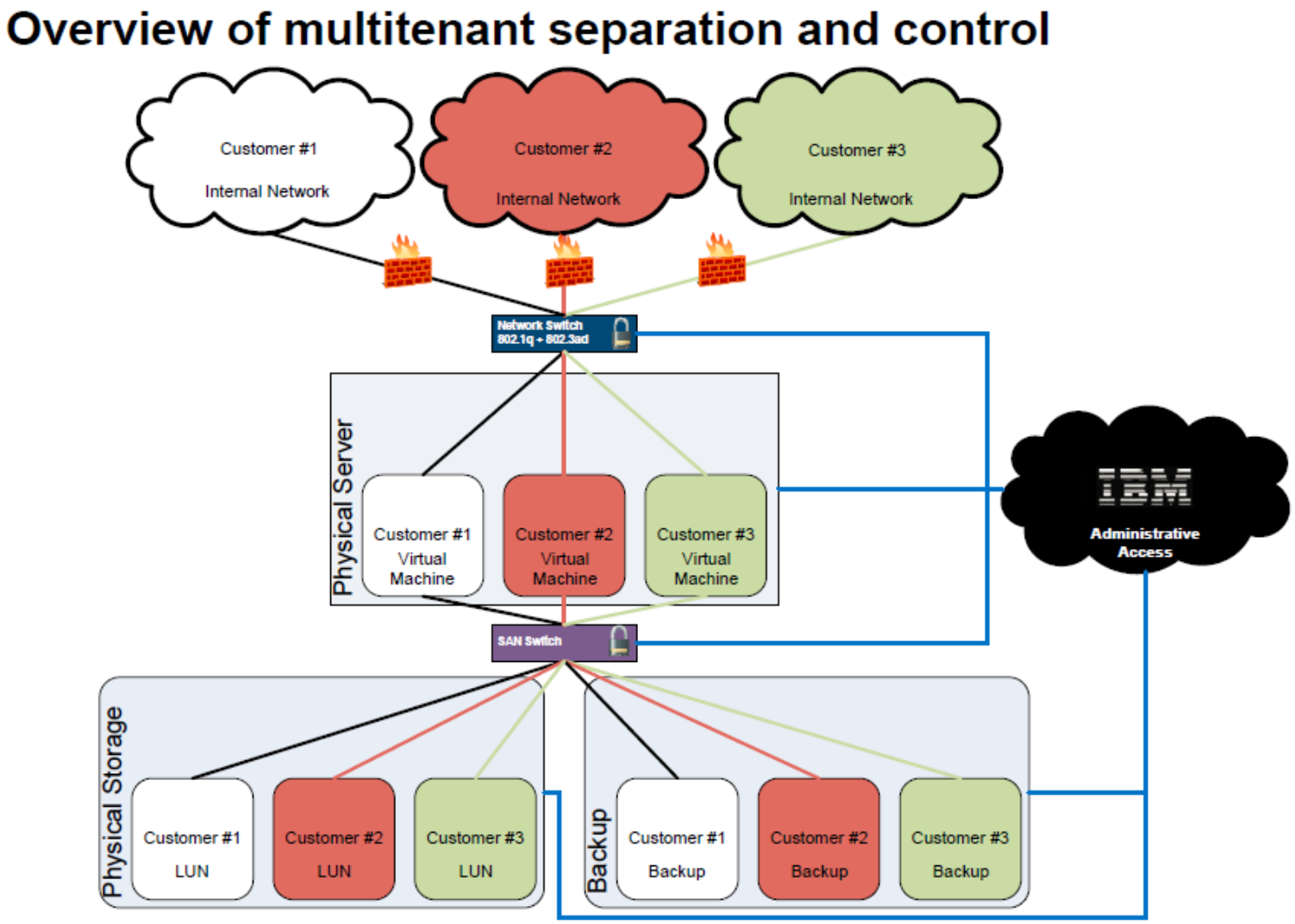
Example – internal security assurance (logging)

Scenario: Threat Detection in Virtual Application & System



- Centralized security log management and correlation
- Detect external threats e.g. SQL Injection, Brute force attacks, Login attempts, etc.
- Detect internal threats

Example – security assurance (CMS)



Quiz – question 1

Quiz: Which of following standards is related to security
a. ISO 27002
b. Multi tenancy
c. ISO 27017
d. Open Stack
e. ISO 9001

Quiz – question 2

Do proper match between proactive and reactive security approaches	
a. Scan for vulnerability	1. Execute real time advanced threat detection and forensics
b. Manage identities per applications	2. Build security from day one
c. Deploy access control and encryption	3. Employ role-based dashboard and privileged user management
d. Block unwanted network access and viruses	4. Monitor usage and control leakage

Quiz – question 3

Quiz: Which of following is not threat to cloud environment
a. Data breach
b. Multi tenancy
c. Account hijacking
d. Advanced persistent thread
e. Data loss
f. DoS attack
g. Cloud services abuse
h.. Vulnerable API
i. Implement an existing cryptographic algorithm on your own
j. Compromised credentials
k. Dictionary attack
l. Machine to machine attacks
m Password: asdfghasdfghasdfghasdfgh

Quiz – question 4

Quiz: What is minimum number of firewalls needed for virtual private cloud environment to provide at least basic security boundary?
a. 1
b. 2
c. 3
d. As many as needed – there does not have to be any
e. 0 as it is protected by antiviruses and IPS

Quiz – question 5

Quiz: What privacy standard cloud providers should adopt to address privacy regulations for their clients?
a. Safe harbor.
b. None as privacy standards is responsibility of clients.
c. Any privacy standard or agreement that may be required by clients in their country.
d. ISO27001
e. ISO27018

Additional Links and used materials

- Security for cloud computing
http://www.cloudstandardscustomercouncil.org/security-d.htm

- IBM Security Technology Outlook: An outlook on emerging security technology trends
ftp://public.dhe.ibm.com/software/tivoli/whitepapers/outlook_emerging_security_technology_trends.pdf

- Security Guidance - IBM Recommendations for the Implementation of Cloud Security
http://www.redbooks.ibm.com/redpapers/pdfs/redp4614.pdf

- Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security
http://www.redbooks.ibm.com/redpapers/pdfs/redp4528.pdf

- Using the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security
*www.redbooks.ibm.com/redbooks/pdfs/**sg248100**.pdf*

- Review and summary of cloud security scenarios - From "Cloud Computing Use Cases Whitepaper" Version 3.0 (cl-rev1security-pdf)
http://www.ibm.com/developerworks/cloud/library/cl-rev1security.html

- IBM Security Services - Security examples – scenarios and solutions (products) that might be used
http://public.dhe.ibm.com/common/ssi/ecm/en/sec03016gben/SEC03016GBEN.PDF

- Demystifying the cloud: The new economics of cloud computing
https://www-304.ibm.com/events/wwe/grp/grp004.nsf/vLookupPDFs/FINAL--Demystifying%20Cloud--Defining%20a%20Path%20Forward/$file/FINAL--Demystifying%20Cloud--Defining%20a%20Path%20Forward.pdf

- IBM Cloud Security
ftp://ftp.software.ibm.com/software/th/downloads/03_Virtualization_Cloud_Security_How_to_de-risk_Security_in_a_Cloud_Virtual_environment.pdf

- Cloud Security: Who do you trust?
http://www.ibm.com/ibm/files/I581626T50867W87/IBM_Cloud_Security_Who_do_you_trust_LR.pdf

-

Additional Links and used materials

- Cloud Security Alliance - generall
https://cloudsecurityalliance.org/
https://cloudsecurityalliance.org/education/white-papers-and-educational-material/white-papers/

- Security Considerations for Private vs. Public Clouds
https://downloads.cloudsecurityalliance.org/assets/research/collaborative/Security-Considerations-for-Private-vs-Public-Clouds.pdf

- Security Guidance for Critical Areas of Focus in Cloud Computing V3.0
http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

- Building multi-tenancy applications with IBM middleware
https://www6.software.ibm.com/developerworks/offers/techbriefings/cc4d-replays/session2_dcarew.pdf

BACKUP SLIDES

Security risks associated with cloud computing that must be adequately addressed

- Loss of governance.
- Responsibility ambiguity.
- Isolation failure.
- Vendor lock-in.
- Compliance and legal risks.
- Handling of security incidents.
- Management interface vulnerability.
- Data protection.
- Malicious behavior of insiders..
- Business failure of the provider.
- Service unavailability.
- Insecure or incomplete data deletion

Source and details description on http://www.cloudstandardscustomercouncil.org/security-d.htm

Security challenges and questions in nutshell

Governance
Achieving and maintaining governance and compliance in cloud environments brings new challenges to many organizations. (This paper should not be seen as legal advice or guidance specific to any one organization.)

Things you might need to consider include:

Jurisdiction and regulatory requirements
• Can data be accessed and stored at rest within regulatory constraints?
• Are development, test and operational clouds managing data within the required jurisdictions including backups?

Complying with Export/Import controls
•Applying encryption software to data in the cloud, are these controls permitted in a particular country/jurisdiction?
•Can you legally operate with the security mechanisms being applied?

Compliance of the infrastructure
•Are you buying into a cloud architecture/infrastructure/ service which is not compliant?

Audit and reporting
•Can you provide the required evidence and reports to show compliance to regulations such as PCI and SOX?
•Can you satisfy legal requirements for information when operating in the cloud?

Security challenges and questions in nutshell

Data
Cloud places data in new and different places, not just the user data but also the application (source) code. Who has access, and what is left behind when you scale down a service?

Other key issues include:

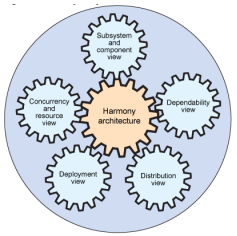
Data location and segregation
•Where does the data reside? How do you know?
•What happens when investigations require access to servers and possibly other people's data?

Data footprints
•How do you ensure that the data is where you need it when you need it, yet not left behind?
•How is it deleted?
•Can the application code be exposed in the cloud?

Backup and recovery
•How can you retrieve data when you need it?
•Can you ensure that the backup is maintained securely, in geographically separated locations?

Administration
•How can you control the increased access administrators have working in a virtualized model?
•Can privileged access be appropriately controlled in cloud environments?

Security challenges and questions in nutshell



Architecture
Standardized infrastructure and applications; increased commoditization leading to more opportunity to exploit a single vulnerability many times.

Looking at the underlying architecture and infrastructure, some of the considerations include:

Protection
•How do you protect against attack when you have a standard infrastructure and the same vulnerability exists in many places across that infrastructure?

Hypervisor vulnerabilities
•How can you protect the hypervisor (a key component for cloud infrastructures) which interacts and manages multiple environments in the cloud? The hypervisor being a potential target to gain access to more systems, and hosted images.

Multi-tenant environments
•How do you ensure that systems and applications are appropriately and sufficiently isolated and protecting against malicious server to server communication?

Security policies
•How do you ensure that security policies are accurately and fully implemented across the cloud architectures you are using and buying into?

Identity Management
•How do you control passwords and access tokens in the cloud?
•How do you federate identity in the cloud?
•How can you prevent userids / passwords being passed and exposed in the cloud unnecessarily, increasing risk?

Security challenges and questions in nutshell

Applications

There has been a significant increase in web application vulnerabilities, so much so that these vulnerabilities make up more than half of the disclosed vulnerabilities over the past 4 years.

Software Vulnerabilities

•How do you check and manage vulnerabilities in applications?

•How do you secure applications in the cloud that are increasing targets due to the large user population?

Patch management

•How do you secure applications where patches are not available?

•How do you ensure images are patched and up to date when deployed in the cloud?

Application devices

• How do you manage the new access devices using their own new application software?

• How do you ensure they are not introducing a new set of vulnerabilities and ways to exploit your data?

Security challenges and questions in nutshell

Assurance
Challenges exist for testing and assuring the infrastructure, especially when there is no easy way for data centre visits or penetration (pen) tests.

Operational oversight
•When logs no longer just cover your own environment do you need to retrieve and analyze audit logs from diverse systems potentially containing information with multiple customers?

Audit and assurance
•What level of assurance and how many providers will you need to deal with?
•Do you need to have an audit of every cloud service provider?

Investigating an incident
•How much experience does your provider have of audit and investigation in a shared environment?
•How much experience do they have of conducting investigations without impacting service or data confidentiality?

Experience of new cloud providers
•What will the security of data be if the cloud providers are no longer in business?
•Has business continuity been considered for this eventuality?