Security and regulatory requirements for public cloud offerings to support selected customer use cases

TROOPERS11, 30.03. - 31.03.2011, Heidelberg (Germany)

Mark Gall
Fraunhofer Institute for Secure Information Technology

Joachim Lüken
Nokia Siemens Networks GmbH & Co KG

Version: 6

About me

Secure Services & Quality Testings – SST

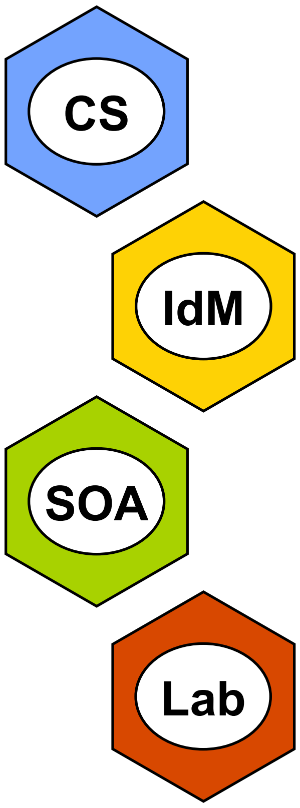
Mark Gall

Research Fellow

Phone: +49-(0)89 322 9986 -124
Fax: +49-(0)89 322 9986 -299

eMail: mark.gall@sit.fraunhofer.de
Web: http://www.sit.fraunhofer.de

About Fraunhofer SIT
Secure Services and Quality Testings



Cloud Security

Security Implications in Cloud Computing Ecosystems – Risk Analyses and Technology Studies

Identity Management

Development of Security Concepts in Identity Ecosystems

SOA Security

Research and development of service oriented achitectures for the Internet of People, Things and Services

Testlab

Installation & Evaluation of Open Source Solutions for Cloud Computing, Identity Management and Service Architectures

About me

Nokia Siemens Networks GmbH & Co. KG
81541 München
St. Martinstr. 76
Germany

Joachim Lüken
CEF CTO R SWS ST
Security Solutions for Applications, (IPTV, VoIP)

Phone: + 49 89 5159-29107
Mobile: + 49 170 1868472
E-Mail: joachim.lueken@nsn.com

Background

EWSD -> ATM -> VoIP -> IPTV -> SEC
PSTN and VoIP Standardisation (ETSI, ITU-T)
IPTV Standardisation (DVB, BBF)

About Nokia Siemens Networks Global company with a rich heritage

- Joint Venture of Nokia and Siemens
- Started operations on April 1, 2007
- €12.7 bn net sales in 2010
- 120+ years of telecom experience
- 65,000+ employees
- 45,000 service employees
- 75 of top 100 operators worldwide
- 150 countries
- 2.8 billion connections served

Agenda

1. Cloud Computing Introduction

2. Security Issues

3. Regulation and National Initiatives

4. Use Cases

5. References

Agenda

1. Cloud Computing Introduction

2. Security Issues

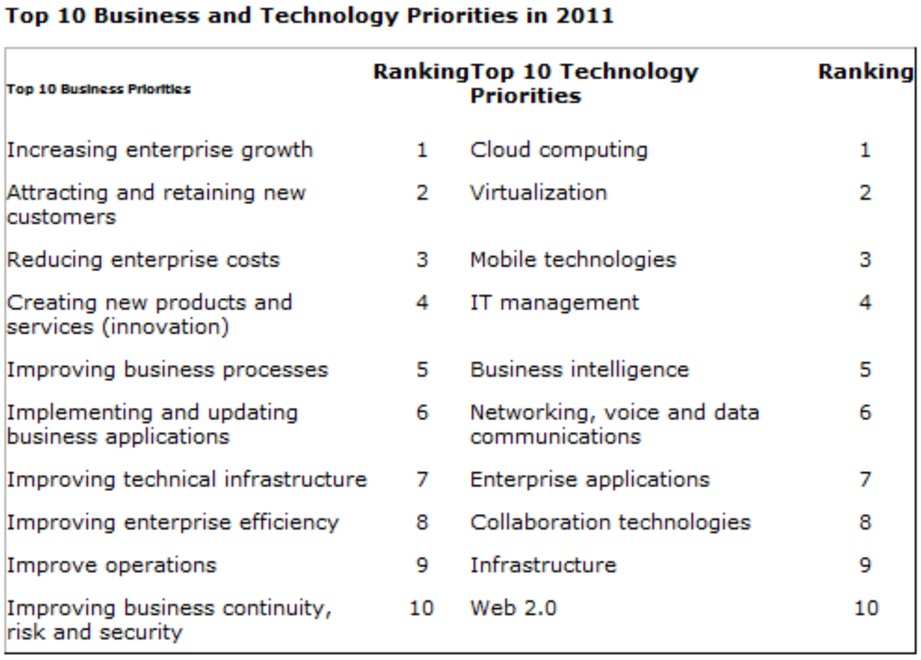
3. Regulation and National Initiatives

4. Use Cases

5. References

Cloud Computing Top Priorities for CIOs Gartner EXP CIO Survey from January 2011

- Gartner Executive Programs (EXP) conducted a worldwide CIO survey from September to December 2010 amongst more than 2,000 CIOs across 50 countries and 38 industries.
- Although IT budgets projections will remain flat, almost half of all CIOs expect to operate their applications and infrastructures via cloud technologies within the next five years.



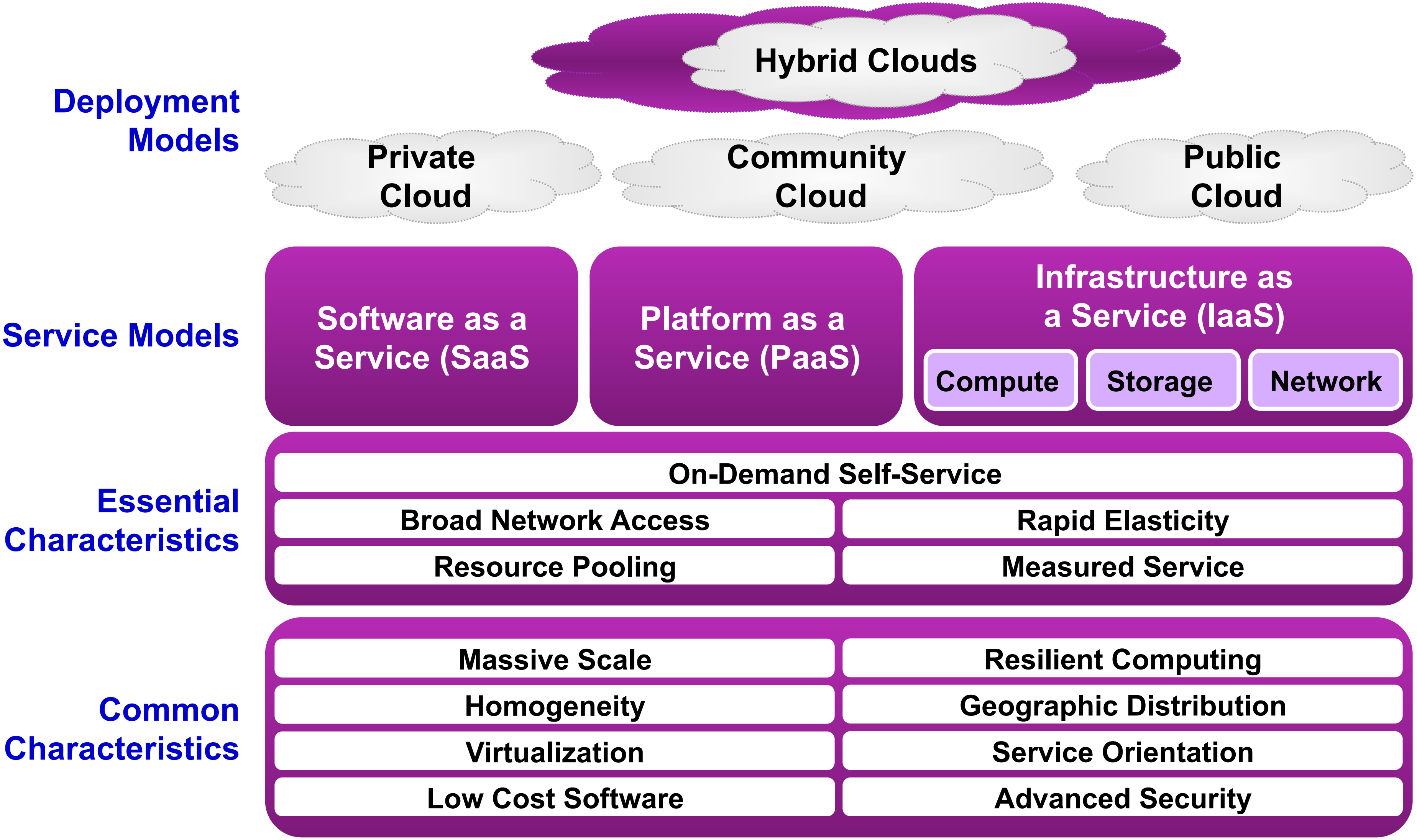
Top 10 Business and Technology Priorities in 2011

Top 10 Business Priorities	Ranking	Top 10 Technology Priorities	Ranking
Increasing enterprise growth	1	Cloud computing	1
Attracting and retaining new customers	2	Virtualization	2
Reducing enterprise costs	3	Mobile technologies	3
Creating new products and services (innovation)	4	IT management	4
Improving business processes	5	Business intelligence	5
Implementing and updating business applications	6	Networking, voice and data communications	6
Improving technical infrastructure	7	Enterprise applications	7
Improving enterprise efficiency	8	Collaboration technologies	8
Improve operations	9	Infrastructure	9
Improving business continuity, risk and security	10	Web 2.0	10

Source: Gartner EXP (January 2011)

- **Currently, 3 percent of CIOs have the majority of IT running in the cloud or on SaaS technologies, but over the next four years CIOs expect this number to increase to 43 percent.**

The NIST Cloud Definition Framework



Deployment Models

Hybrid Clouds

Private Cloud

Community Cloud

Public Cloud

Service Models

Software as a Service (SaaS

Platform as a Service (PaaS)

Infrastructure as a Service (IaaS)

Compute

Storage

Network

Essential Characteristics

On-Demand Self-Service

Broad Network Access

Rapid Elasticity

Resource Pooling

Measured Service

Common Characteristics

Massive Scale

Resilient Computing

Homogeneity

Geographic Distribution

Virtualization

Service Orientation

Low Cost Software

Advanced Security

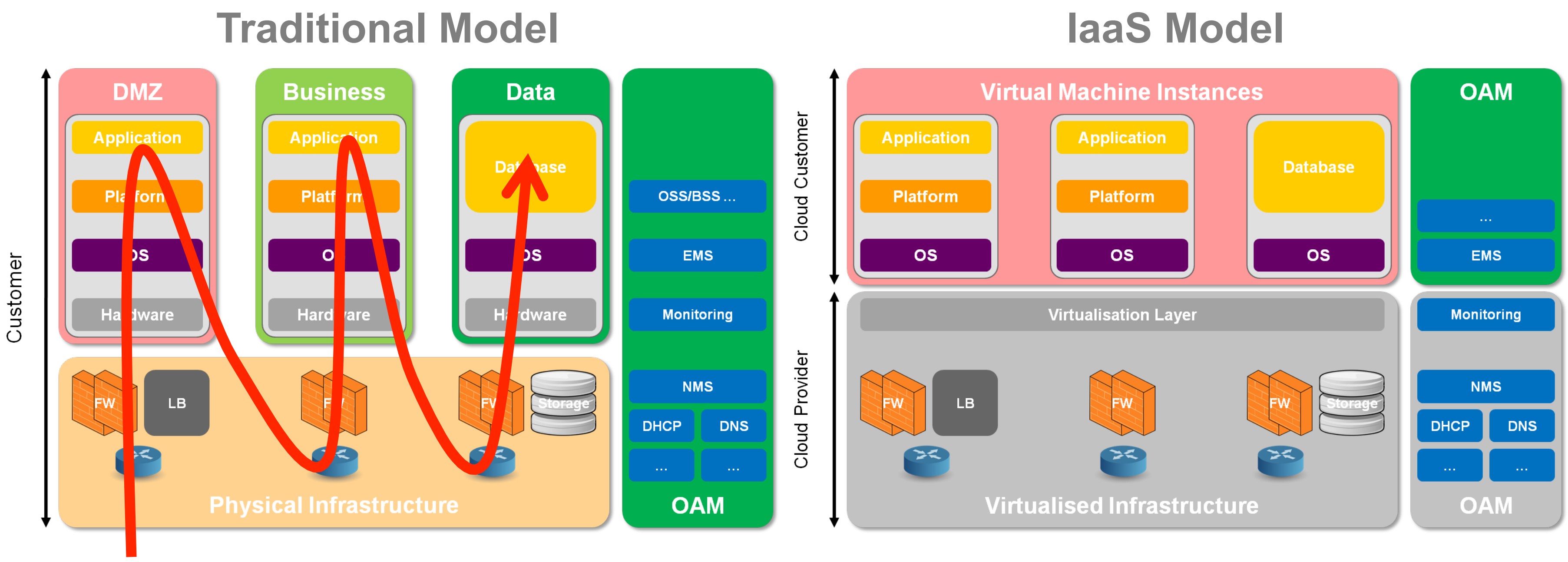
TOP 10 Cloud Computing Providers

SearchCloudComputing.com TOP 10 CLOUD COMPUTING PROVIDERS OF 2011

Provider	Sector	2011		2010
Amazon AWS	Public IaaS	1	→	1
Verizon/Terremark	Public IaaS	2	↗	10/8
IBM Cloud	Private IaaS	3	↗	-
Salesforce	Public SaaS and PaaS	4	→	3
CSC BizCloud	Cloud/IT Integrator	5	↗	-
Rackspace	Public IaaS	6	↘	2
Google App Engine	Public PaaS	7	↘	4
BlueLock	Public IaaS	8	↗	-
Microsoft Azure	Public PaaS	9	↘	5
Joyent	Private IaaS and PaaS, Public IaaS	10	↘	6

Reference: Top 10 cloud computing providers of 2011, by SearchCloudComputing.com Staff

Traditional versus IaaS Model



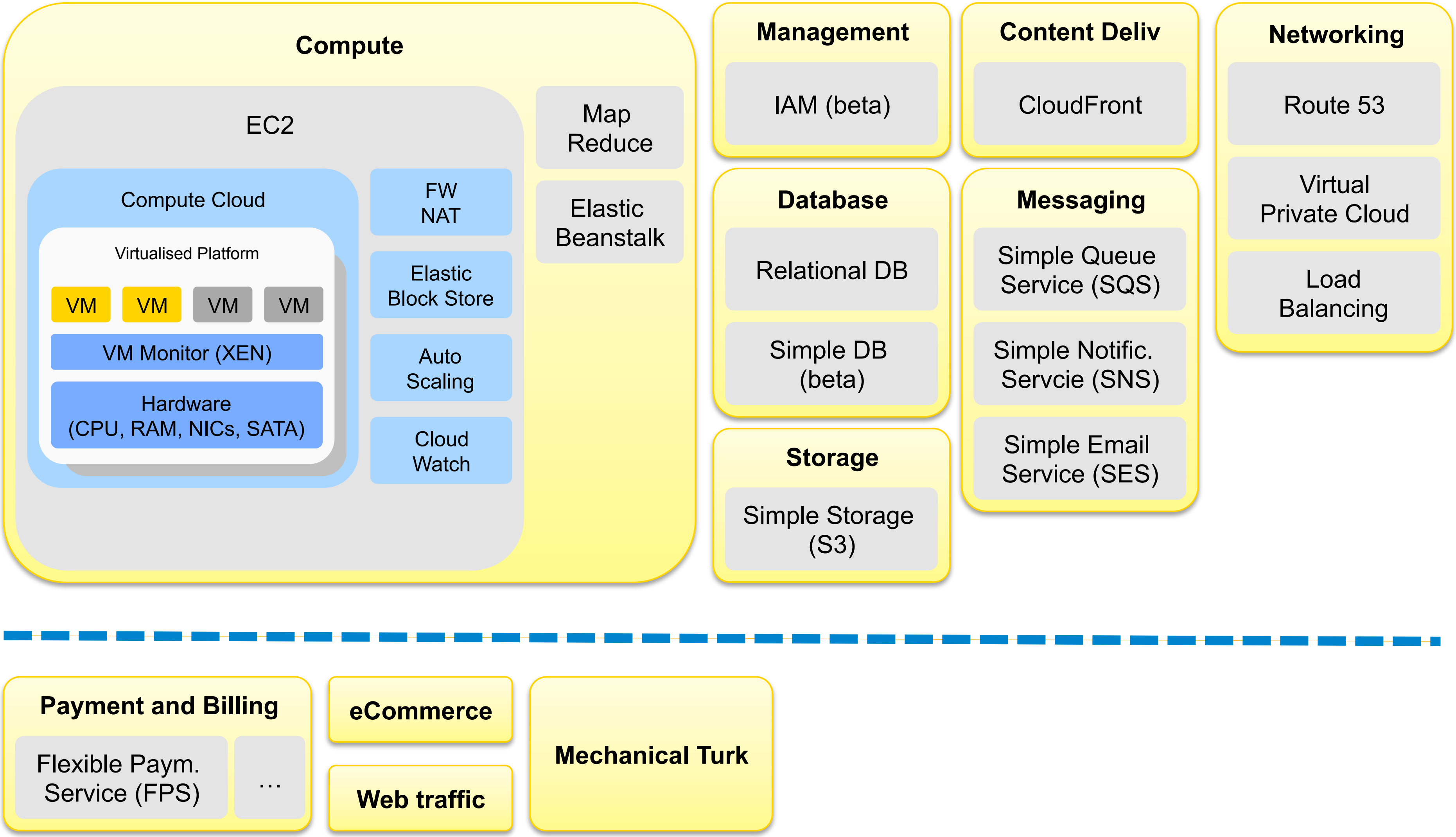
Physical and / or VLAN separation of traffic types, e.g. user, media, management traffic → **Virtualised** hardware, **logical** traffic separation (based on addresses, no VLANs)

Perimeter security, physical separation of server functions and mutliple tier architecture → **Logical** separation of VMs based on addresses

Authentication and encryption on demand → Strong **authentication** and **encryption** of all interfaces

Flexible adaption to security needs (web application firewalls, etc.) → **Basic security responsibility with cloud provider**, define requirements in SLA

Amazon Web Services (AWS): Overview



Compute

EC2

Compute Cloud

Virtualised Platform

VM VM VM VM

VM Monitor (XEN)

Hardware (CPU, RAM, NICs, SATA)

FW NAT

Elastic Block Store

Auto Scaling

Cloud Watch

Map Reduce

Elastic Beanstalk

Management

IAM (beta)

Content Deliv

CloudFront

Networking

Route 53

Virtual Private Cloud

Load Balancing

Database

Relational DB

Simple DB (beta)

Messaging

Simple Queue Service (SQS)

Simple Notific. Servcie (SNS)

Simple Email Service (SES)

Storage

Simple Storage (S3)

Payment and Billing

Flexible Paym. Service (FPS)

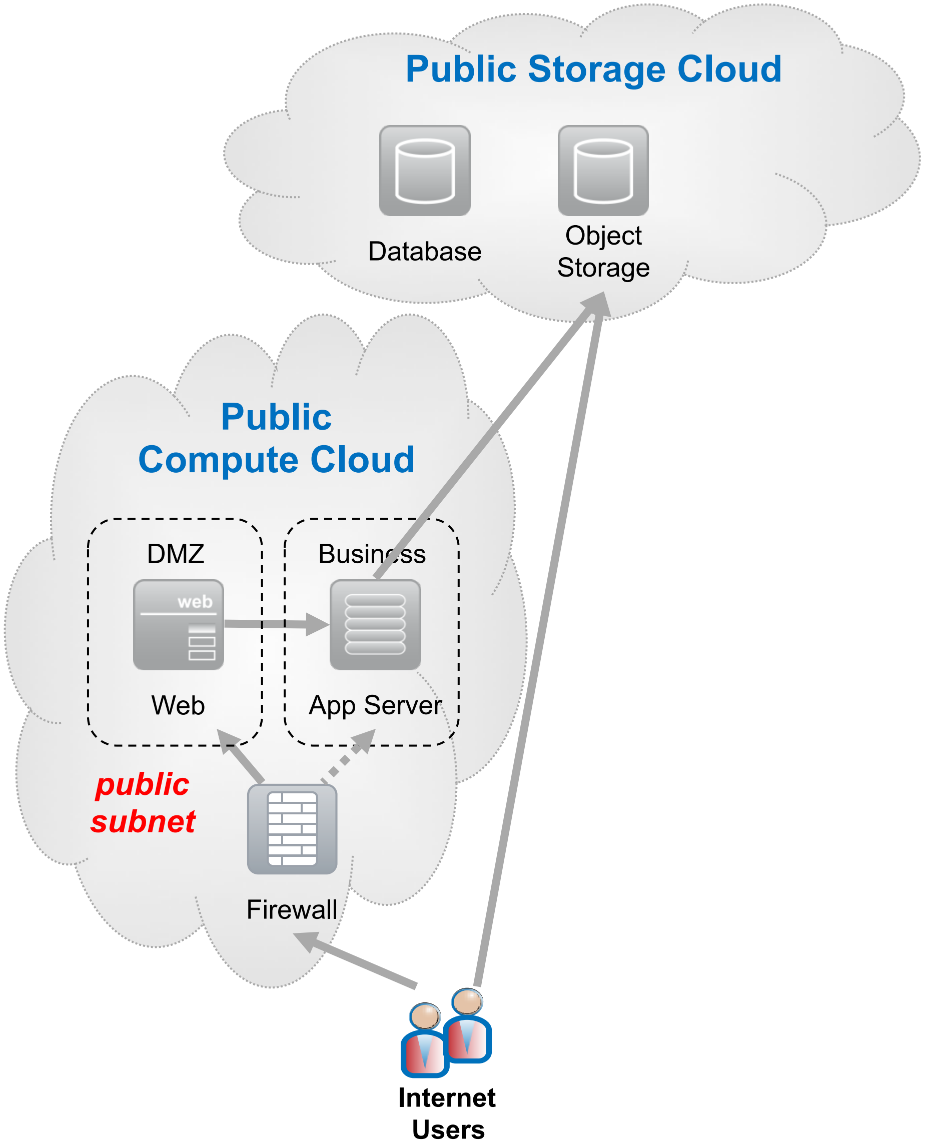
…

eCommerce

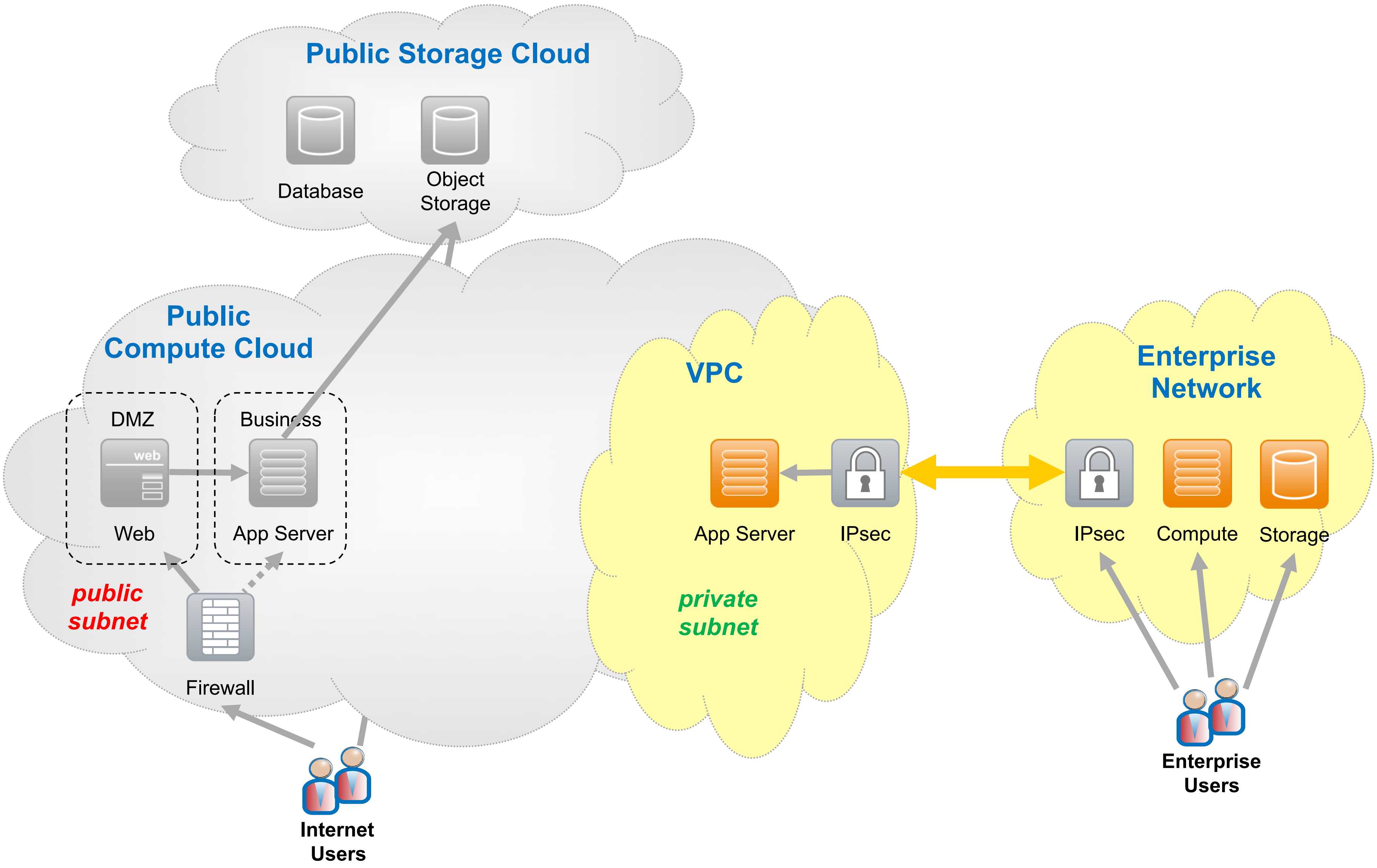
Web traffic

Mechanical Turk

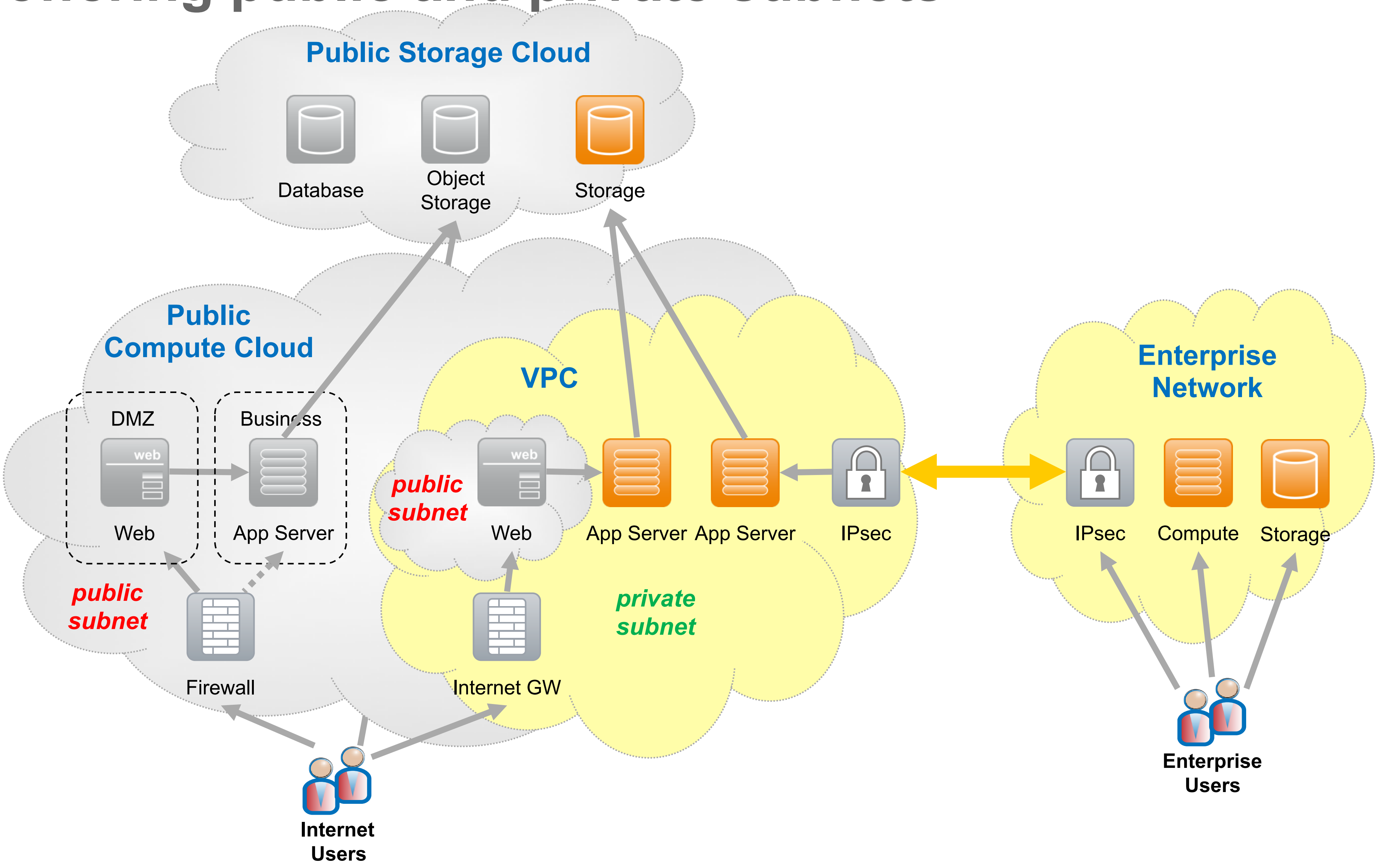
Cloud Architectures: Public Cloud



Cloud Architectures: Public Cloud with VPC



Cloud Architectures: Public Cloud with VPC offering public and private subnets



Agenda

1. Cloud Computing Introduction

2. Security Issues

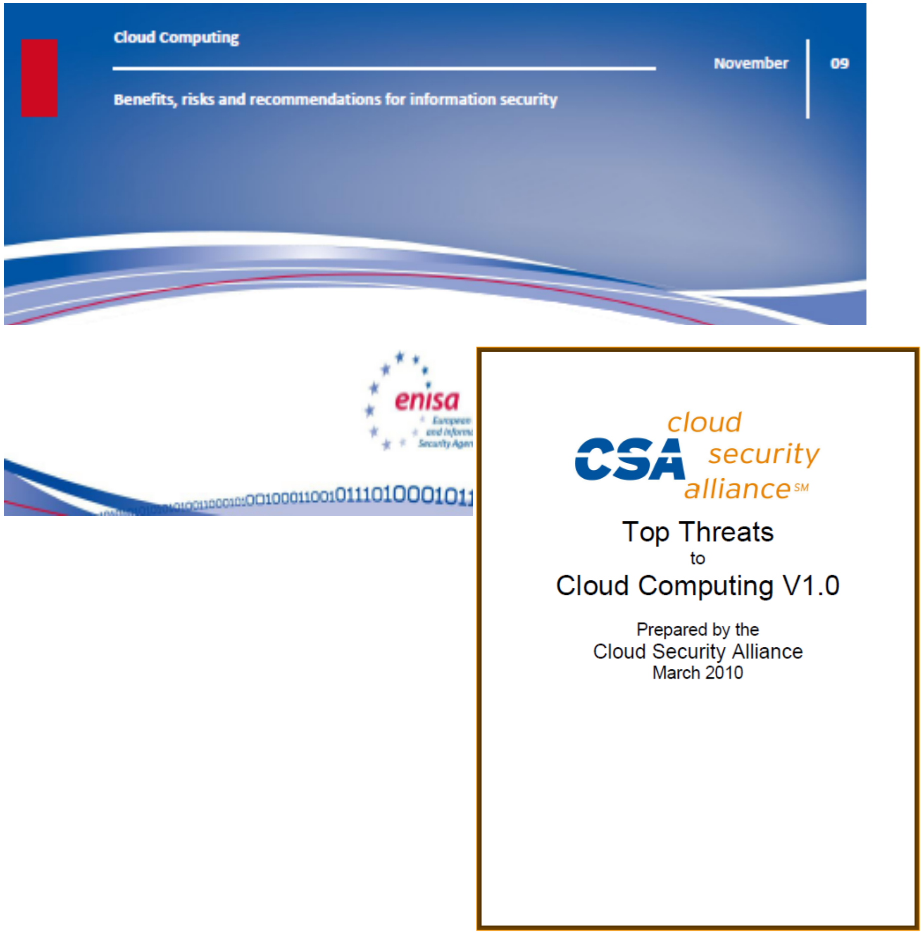
3. Regulation and National Initiatives

4. Use Cases

5. References

Cloud Security Threat / Risk Assessment

- Risk assessment material from **ENISA** and **CSA**



Cloud Computing

Benefits, risks and recommendations for information security

November 09

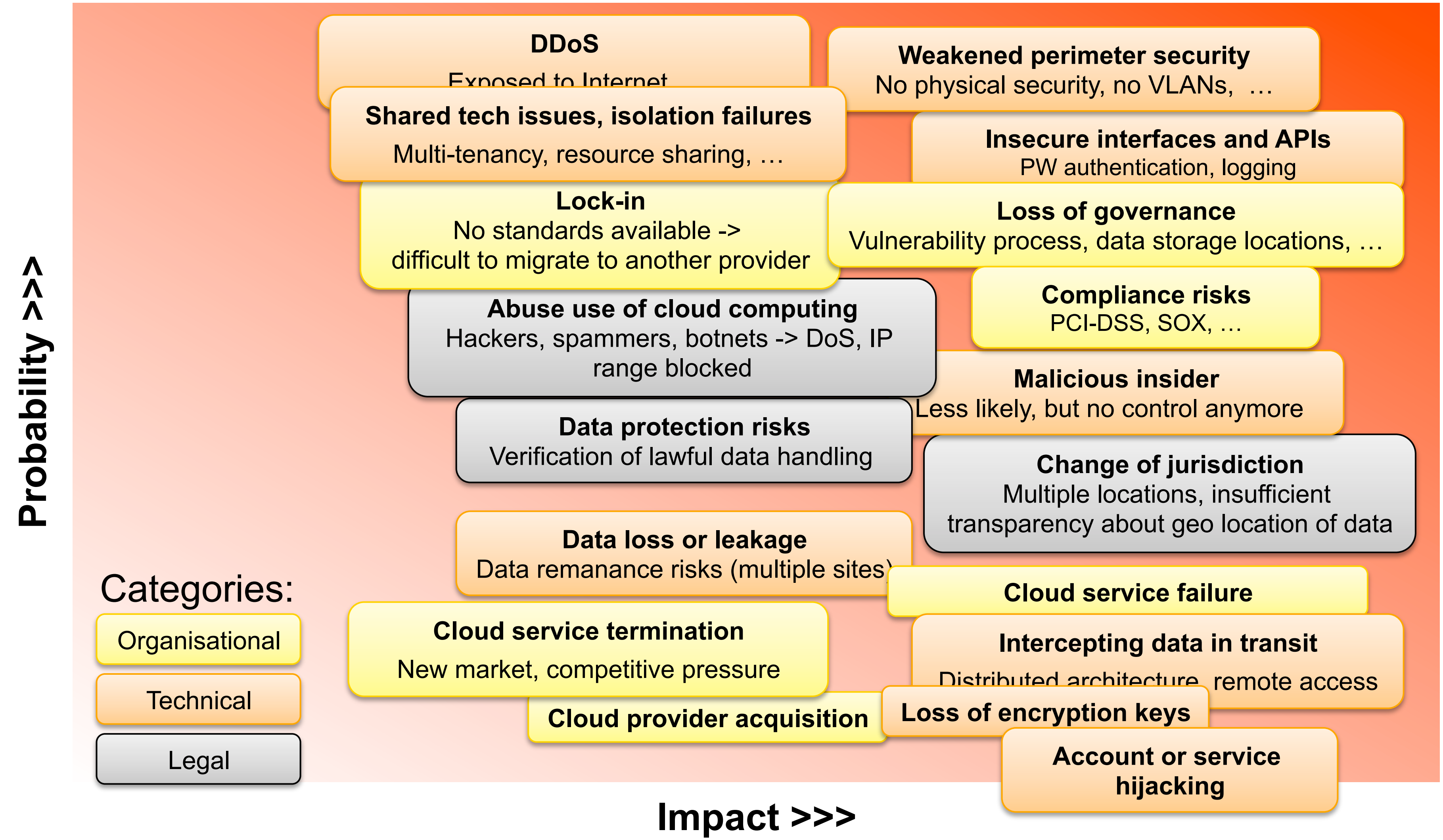
cloud security alliance℠

Top Threats to Cloud Computing V1.0

Prepared by the Cloud Security Alliance
March 2010

- The security risks sometimes differ dependent on the XaaS cloud service e.g. lock-in risk is higher with SaaS (e.g. CRM software service) than with IaaS (e.g. Amazon EC2 cloud infrastructure).
- Many security risks are equally valid both for legacy architectures and for cloud platforms.
- Nevertheless compared to legacy architectures the cloud computing risks are sometimes higher since
  - probability is higher for threats such as lock-in, compliance challenges, etc.
  - impact is greater for threats such as malicious insider (considering the aggregate of customers), etc.

Cloud Security Risks: Important organisational, technical, and legal risks



DDoS
Exposed to Internet

Weakened perimeter security
No physical security, no VLANs, …

Shared tech issues, isolation failures
Multi-tenancy, resource sharing, …

Insecure interfaces and APIs
PW authentication, logging

Lock-in
No standards available -> difficult to migrate to another provider

Loss of governance
Vulnerability process, data storage locations, …

Compliance risks
PCI-DSS, SOX, …

Abuse use of cloud computing
Hackers, spammers, botnets -> DoS, IP range blocked

Malicious insider
Less likely, but no control anymore

Data protection risks
Verification of lawful data handling

Change of jurisdiction
Multiple locations, insufficient transparency about geo location of data

Data loss or leakage
Data remanance risks (multiple sites)

Cloud service failure

Cloud service termination
New market, competitive pressure

Intercepting data in transit
Distributed architecture, remote access

Cloud provider acquisition

Loss of encryption keys

Account or service hijacking

Categories:

- Organisational
- Technical
- Legal

Probability >>>

Impact >>>

Cloud Provider Security: Some major differences

Security Feature	A	R	T
Disaster redundant data centers	x		
Configurable packet filter rules in firewall	x		x
Network zones (security groups) support	x		x
VM backup / restore		x	
Resource (compute/storage) location choice	x		
Secure remote shell access using keys	x		x
Central credential management	x	(x)	(x)
External audits (SAS 70 Type II, ISAE 3402)	x	x	x
ISO 27001/27002 certification	x		
PCI-DSS compliance	x		

Cloud Provider Security: The major observed shortcomings of current cloud offerings (1)

Shortcoming	Best practice security solution
Data encryption	Data must be encrypted at all stages.
Logging of management actions	Every management action must be logged.
Multiple users with role based access control	It must be possible to create multiple users per account and manage roles and permissions for each of these users.
Event management logs for audits and relevant security events	Security violations at a system (e.g. authentication failures, unauthorized access attempts) must be logged.
Push of log files	It must be possible to configure pushing of log files to external destinations, e.g. via e-mail.
Consistent monitoring data	Cloud providers must supply consistent formats to monitor cloud applications and service performance compatible with existing monitoring systems.

Cloud Provider Security: The major observed shortcomings of current cloud offerings (2)

Shortcoming	Best practice security solution
Support for common IDM standards	Cloud provider must support common IDM standards in order to integrate cloud access management in the enterprise IT infrastructure.
Portability / Interoperability	Cloud providers must support interoperability standards so that organizations can combine any cloud provider's capabilities into their solutions, i.e. must support common APIs, e.g. OVF 1.0.

Major Security Challenges for the Cloud Customer

Cloud Indepence

Cloud service termination
New market, competitive pressure

Lock-in
No standards available ->
difficult to migrate to another provider

Cloud provider acquisition

Cloud service failure

Authentication and Encrpytion

Shared tech issues, isolation failures
Multi-tenancy, resource sharing, …

Insecure interfaces and APIs
PW authentication, logging

Malicious insider
Less likely, but no control anymore

Data loss or leakage
Data remanance r

Intercepting data in transit
Distributed architecture, remote access

Defense In-Depth

Weakened perimeter security
No physical security, no VLANs, …

DDoS
Exposed to Internet,

Credential Management

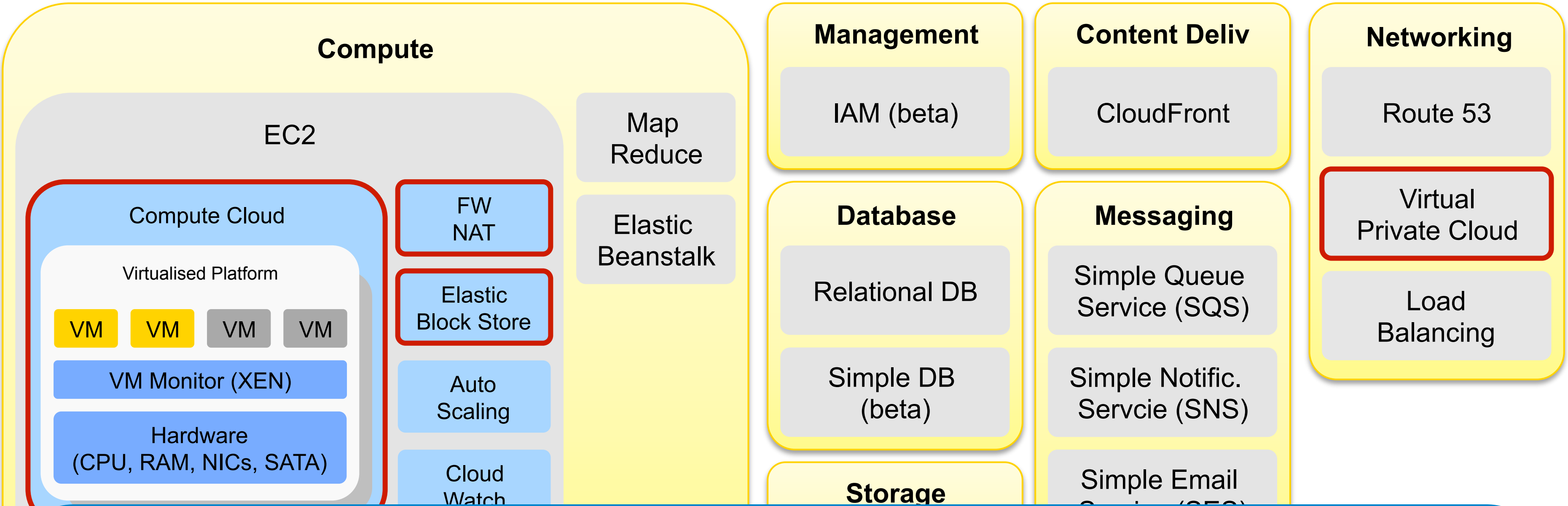
Loss of encryption keys

Account or service hijacking

Cloud Independence through Standards? … under discussion, but no real deployments

- DMTF’s Open Virtualization Format (format for the packaging and distribution of one or more virtual machines)
  - OVF became also an ANSI standard in August 2010.
  - OVF can be imported in some hypervisors, i.e. converted to the proprietary virtualisation format.
  - Export to OVF is in most cases not possible.
- SNIA’s The Cloud Data Management Interface (CDMI), V1.0, 2010: The Cloud Data Management Interface defines the functional interface that applications will use to create, retrieve, update and delete data elements from the Cloud.
- OGF’s Open Cloud Computing Interface (OCCI) is an API specification for remote management of cloud computing infrastructure supporting deployment, autonomic scaling and monitoring.
- Amazon APIs are the de-facto standard for management APIs and used in some open source cloud solutions.
- Dasein Cloud is an Open Source cloud abstraction API for the Java programming language. The API is heavily driven by George Reese, CTO of enStratus, which is a cloud infrastructure management solution for deploying and managing enterprise-class applications in public and private clouds.
- DeltaCloud is open source project within Red Hat to create a common, REST-based API with drivers that map the API to both public clouds like EC2, and private virtualized clouds based on VMWare and Red Hat Enterprise Linux with integrated KVM.
- libcloud is a standard client library for many popular cloud providers, written in python and java.

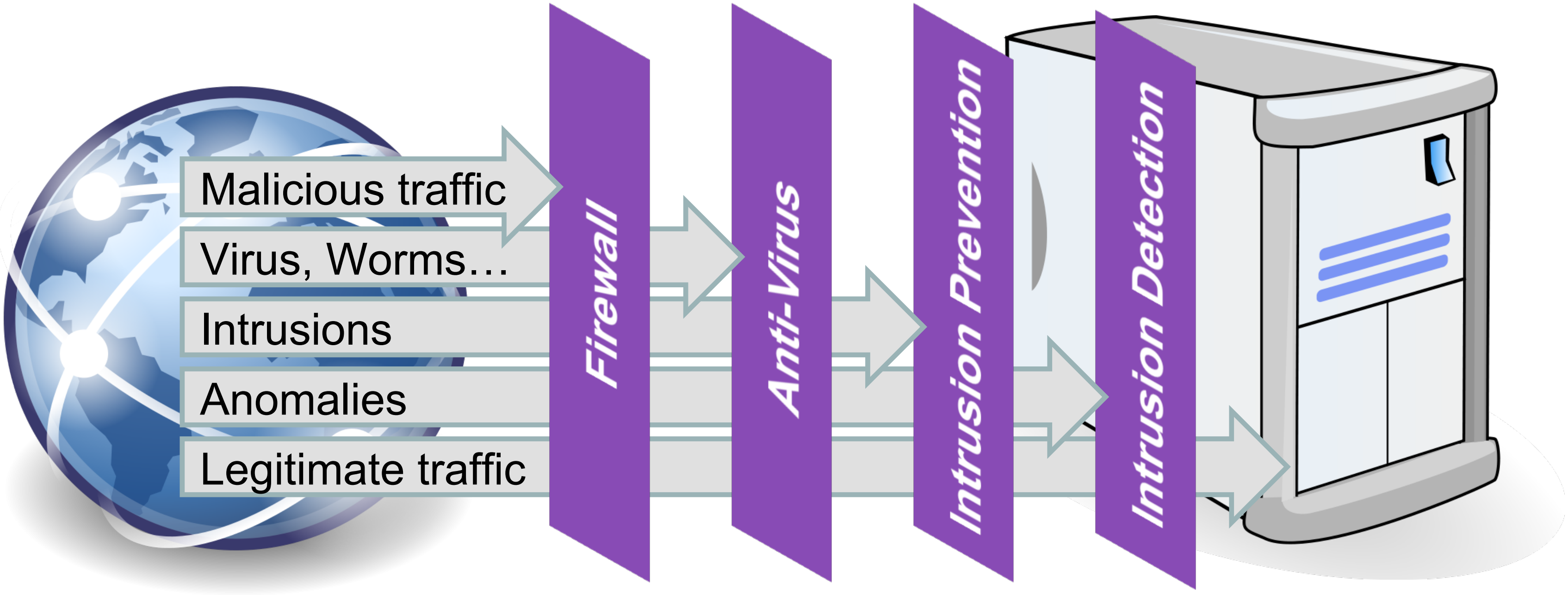
Cloud Independence through Usage of Common Services



Recommendation

- ❖ Design the solution such that it does not rely on proprietary cloud provider services.
- ❖ Investigate which services are mandatory for the cloud solution.
- ❖ Possibly construct own services as virtual appliances for usage in multiple cloud environments (e.g. load balancer)

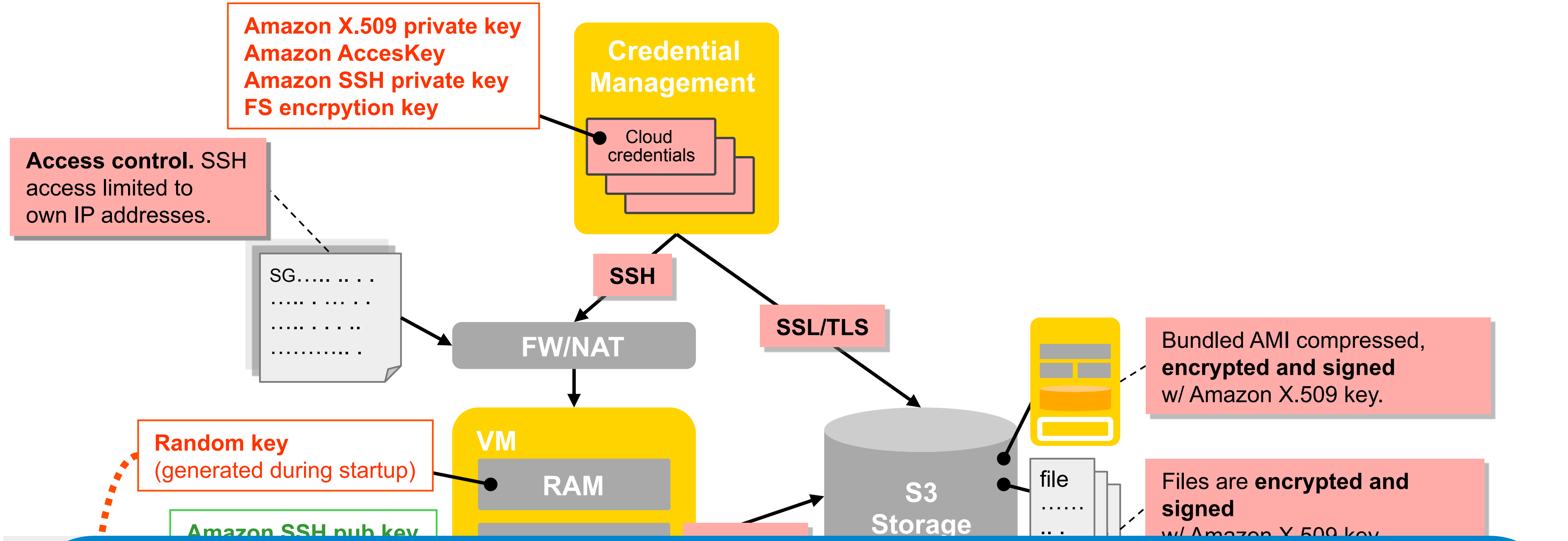
Layered Defense In-Depth Strategy



Recommendation

- Install and configure a host-based firewall (like ipfilter or iptables)
- Use firewall rules to configure IP traffic to/from VMs in order completely isolate every tier.
- Configure the firewall such that SSH access to the VMs is limited to own location.
- Install Anti-Virus software (if applicable)
- Install a host-based IDS and a network IDS (such as Snort)

Authentication and Encryption



Amazon X.509 private key
Amazon AccesKey
Amazon SSH private key
FS encrpytion key

Credential Management

Cloud credentials

Access control. SSH access limited to own IP addresses.

SG….. .. . .
….. . … . .
….. . . . ..
……….. .

SSH

SSL/TLS

FW/NAT

VM

RAM

Random key (generated during startup)

Amazon SSH pub key

en

S3 Storage

file
……

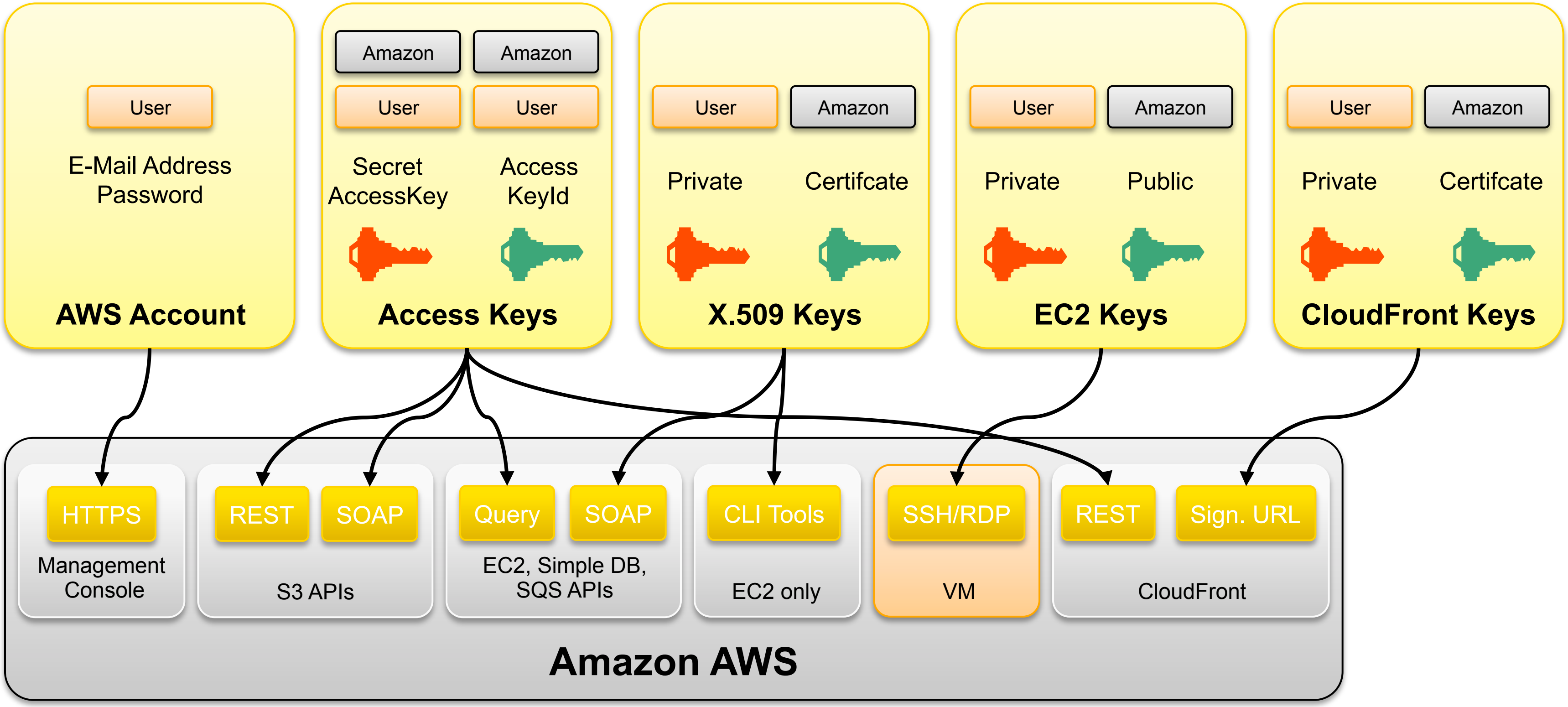
Bundled AMI compressed, **encrypted and signed** w/ Amazon X.509 key.

Files are **encrypted and signed** w/ Amazon X.509 key.

Recommendation

- ❖ **Perform strong authentication .i.e. strong password policy (complexity, aging, login attempts) or use keys.**
- ❖ **Encrpyt all network traffic.**
- ❖ **Use only encrypted file systems for block devices and non-root local devices.**
- ❖ **Encrypt objects stored in cloud storage using strong encryption.**
- ❖ **Sign objects stored in the cloud.**

Credential Management is Key for a Public Cloud Deployment



AWS Account
User
E-Mail Address
Password

Access Keys
Amazon | Amazon
User | User
Secret AccessKey | Access KeyId

X.509 Keys
User | Amazon
Private | Certifcate

EC2 Keys
User | Amazon
Private | Public

CloudFront Keys
User | Amazon
Private | Certifcate

Amazon AWS
HTTPS – Management Console
REST, SOAP – S3 APIs
Query, SOAP – EC2, Simple DB, SQS APIs
CLI Tools – EC2 only
SSH/RDP – VM
REST, Sign. URL – CloudFront

Recommendation

- ❖ Store credentials securely and allow only authorized access.
- ❖ Automatically generate new credentials in regular intervals.

❖ Automatically generate new credentials in regular intervals.

Agenda

1. Cloud Computing Introduction

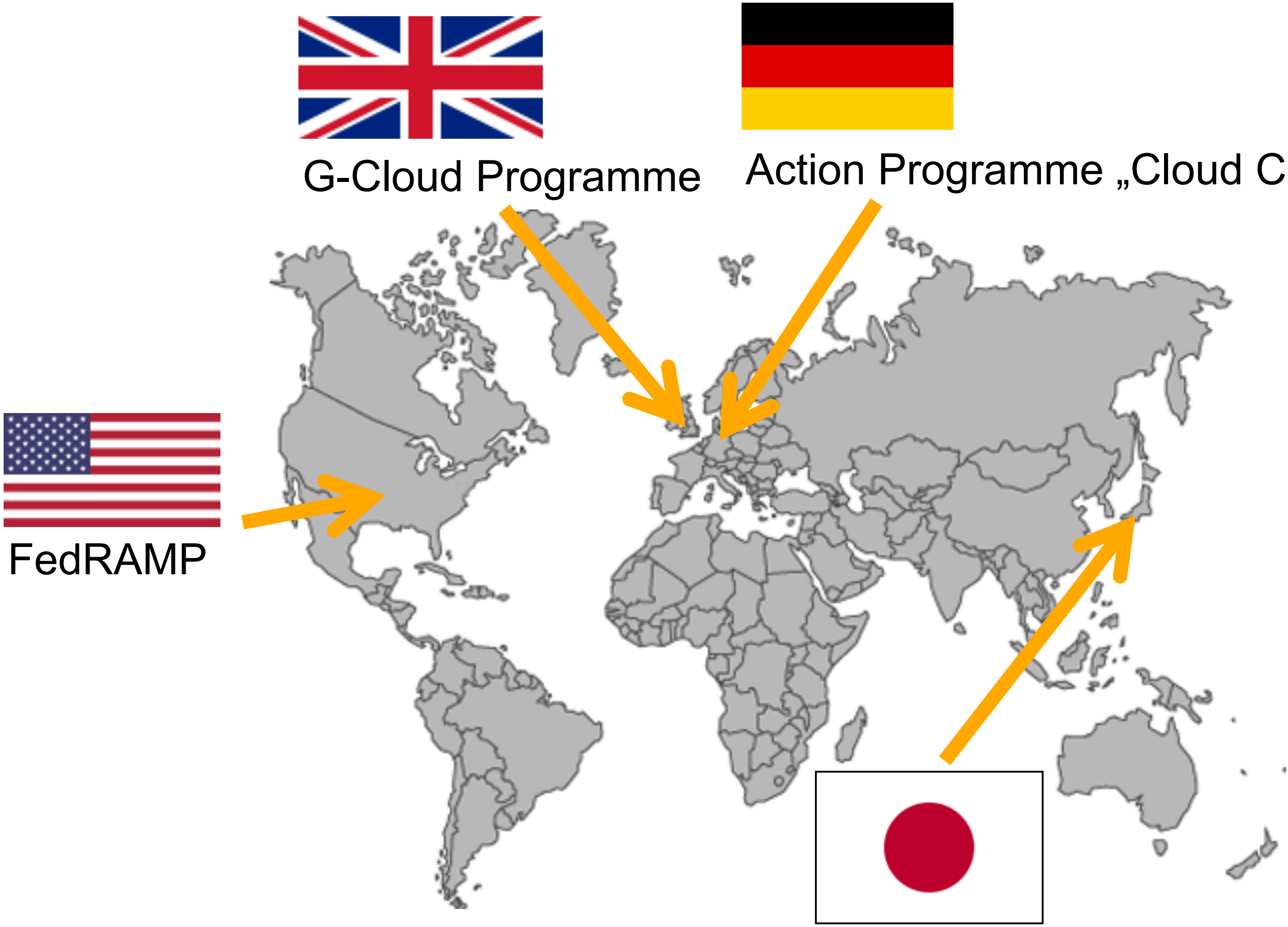
2. Security Issues

3. Regulation and National Initiatives

4. Use Cases

5. References

National Initiatives (selection)



G-Cloud Programme

Action Programme „Cloud Computing“

FedRAMP

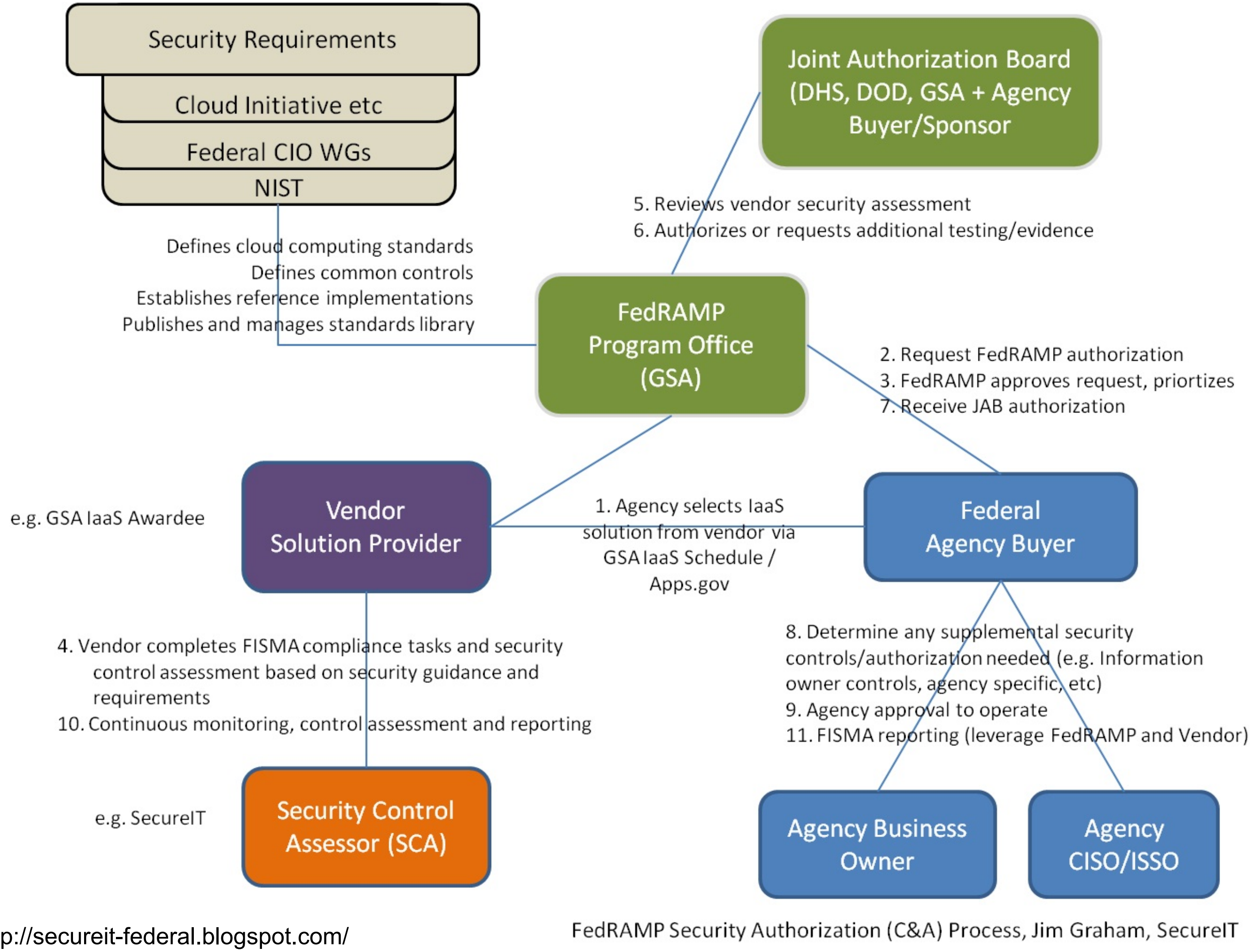
Kasumigaseki Cloud

… and many more

FedRAMP

- Released 11/2010 by GSA
- Aims to create a federal risk management process
  - Establishing security requirements among federal departments
  - Facilitating compatible security requirements on shared systems
  - Reducing duplication of effort
  - Eliminate unnecessary costs
  - Enabling rapid acquisition through pre-authorized solutions
  - Encouraging improved system integration with government-wide security initiatives
  - Using focus assessments to increase security

FedRAMP


Security Requirements
Cloud Initiative etc
Federal CIO WGs
NIST
Defines cloud computing standards
Defines common controls
Establishes reference implementations
Publishes and manages standards library
Joint Authorization Board (DHS, DOD, GSA + Agency Buyer/Sponsor
5. Reviews vendor security assessment
6. Authorizes or requests additional testing/evidence
FedRAMP Program Office (GSA)
2. Request FedRAMP authorization
3. FedRAMP approves request, priortizes
7. Receive JAB authorization
e.g. GSA IaaS Awardee
Vendor Solution Provider
1. Agency selects IaaS solution from vendor via GSA IaaS Schedule / Apps.gov
Federal Agency Buyer
4. Vendor completes FISMA compliance tasks and security control assessment based on security guidance and requirements
10. Continuous monitoring, control assessment and reporting
8. Determine any supplemental security controls/authorization needed (e.g. Information owner controls, agency specific, etc)
9. Agency approval to operate
11. FISMA reporting (leverage FedRAMP and Vendor)
e.g. SecureIT
Security Control Assessor (SCA)
Agency Business Owner
Agency CISO/ISSO

FedRAMP Security Authorization (C&A) Process, Jim Graham, SecureIT

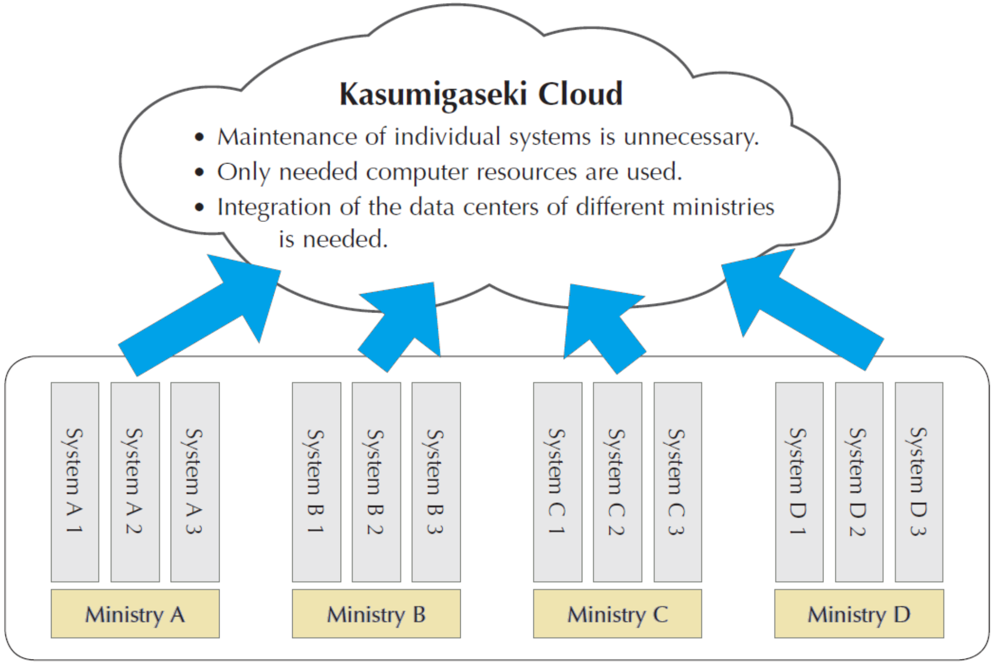
Source: http://secureit-federal.blogspot.com/

G-Cloud Programme

- Phase 1 (5/2009 – 10/2009): Feasibility study
- Phase 2 (10/2009 – 4/2010): High level design
  1. G-Cloud Vision
  2. G-Cloud Commercial Strategy
  3. G-Cloud Strategic Outline Business Case
  4. G-Cloud Implementation Strategy
  5. G-Cloud Information Assurance Report **(not published)**
  6. G-Cloud Service Management, Organizational Structure and Governance
  7. G-Cloud Service Specification
  8. G-Cloud Technical Architecture
  9. G-Cloud Founding Principles
- Further development of plans for adoption of cloud computing to the public sector is on-going

Kasumigaseki Cloud

- Outline presented 3/2009 by Ministry of International Affairs and Communications (MIC), Japan
- Aims to develop a private cloud for hosting all of the Japanese government's computing
- Part of the Digital Japan Creation Project (ICT Hatoyama Plan which seeks to create new ICT markets to help boost Japan's economy



Source: Government of Japan, MIC (2009)

Action Programme Cloud Computing

- Presented 10/2010 by BMWi
- Included an estimation for the expected market development:
  - 2010: 1142 Mio. € spent for cloud computing
  - 2013: 4452 Mio. € spent for cloud computing
- Estimates that in 2025 (or earlier) 75% of all private and business data are stored in the internet

- Technology Competition Trusted Cloud
  - Started 09/2010
  - 12 Winners presented at Cebit (March 1st)
  - BMWi will spend 50 Mio. € over the next 3 years for funding

National IT-Summit

- Central collaboration platform for politics, industry and science
- Consists of 8 Working groups
- Working group 4 ”Trust, Privacy and Security in the internet“ works on two topics
  1. Secure identities in the internet
  2. Cloud Computing
- Topic Cloud Computing consists of
  – Definition of legal requirements for the use of cloud services
  – Definition of technical requirements for the use of cloud services
  – Support of projects and best practices for a secure cloud environment
  – Identification of domains for further research for the IT-Security Research Program of the government

Agenda

1. Cloud Computing Introduction

2. Security Issues

3. Regulation and National Initiatives

4. Use Cases

5. References

Logistics Mall

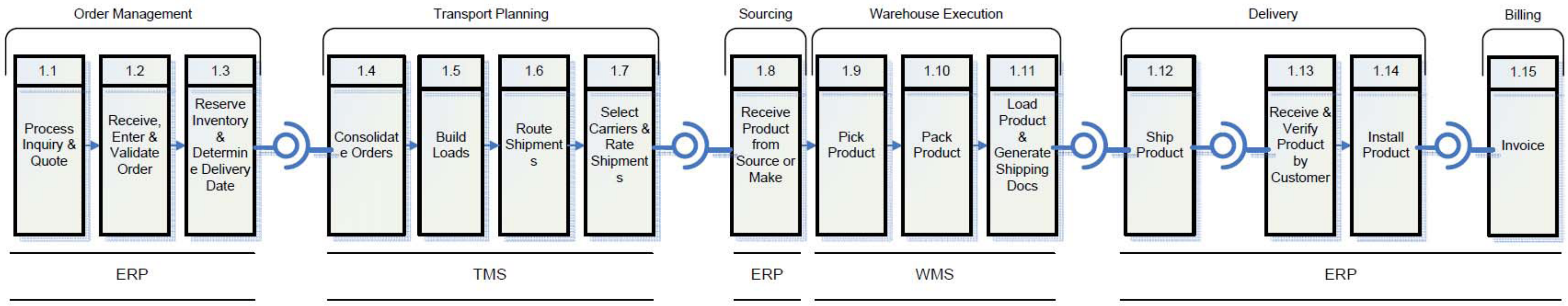
Some Facts about Logistics:

- 4,200 bn € market volume worldwide
- 205 bn € market volume in Germany
  - Third largest industry sector
  - 2.7 m employees
  - 4 bn € IT-Budget
- ~ 7 % growth rate (2009)
- 10%-15% portion of product price (end-consumer)
- Over 95% of involved enterprises are small or medium-sized

Logistics Mall

Software needs of a typical logistic company:

- ERP (Enterprise Resource Planning)
- WMS (Warehouse Management System)
- TMS (Tour Management System)
- DMS (Document Management System)
- Various Converters (EDI, XML, etc.)



Order Management: 1.1 Process Inquiry & Quote; 1.2 Receive, Enter & Validate Order; 1.3 Reserve Inventory & Determine Delivery Date — ERP

Transport Planning: 1.4 Consolidate Orders; 1.5 Build Loads; 1.6 Route Shipments; 1.7 Select Carriers & Rate Shipments — TMS

Sourcing: 1.8 Receive Product from Source or Make — ERP

Warehouse Execution: 1.9 Pick Product; 1.10 Pack Product; 1.11 Load Product & Generate Shipping Docs — WMS

Delivery: 1.12 Ship Product; 1.13 Receive & Verify Product by Customer; 1.14 Install Product — ERP

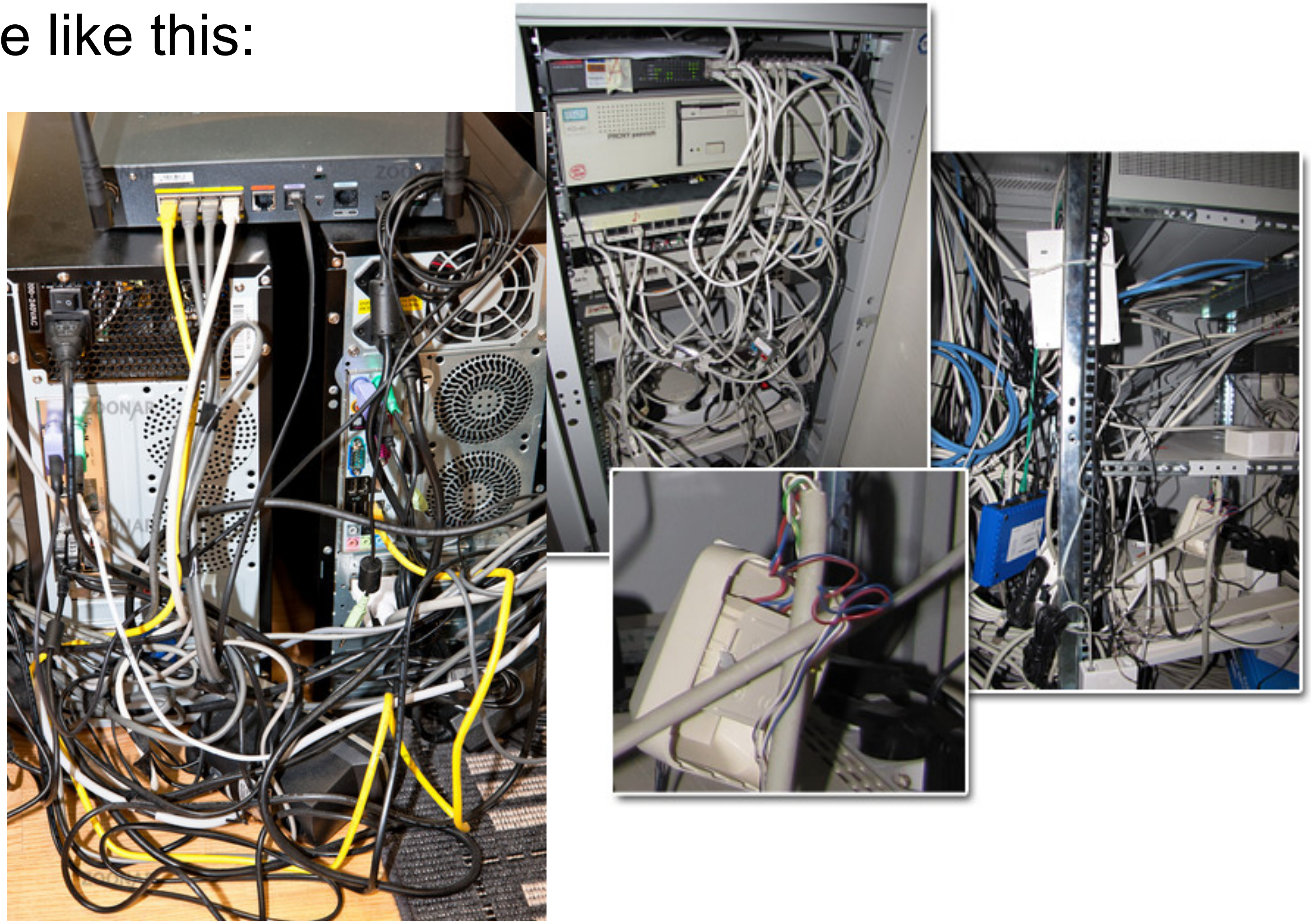
Billing: 1.15 Invoice — ERP

Logistics Mall

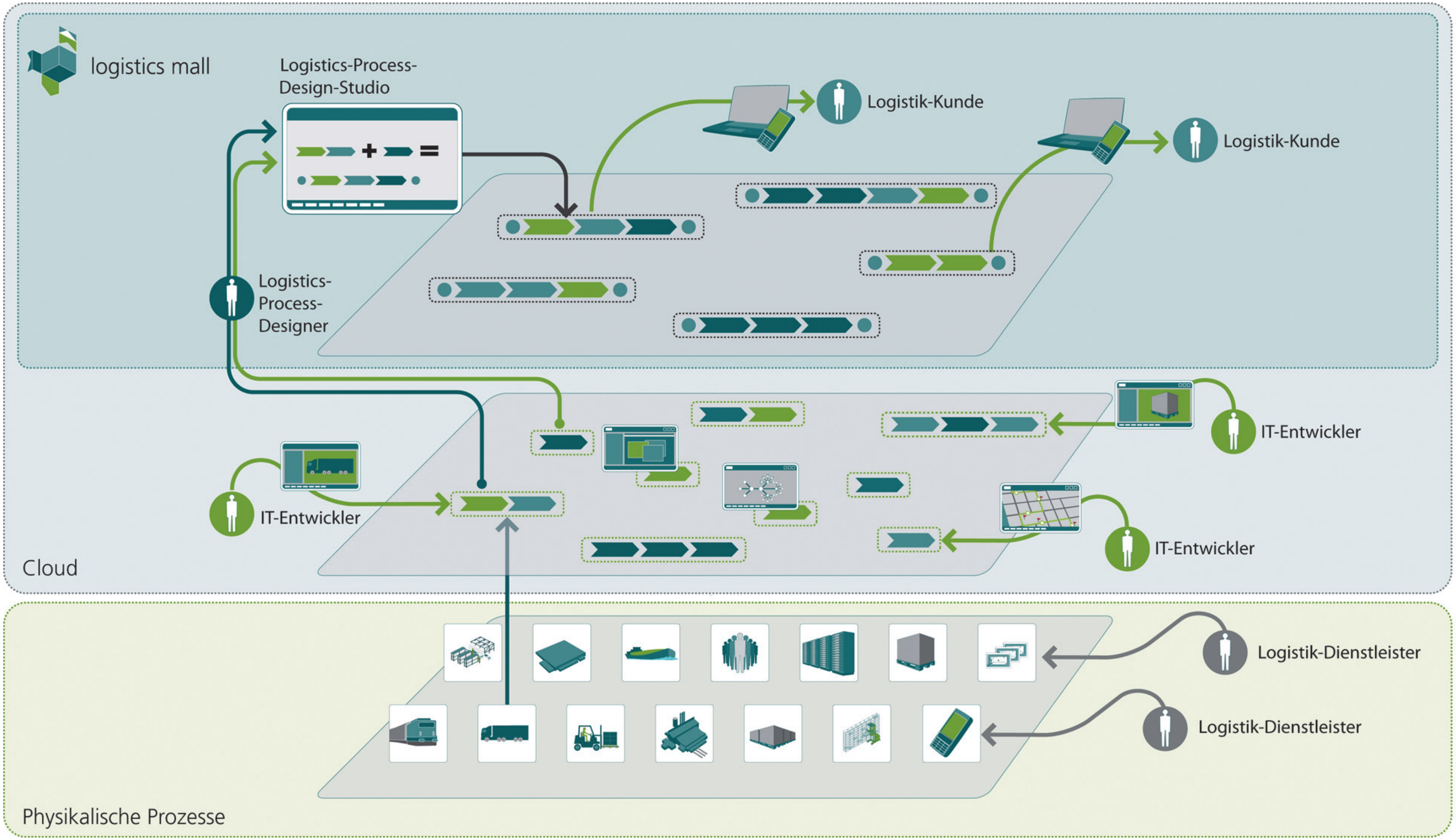
Don‘t expect something like this:

Logistics Mall

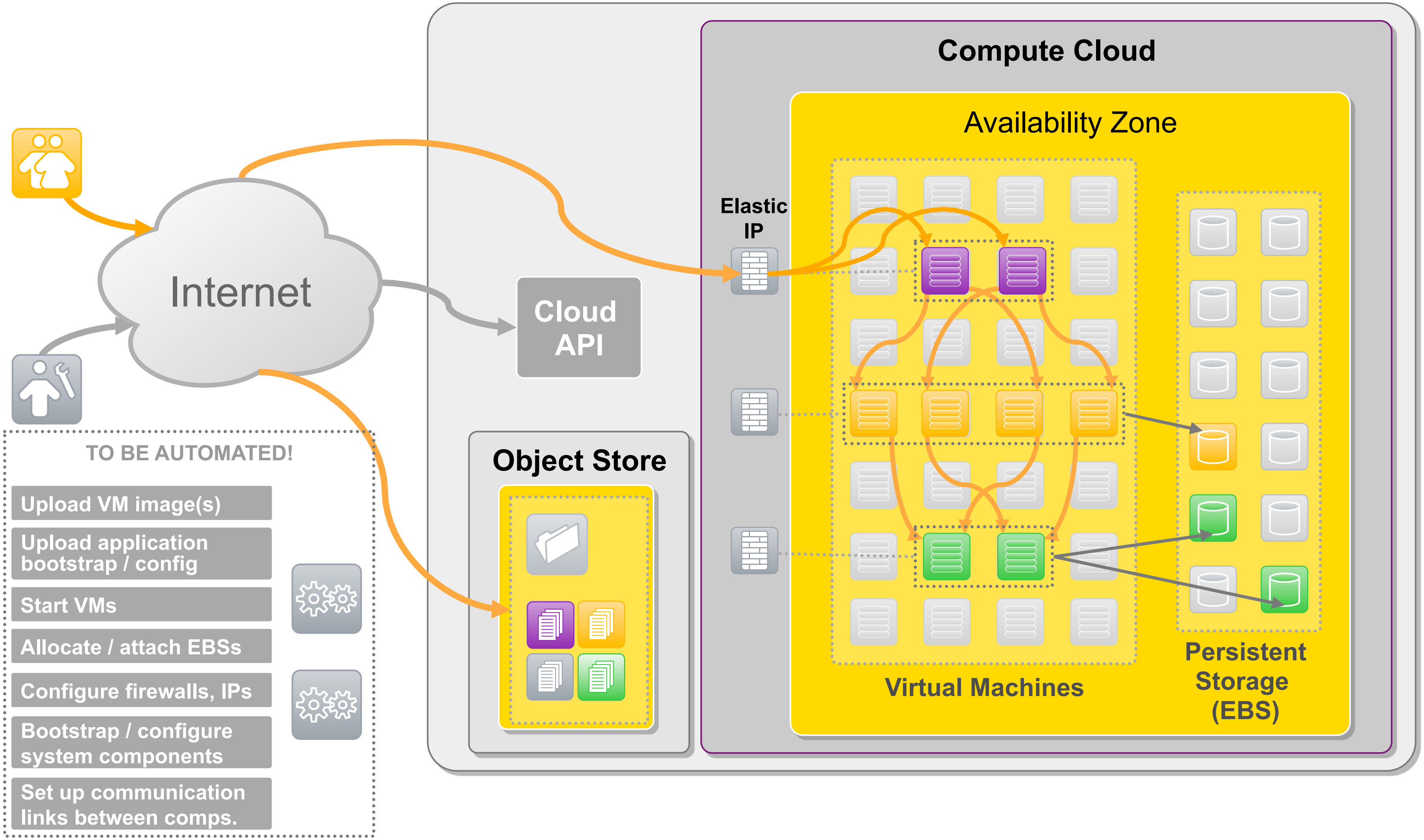
It‘s more like this:



Logistics Mall



IaaS Cloud Case Study
Deployment of Multi-tier Application Blueprints



TO BE AUTOMATED!

- Upload VM image(s)
- Upload application bootstrap / config
- Start VMs
- Allocate / attach EBSs
- Configure firewalls, IPs
- Bootstrap / configure system components
- Set up communication links between comps.

Experience with public Cloud Deployments

- In general, a reliable service, we haven't observed any major outage over the past 2 years of usage.
- A few times API access was suspended for several hours especially with one cloud provider.
- Performance of API interfaces are limited (API request limit exceeded)
- Parallel instantiation of multiple VMs causes problems on some cloud infrastructures.
- Unattended automatic deployment via APIs is not possible with all cloud providers, i.e. sometimes manual intervention is necessary.
- **Be aware that development on clouds is different compared to traditional lab environments.**
  - **Developers tend to assume a secure environment.**
  - **Unsecured VMs on public clouds are misused very quickly to e.g. act as a Spammer.**

Agenda

1. Cloud Computing Introduction

2. Security Issues

3. Regulation and National Initiatives

4. Use Cases

5. References

References

Abbreviation	Reference
[BITKOM_ENTSCH]	Bitkom, Leitfaden Cloud Computing – Was Entscheider wissen müssen, 2010, < http://www.bitkom.org/60376.aspx?url=BITKOM_Leitfaden_Cloud_Computing-Was_Entscheider_wissen_muessen.pdf&mode=0&b=Publikationen>
[BRADSHAW]	S. Bradshaw, C. Millard and I. Walden, Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services, Queen Mary University of London, September 2010, < http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374>
[CSA_TOPTHREATS]	Cloud Security Alliance, Top Threats to Cloud Computing V1.0, March 2010 <http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf>

References (cont‘d)

Abbreviation	Reference
[ENISA_CCRISK]	Enisa, "Cloud Computing – Benefits, risks and recommendations for information security", November 2009 < http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport>
[NIST_CLOUD]	NIST (Peter Mell and Tim Grance), "The NIST Definition of Cloud Computing", Version 15, July 2010, < http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc>
[REESE_KEYISSUES]	George Reese, "Key Security Issues for the Amazon Cloud" < http://broadcast.oreilly.com/2008/11/key-security-issues-for-the-am.html>
[REESE_20R]	George Reese; "Twenty Rules for Amazon Cloud Security" < http://broadcast.oreilly.com/2008/11/20-rules-for-amazon-cloud-security.html>

Thank You!