

Cloud computing

An overview (Part 2 draft version)
Cloud Security Issues

yvette@yvetteagostini.it

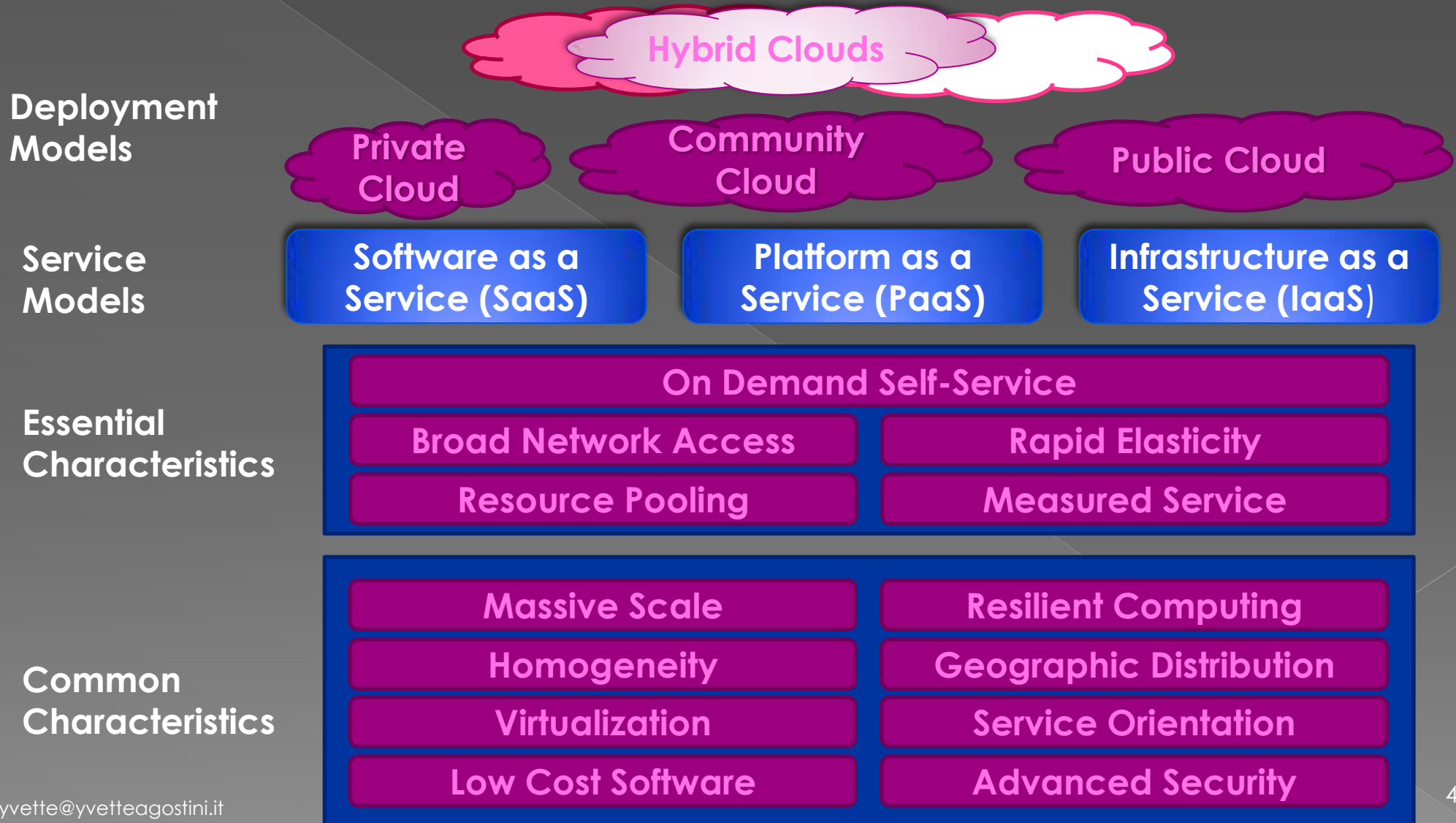
About this work

- The following is merely a collection of notes taken during works, study and just-for-fun activities
- No copyright infringements intended: all sources are duly listed at the end of the document
- This work is licensed under Creative Commons Attribution-Share Alike License
- No warranties on accuracy. Use it at your own risk, under the license terms.
- Feel free to drop me a line if you want to discuss the content of this document. My email address is yvette@yvetteagostini.it

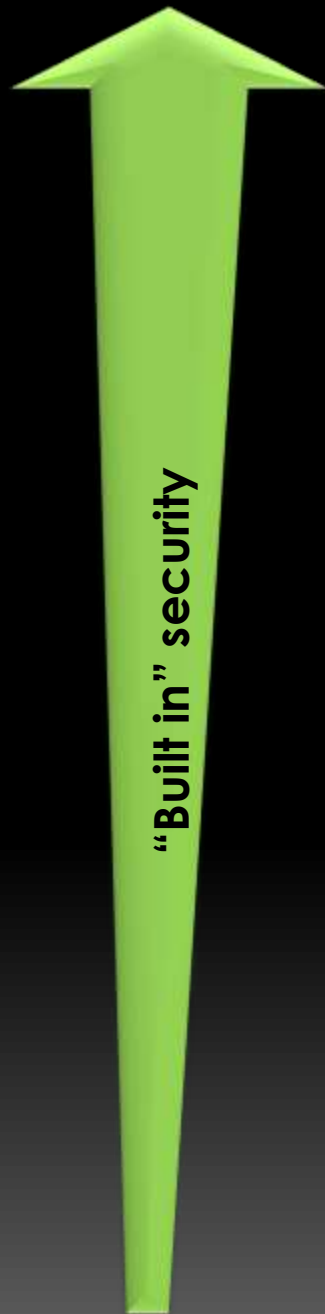
What we're talking about

- Both ENISA (European Network Information Security Agency) and Cloud Security Alliance approached the subject of assessing the risk involved in the adoption of cloud computing
- This presentation aims to summarize briefly the main points from the work of both mentioned organizations

Defining the Cloud: The NIST Cloud Definition Framework



CLOUD REFERENCE MODEL



SaaS

Presentation
modality

Presentation
platform

APIs

Applications

Data

Metadata

Content

PaaS

Integration & Middleware

IaaS

APIs

Core connectivity &
Delivery

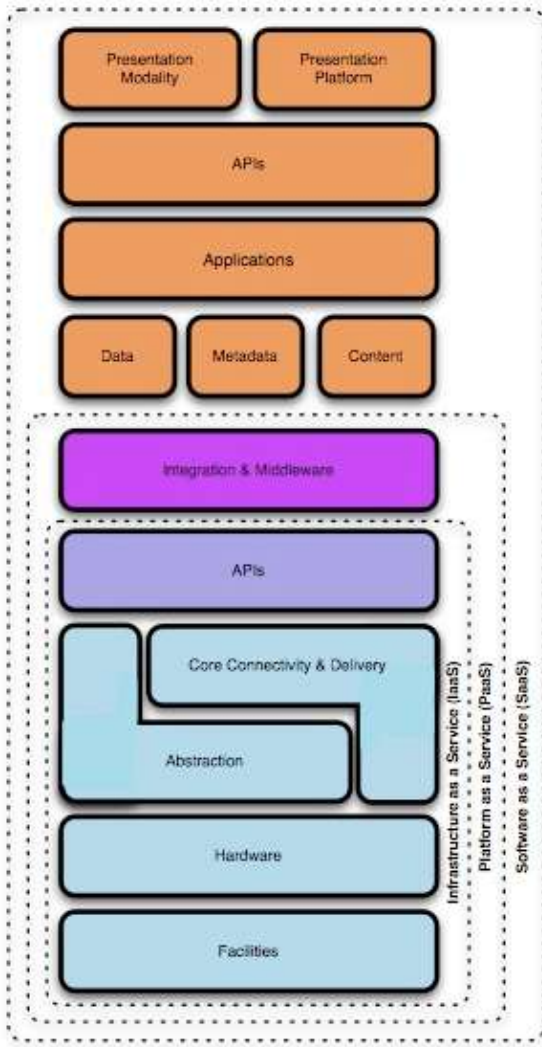
Abstraction

Hardware

Facilities

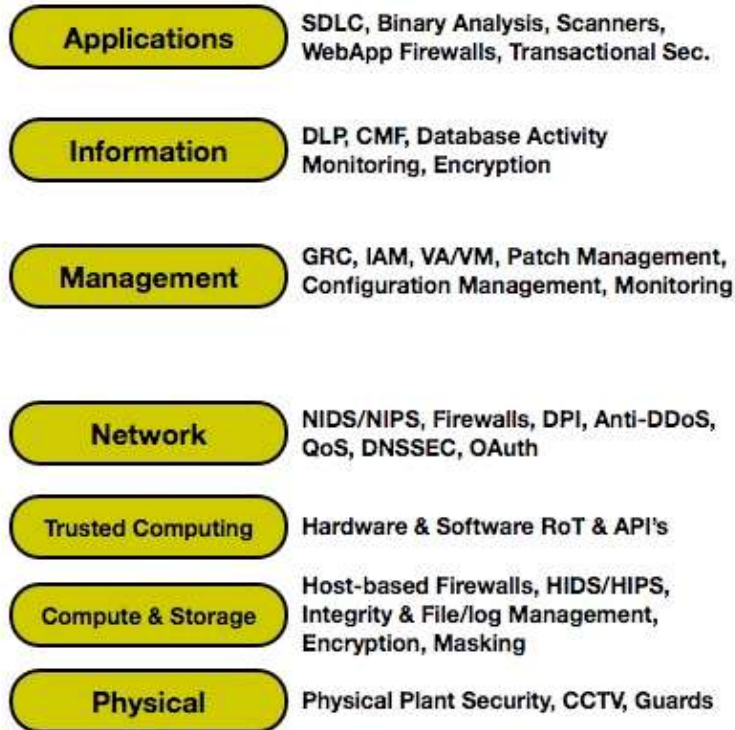
Cloud model and Security control

Cloud Model

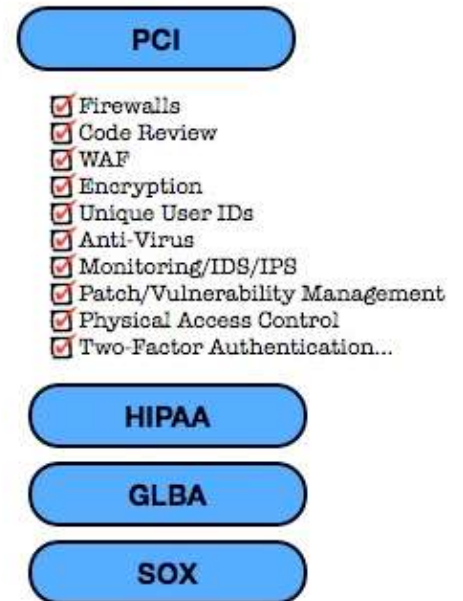


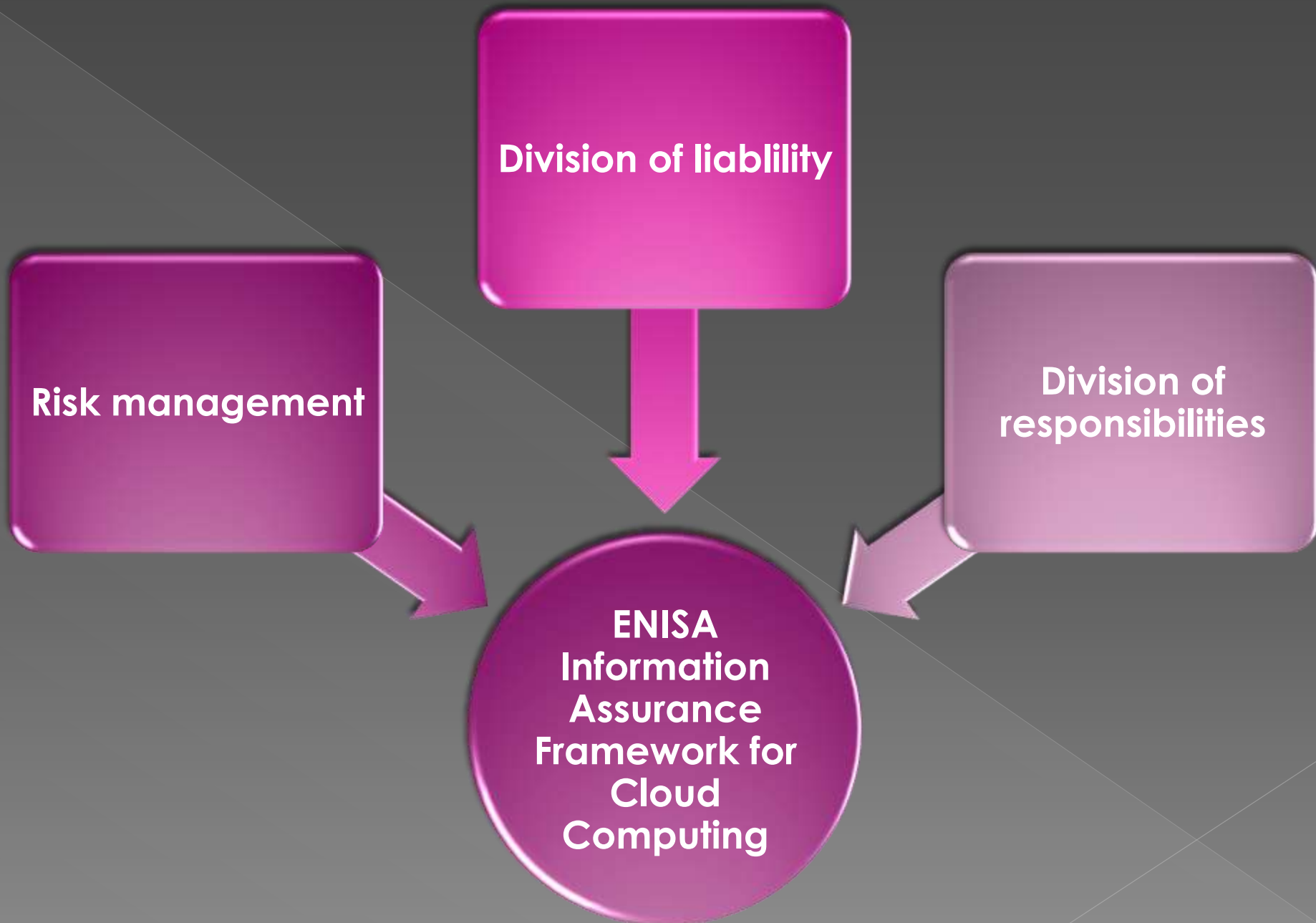
Find the Gaps!

Security Control Model



Compliance Model





set of assurance criteria designed to provide a minimum baseline (organisations may have additional specific requirements) :

1 assess the risk of adopting cloud services by comparing the risks of maintaining a 'classical' organization and architecture with risks to migrate in a cloud computing environment

2 compare different Cloud Provider offers

ENISA's Information Assurance Framework

3 obtain assurance from the selected cloud providers. The preparation of effective security questionnaires for third party service providers is a significant resource drain for cloud customers and one which is difficult to achieve without expertise in cloud-specific architectures.

4 reduce the assurance burden on cloud providers. A very important risk specific to cloud infrastructures is introduced by the requirement for NIS assurance. Many cloud providers find that a large number of customers request audits of their infrastructure and policies. This can create a critically high burden on security personnel and it also increases the number of people with access to the infrastructure, which significantly increases the risk of attack due to misuse of security-critical information, theft of critical or sensitive data etc. Cloud providers will need to deal with this by establishing clear framework for handling such requests.

Policy and organizational

- R.1 Lock-in
- R.2 Loss of governance
- R.3 Compliance challenges
- R.4 Loss of business reputation due to co-tenant activities
- R.5 Cloud service termination or failure
- R.6 Cloud provider acquisition
- R.7 Supply chain failure

Technical

- R.8 Resource exhaustion (under or over provisioning)
- R.9 Isolation failure
- R.10 Cloud provider malicious insider - abuse of high privilege roles
- R.11 Management interface compromise (manipulation, availability of infrastructure)
- R.12 Intercepting data in transit
- R.13 Data leakage on up/download, intra-cloud
- R.14 Insecure or ineffective deletion of data
- R.15 Distributed denial of service (DDoS)
- R.16 Economic denial of service (EDOS)
- R.17 Loss of encryption keys
- R.18 Undertaking malicious probes or scans
- R.19 Compromise service engine
- R.20 Conflicts between customer hardening procedures and cloud

Legal

- R.21 Subpoena and e-discovery
- R.22 Risk from changes of jurisdiction
- R.23 Data protection risks
- R.24 Licensing risks

Cloud security risks (ENISA)

Not Cloud specific

- R.25 Network breaks
- R.26 Network management (ie, network congestion / mis-connection / non-optimal use)
- R.27 Modifying network traffic
- R.28 Privilege escalation
- R.29 Social engineering attacks (ie, impersonation)
- R.30 Loss or compromise of operational logs
- R.31 Loss or compromise of security logs (manipulation of forensic investigation)
- R.32 Backups lost, stolen
- R.33 Unauthorized access to premises (including physical access to machines and other facilities)
- R.34 Theft of computer equipment
- R.35 Natural disasters

What, When, and How to Move to the Cloud

Identify the asset

- Data
- Applications/Functions/Process

Evaluate the asset

- What if the asset became widely public and widely distributed?
- What if an employee of our cloud provider accessed the asset?
- What if the process or function were manipulated by an outsider?
- What if the process or function failed to provide expected results?
- What if the information/data were unexpectedly changed?
- How would we be harmed if the asset were unavailable for a period of time?

Map the asset to potential cloud deployment models

- Public
- Private, internal/on-premises
- Private, external (including dedicated or shared infrastructure)
- Community; taking into account the hosting location, potential service provider, and identification of other community members
- Hybrid. To effectively evaluate a potential hybrid deployment, you must have in mind at least a rough architecture of where components, functions, and data will reside.

Evaluate potential cloud service models and providers

- focus on the degree of control you have to implement risk mitigations in the different SPI tiers. If you already have specific requirements (e.g., for handling of regulated data) include them in the evaluation.

Sketch the potential data flow

- map out the data flow between organization, the cloud service, and any customers/other nodes. This is to insure that as you make final decisions, you'll be able to identify risk exposure points.

Risk Assessment

- Risk level estimated on the basis of likelihood of an incident scenario, mapped against the estimated negative impact.
- The likelihood of an incident scenario is given by a threat exploiting vulnerability with a given likelihood.
- The estimate of likelihood of each incident scenario and the business impact depends heavily on the cloud model or architecture under consideration

RISK ASSESSMENT (ENISA)

	Likelihood of incident scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

- Risk level as a function of the business impact and the likelihood of the incident scenario.
- The resulting risk is measured on a scale of 0 to 8 that can be evaluated against risk acceptance criteria.
- This risk scale could also be mapped to a simple overall risk rating:
 - Low : 0-2
 - Medium : 3-5
 - High : 6-8

[estimation of risk levels based on ISO/IEC 27005:2008]

RISK DISTRIBUTION (ENISA)

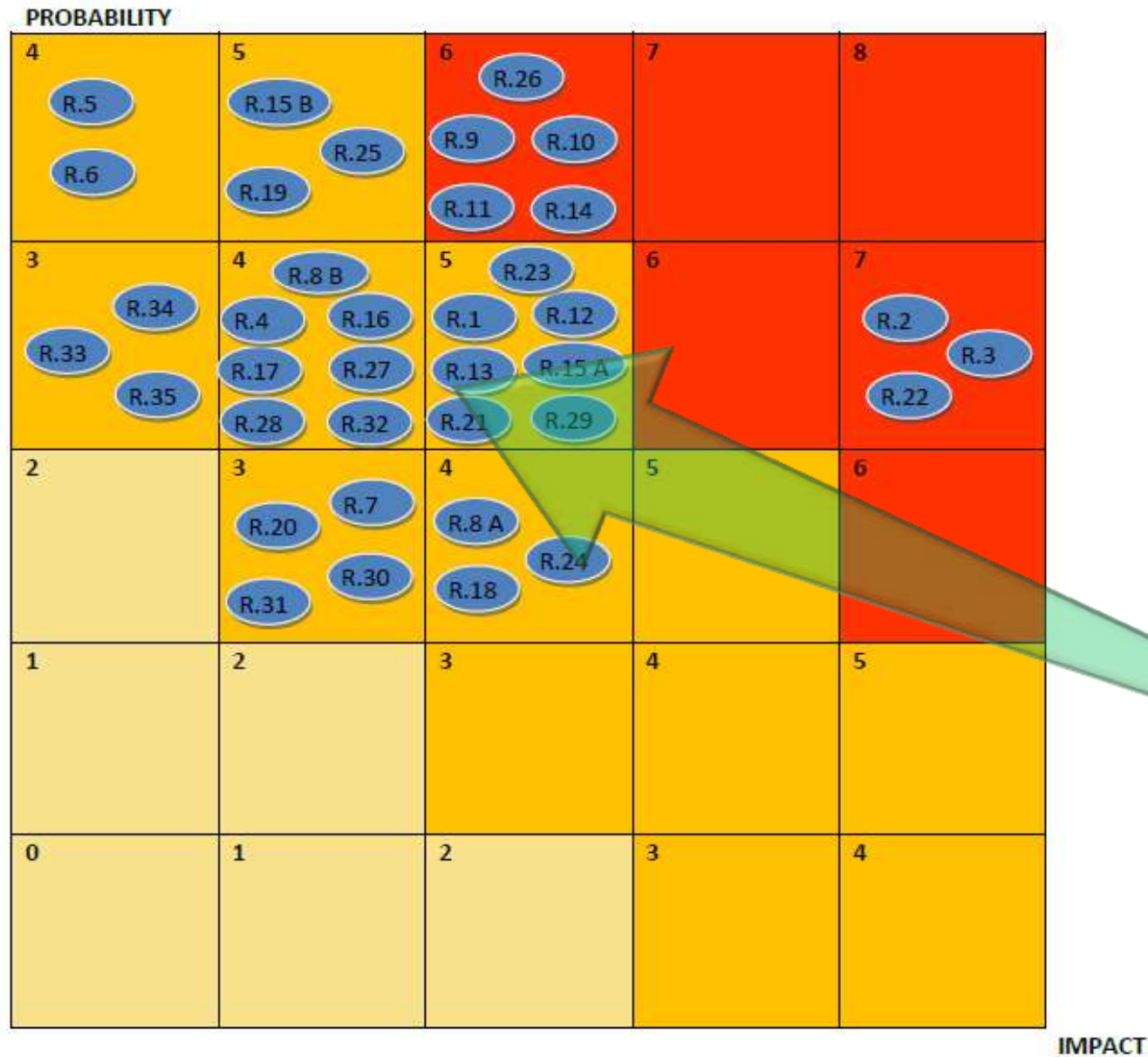


FIGURE 2: RISK DISTRIBUTION

Medium to high

Risk distribution mapping cloud vulnerabilities vs impact likelihood

Top Threats to Cloud Computing (CSA)

- ◉ Abuse and Nefarious Use of Cloud Computing
- ◉ Insecure Application Programming Interfaces
- ◉ Malicious Insiders
- ◉ Shared Technology Vulnerabilities
- ◉ Data Loss/Leakage
- ◉ Account, Service & Traffic Hijacking
- ◉ Unknown Risk Profile

Areas Of Critical Focus (CSA)

Governance Domains

- Governance and Enterprise Risk Management
- Legal and Electronic Discovery
- Compliance and Audit
- Information Lifecycle Management
- Portability and Interoperability

Operational Domains

- Traditional Security, Business Continuity and Disaster Recovery
- Data Center Operations
- Incident Response, Notification and Remediation
- Application Security
- Encryption and Key Management
- Identity and Access Management
- Virtualization

	Governance Domains							Operational Domains							Service Models		
	Governance and Enterprise Risk Management	Legal and Electronic Discovery	Compliance and Audit	Information Lifecycle Management	Portability and Interoperability	Traditional Security, Business Continuity and Disaster Recovery	Data Center Operations	Incident Response, Notification and Remediation	Application Security	Encryption and Key Management	Identity and Access Management	Virtualization	IaaS	PaaS	SaaS		
Abuse and Nefarious Use of Cloud Computing							✗	✗					✗	✗			
Insecure Application Programming Interfaces									✗				✗	✗	✗		
Malicious Insiders	✗					✗							✗	✗	✗		
Shared Technology Vulnerabilities							✗				✗		✗				
Data Loss/Leakage				✗					✗	✗			✗	✗	✗		
Account, Service & Traffic Hijacking	✗							✗		✗			✗	✗	✗		
Unknown Risk Profile	✗	✗					✗	✗					✗	✗	✗		

Areas Of Critical Focus

Governance Domains

Governance and Enterprise Risk Management

Legal and Electronic Discovery

Compliance and Audit

Information Lifecycle Management

Portability and Interoperability

Operational Domains

Traditional Security, Business Continuity and
Disaster Recovery

Data Center Operations

Incident Response, Notification and Remediation

Application Security

Encryption and Key Management

Identity and Access Management

Virtualization

Cloud Security Risks (ENISA)

POLICY AND ORGANIZATIONAL

TECHNICAL

LEGAL

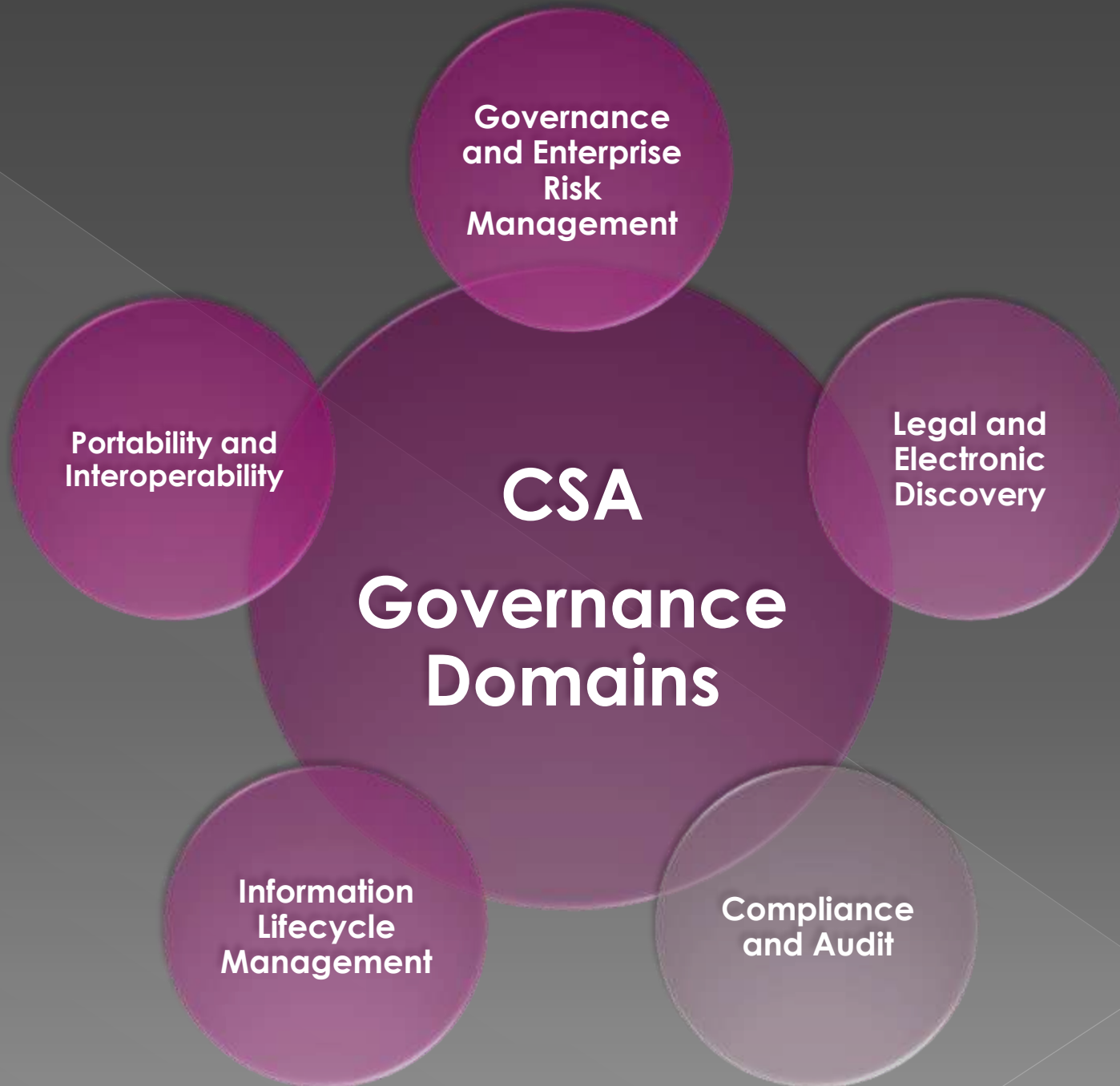
NOT CLOUD SPECIFIC

Architecture & Framework

Governance Domains

Operational Domains

Areas Of Critical Focus (CSA)



Governance and Enterprise Risk Management

- The ability of an organization to govern and measure enterprise risk introduced by Cloud Computing.
- Items:
 - legal precedence for agreement breaches
 - ability of user organizations to adequately assess risk of a cloud provider
 - responsibility to protect sensitive data when both user and provider may be at fault
 - how international boundaries may affect these issues

Legal and Electronic Discovery

- Potential legal issues when using Cloud Computing include:
 - protection requirements for information and computer systems
 - security breach disclosure laws
 - regulatory requirements
 - privacy requirements
 - international laws, etc.

Compliance and Audit

- Maintaining and proving compliance when using Cloud Computing.
- Issues dealing with evaluating how Cloud Computing affects compliance with internal security policies, as well as various compliance requirements (regulatory, legislative, and otherwise).
- This domain includes some direction on proving compliance during an audit.

Information Lifecycle Management

- Managing data that is placed in the cloud.
- Items surrounding the identification and control of data in the cloud, as well as compensating controls which can be used to deal with the loss of physical control when moving data to the cloud.
- Other items, such as who is responsible for data confidentiality, integrity, and availability are mentioned.

Portability and Interoperability

- The ability to move data/services from one provider to another, or bring it entirely back inhouse.
- Issues surrounding interoperability between providers.



Traditional Security, Business Continuity and Disaster Recovery

- How Cloud Computing affects the operational processes and procedures currently use to implement security, business continuity, and disaster recovery.
- The focus is to discuss and examine possible risks of Cloud Computing, in hopes of increasing dialogue and debate on the overwhelming demand for better enterprise risk management models.
- Further, the section touches on helping people to identify where Cloud Computing may assist in diminishing certain security risks, or entails increases in other areas.

Traditional Security, Business Continuity and Disaster Recovery

- How Cloud Computing affects the operational processes and procedures currently use to implement security, business continuity, and disaster recovery.
- The focus is to discuss and examine possible risks of Cloud Computing, in hopes of increasing dialogue and debate on the overwhelming demand for better enterprise risk management models.
- Further, the section touches on helping people to identify where Cloud Computing may assist in diminishing certain security risks, or entails increases in other areas.

Data Center Operations

- How to evaluate a provider's data center architecture and operations.
- Focus on how to identify common data center characteristics that could be detrimental to on-going services, as well as characteristics that are fundamental to long-term stability.

Incident Response, Notification and Remediation

- Proper and adequate incident detection, response, notification, and remediation.
- This attempts to address items that should be in place at both provider and user levels to enable proper incident handling and forensics.
- This domain is focused on the complexities the cloud brings to current incident handling program.

Application Security

- Securing application software that is running on, or being developed in, the cloud.
- Includes specific security issues:
 - whether it's appropriate to migrate or design an application to run in the cloud, and if so,
 - what type of cloud platform is most appropriate (SaaS, PaaS, or IaaS).

Encryption and Key Management

- Identifying proper encryption usage and scalable key management.
- This section is not prescriptive, but is more informational is discussing *why they are needed and identifying* issues that arise in use, both for protecting access to resources as well as for protecting data.

Identity and Access Management

- Managing identities and leveraging directory services to provide access control.
- The focus is on issues encountered when extending an organization's identity into the cloud.
- Assessing an organization's readiness to conduct cloud-based Identity and Access Management (IAM).

Virtualization

- The use of virtualization technology in Cloud Computing.
- Includes security issues surrounding system/hardware virtualization:
 - risks associated with multi-tenancy
 - VM isolation
 - VM co-residence
 - hypervisor vulnerabilities, etc.

Bibliography

- ◉ **Cloud Computing Benefits, risks and recommendations for information security ENISA**
[http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport downloaded January, 2010]
- ◉ **Cloud Computing Information Assurance Framework**
[http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework/at_download/fullReport]
- ◉ **The NIST Definition of Cloud Computing** Authors: Peter Mell and Tim Grance Version 15, 10-7-09 [<http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc> downloaded January, 2010]
- ◉ **Effectively and Securely Using the Cloud Computing Paradigm**
Peter Mell, Tim Grance NIST, Information Technology Laboratory 10-7-2009 [<http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-computing-v26.ppt> downloaded January, 2010]
- ◉ **Cloud Security Alliance: Top Threats to Cloud Computing V1.0**
[<http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf> downloaded March, 2010]
- ◉ **Cloud Security Alliance: Security Guidance for Critical Areas of Focus in Cloud Computing V2.1**
[<http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf> downloaded March, 2010]