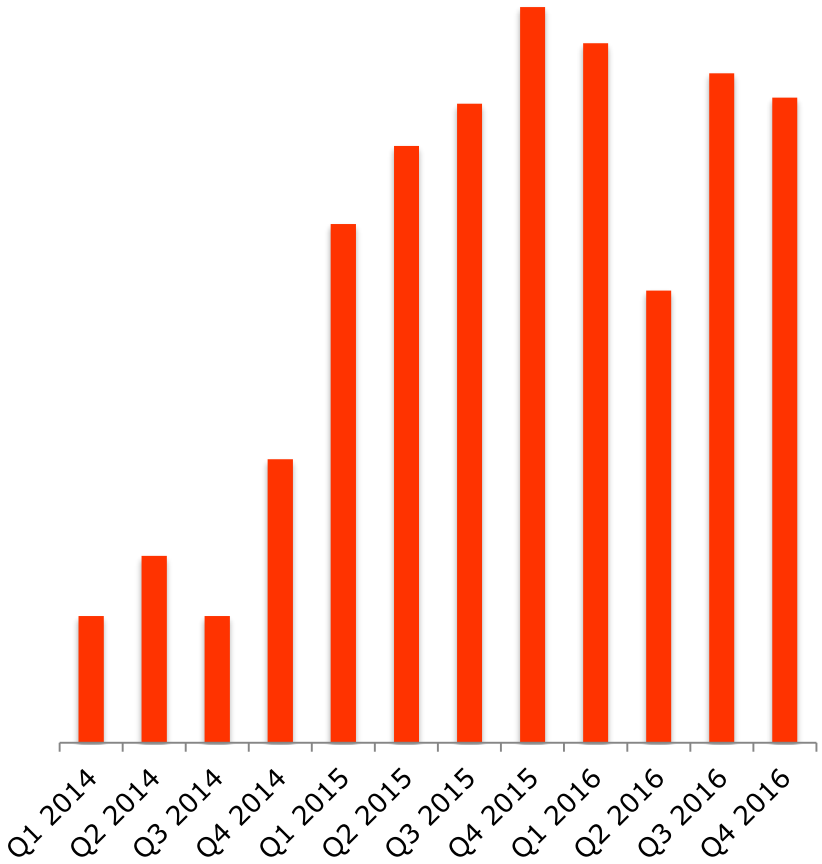
IT Security and Cloud computing

Marnix Dekker,
IT Security directorate, European Commission

Structure of this talk

- **Cloud security benefits and risks**
- Cloud I tender
- Cloud security working group

Background: Heating up



- Sharp increase of events which require handling (analysis, and if needed intervention).
- Why?
  - Better reporting
  - Better detection*
  - Better attackers**
- Increase of sophisticated attacks
- Increased number of attacks

**) still limited in scope*

***) exploiting vulnerabilities within days, malware-less attacks, lateral movement*

ENISA guidance for cloud customers

- 2009 Cloud security risk assessment
- 2015 Cloud security guide for SMEs
  - Updates the 2009 paper
- Online cloud security tool for SMEs
  - For assess risks, opportunities, and asking questions
- Cloud certification tools (list and meta-framework)
  - Explaining the different certification schemes
  - Mapping gov requirements to certification schemes
- ENISA: "Security is a driver for cloud".
  - All cloud providers?

IT Security benefits of cloud services

Security opportunities to be considered when "going cloud":

1. Geographic spread
2. Elasticity
3. Standard formats and interfaces
4. Physical security
5. Incident response around the clock
6. Software development
7. Patching and updating
8. Backups
9. Server-side storage (not on the endpoint)
10. Security as a service and add-ons
11. Certification and compliance

IT security risks of cloud services

IT security risks to be considered when "going cloud".

1. Software security vulnerabilities
2. Network attacks
3. Social engineering attacks
4. Management GUI and API compromise
5. Device theft/loss
6. Physical hazards
7. Overloads
8. Unexpected costs
9. Vendor lock-in
10. Administrative or legal outages
11. Foreign jurisdiction issues

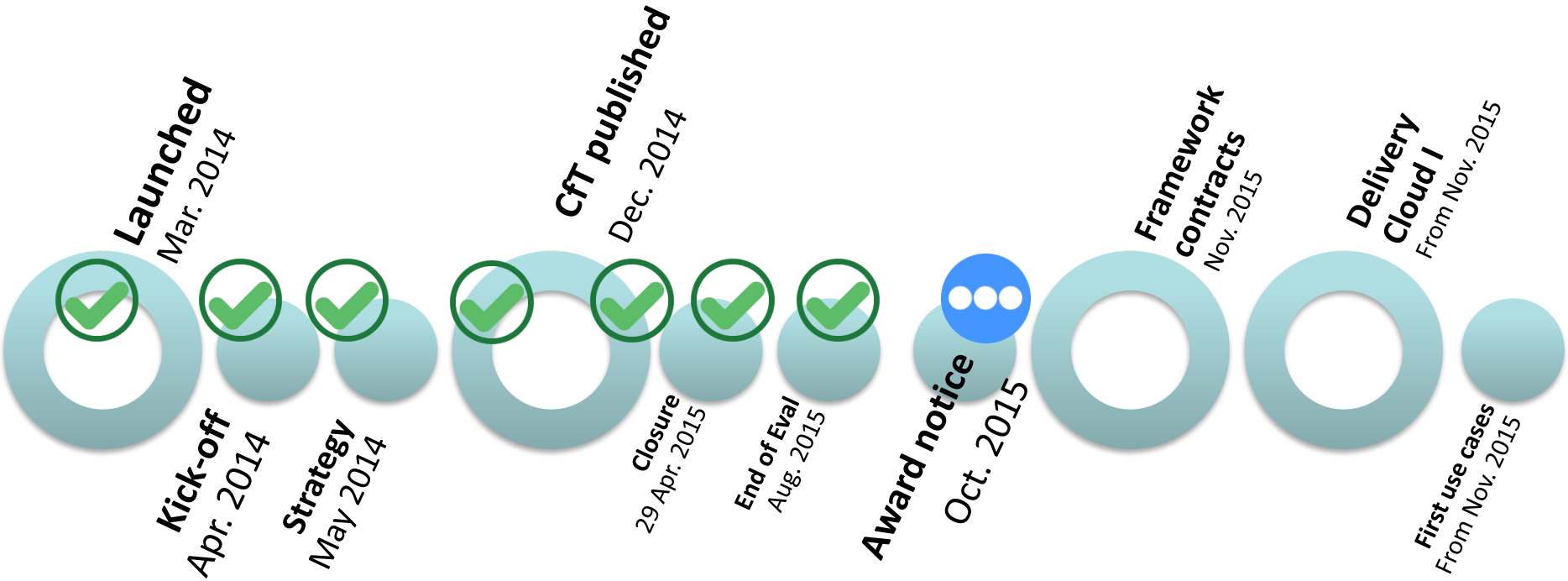
Structure of this talk

- Cloud security benefits and risks
- **Cloud I tender**
- Cloud security working group

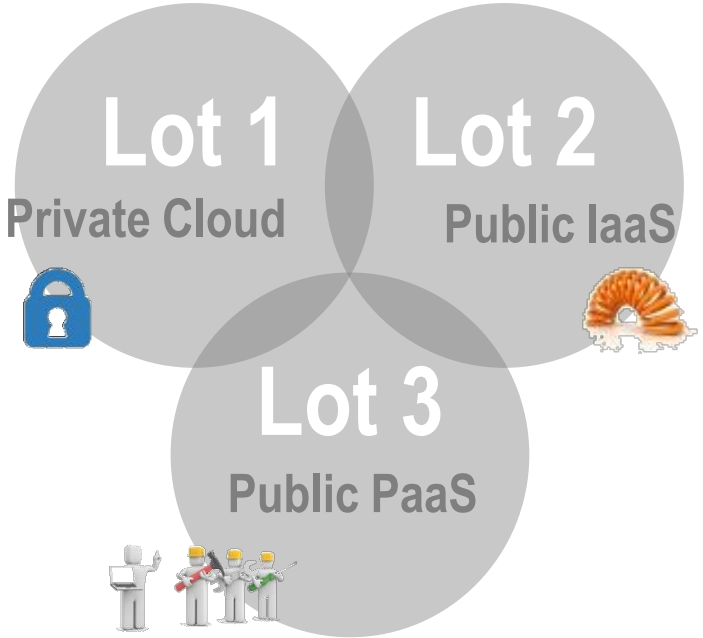
Walking the talk

- Commission promotes cloud adoption
- Asked ENISA to develop cloud procurement tools
  - Working with cloud providers
  - Working with existing cloud certification schemes
- Commission launches a cloud tender
  - Private IaaS, Public IaaS, public PaaS
  - 2500 VMs and 2500 TBs
  - 4 years
  - All EU institutions
  - Using the ENISA tools

EC as a cloud customer: Cloud I



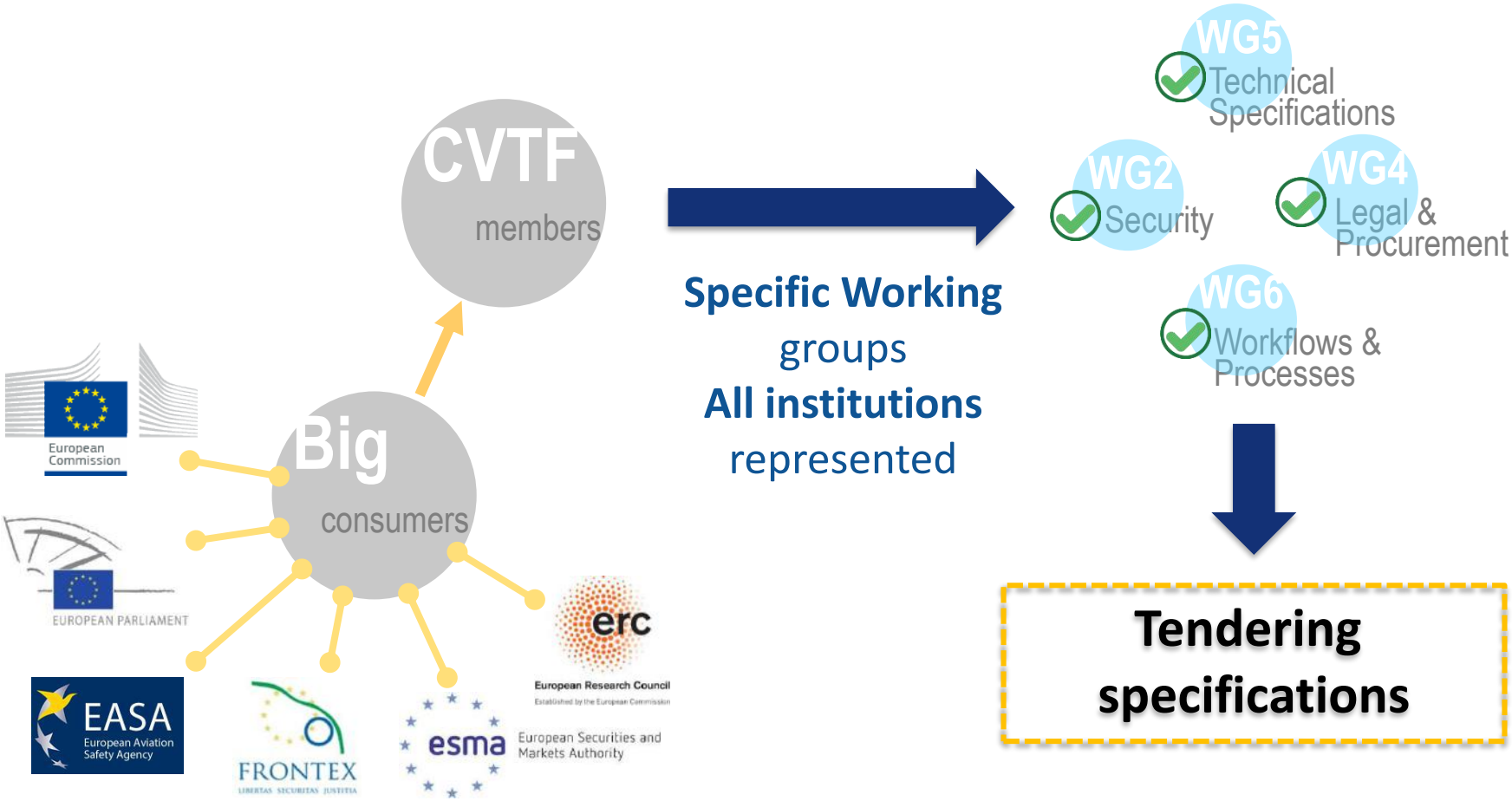
Services in Cloud I tender



Duration: 2 + 1 + 1 years

- Experimental approach
- Best in class **Virtualized** services and **Automation**

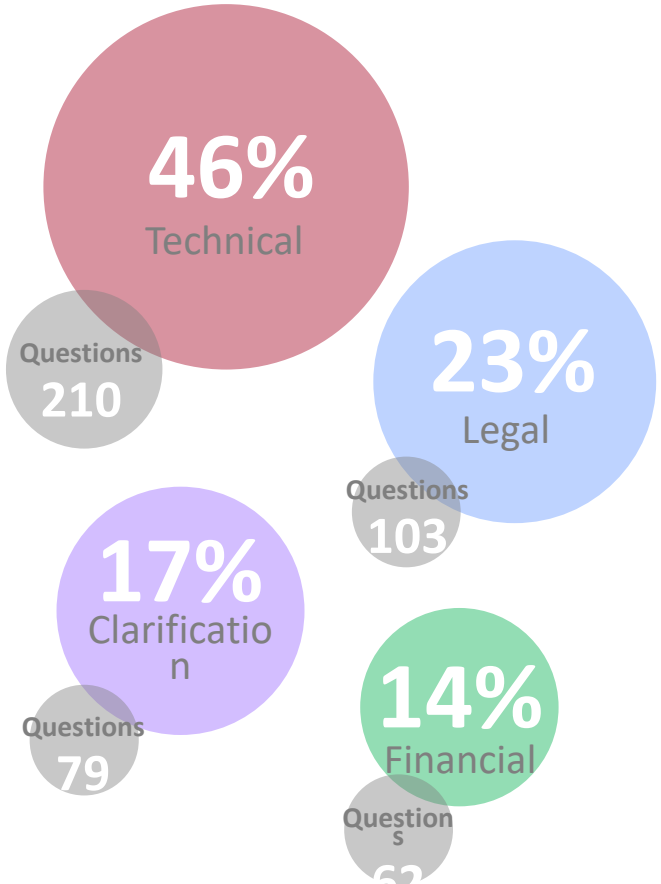
Cloud tender is a joint project



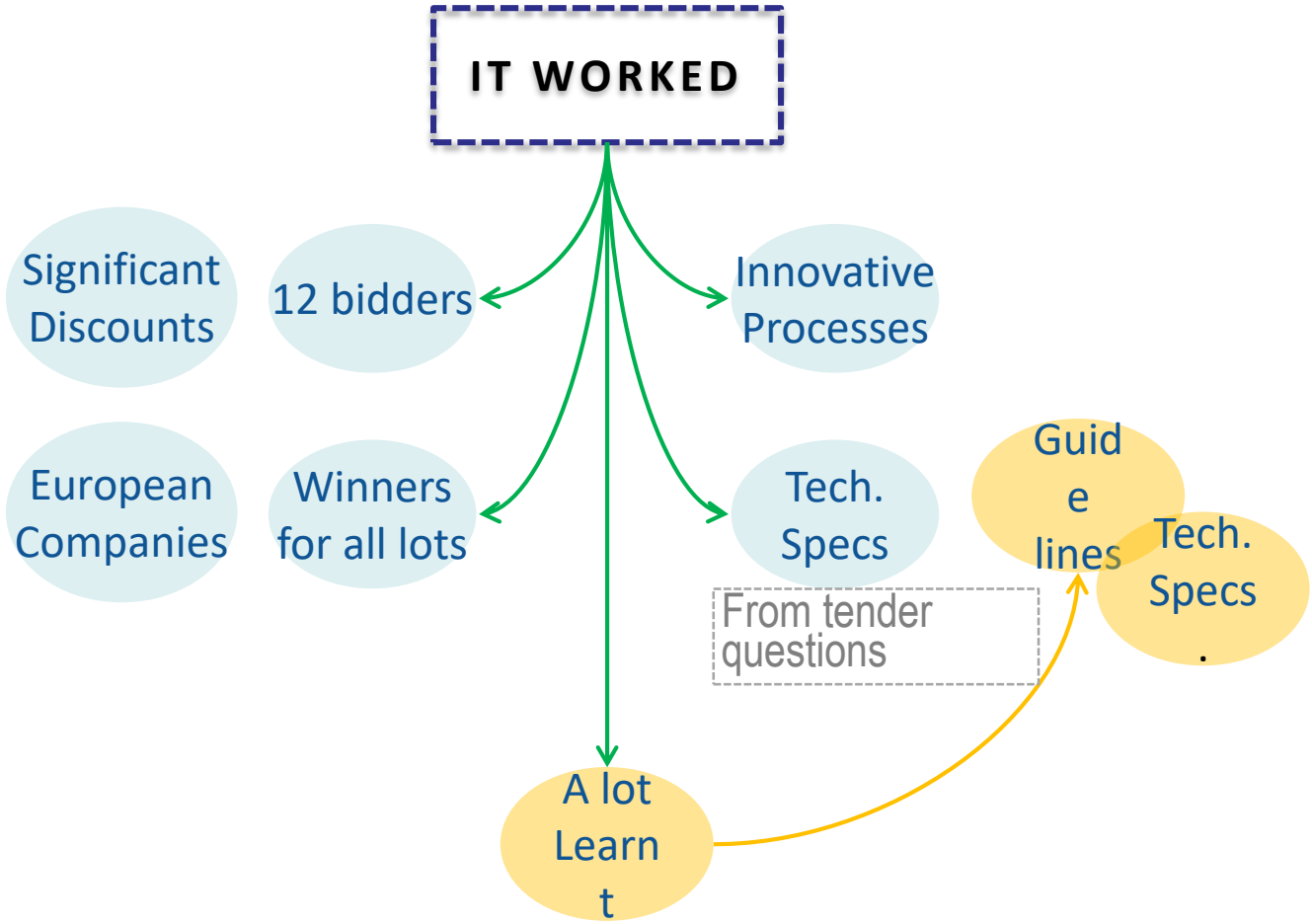
Lots of questions about the tender

Potential Tenderers

454 Questions from tenderers



Lessons learned from Cloud I



Structure of this talk

- Cloud security benefits and risks
- Cloud I tender
- **Cloud security working group**

Cloud security working group

- Started by DIGIT as a customer group for Cloud I tender
- Inter-institutional (all EU-I), CII subgroup
- Includes DPO, DIGIT DPC, HR DS (information security)
- Scope: All cloud use, and all institutions.
- Focus: Help use Cloud I. Prepare for broader cloud use.

IT security responsibilities in cloud

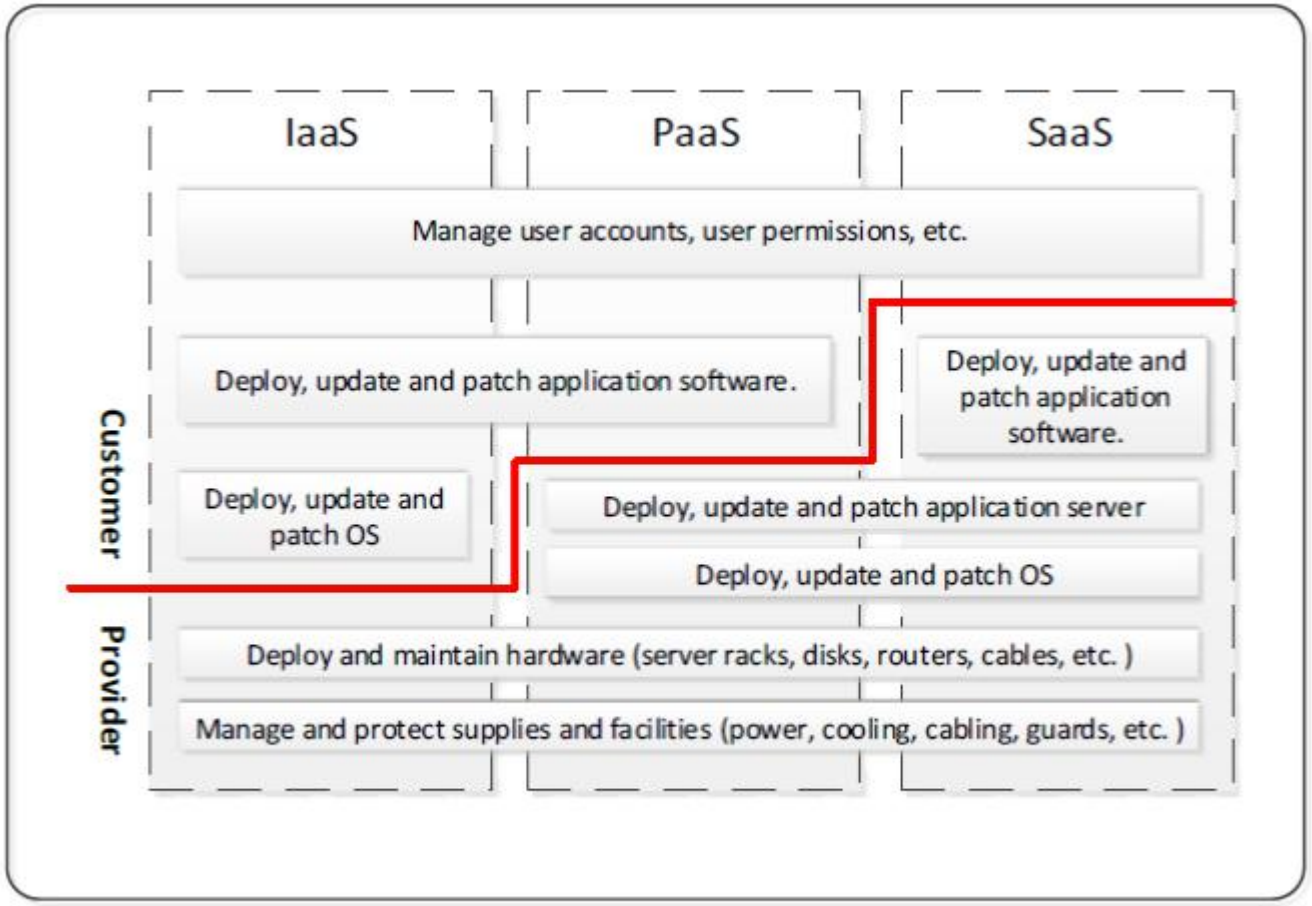


Figure 2: Outsourcing of tasks is different for different types of services

Cloud security questions

- Question is not: Is the provider compliant?
- Real question is: What remains for the customer to do, to be compliant.
- Question is not: Are the security processes of the provider OK?
- Real question is: How to integrate internal security processes with those of the provider

Commission IT security policy

EC Decision 3602

- General roles and responsibilities in the Commission

3602 Implementing rules

- Based on ISO 27001
- 34 security policy objectives
- 85 controls

Several detailed security standards

- Many additional requirements and recommendations
- Many requirements are too internal/specific

Position paper from HR DS on cloud computing

- Can use for PUBLIC, LIMITED BASIC
- If compliant with policy…

Cloud security requirements used

Cloud security requirements used in the tender

- Developed in collaboration with industry
- Based on requirements from different EU governments
- Mapped to existing cloud certification schemes
- ENISA tool developed with EC and industry (CSIG)
- Levels of assurance
  - EAL 0: no assurance
  - EAL1: contractual documents
  - **EAL2: self-assessment**
  - EAL3: internal audit report
  - EAL4: external audit report
  - EAL5: continuous monitoring certification

https://resilience.enisa.europa.eu/cloud-computing-

Cloud I tender security requirements

- 27 security objectives
  - ENISA cloud framework (CCSM)
  - Neutral/mapped to existing certifications or standards
  - **EAL2: self-assessment -> everyone EAL4**
- Additional technical security requirements
  - 14 Eliminatory security requirements
  - 30 Supplementary requirements (encryption etc)
    - 31st requirement is a self-assessment against industry standards (2009 ENISA paper)
- And other security-relevant requirements
  - Right-to-audit, storage, logs, APIs

How to Cloud I in the Commission?

- Many security requirements have been checked
- Tenderers have shown adequate security to be offering cloud services to EU-I

- Questions system owners have:
  - How to use cloud and be compliant with policy?
  - Difficult to answer for the general case
  - Easier: Inform system owners about what security measures are in place.
  - Easier: Help system owners use this information

Staged approach

Step 1: Questionnaire for providers

- Providers self-declare which security measures are in place
- **114 controls** from ISO 27001/2:2013, international standard
- Store completed questionnaires on the Cloud I wiki
- Aligned with Commission policy (implementing rules)
- Useful for other EU-I who have a policy based on ISO27001/2

Step 2: Assess risks for one use case

- Two-tier web application running on IaaS/PaaS
- Simple checklist/decision tree for system owners
- List of non-compliance issues to be approved by senior management

Step 1: Questionnaire

ISO/IEC 27001:2013 Annex A controls			Implementation by provider	Assets covered	Standard, optional, extra cost	Implementation by customers
Clause	**Sec**	**Control Objective/Control**				
5 Security Policies	5.1	Management direction for information security				
	5.1.1	Policies for information				
	5.1.2	Review of the policies for information security				
6 Organisation of information security	6.1	Internal organisation				
	6.1.1	Information security roles and responsibilities				
	6.1.2	Segregation of duties				
	6.1.3	Contact with authorities				
	6.1.4	Contact with special interest groups				
	6.1.5	Information security in project management				
	6.2	Mobile devices and teleworking				
	6.2.1	Mobile device policy				
	6.2.2	Teleworking				

Step 2: Example use case

- 2-tier web application running on IaaS/PaaS
  - OS, web application server (if IaaS), SQL Database
  - Web application code

- Provider implements many controls already
- Checklist for customers
  - Secure software development
  - Procedure for patching OS and app server (if IaaS)
  - App and DB access control for admins and normal users
  - Provide log access to SOC
  - …

Contact us

IT Security Directorate, European Commission
DIGIT S1: Policy, information assurance, security assurance
DIGIT-S1@ec.europa.eu

Marnix Dekker, Dalibor Baskovc, Joel Hubin