European Commission

GovSec and ITSRM²

An attempt to manage risks and compliance at scale,

On premises and in the cloud

Philippe Merle / Daniel Marcenac
European Commission – DIGIT - may 2019

Informatics

The (strange) scene

We are not security specialists

Our colleagues are

We are developers

And cloud broker

We have been forced to learn about security

Before starting that journey...

[redacted] and security plans
are [redacted]
[redacted] to write once a
document [redacted]
[redacted] so [redacted].

DANGER

European Commission Digital Strategy

Security by design

User centric

Digital workplace

Digital solutions

Reusable Solutions Platform

Data Ecosystem

Digital Infrastructure

Cybersecurity

by 2022

A **digitally transformed, user-focused, data driven**, European Commission

European Commission

European Commission Digital Strategy

Security by design

User centric

Cloud

An enabler for this digital transformation

by 2022

A **digitally transformed, user-focused, data driven,** European Commission

European Commission

The European Commission Cloud Strategy

Cloud First

with a

Secure Hybrid Multi-Cloud service offering

THE EUROPEAN COMMISSION CLOUD STRATEGY

EUROPEAN COMMISSION CLOUD STRATEGY

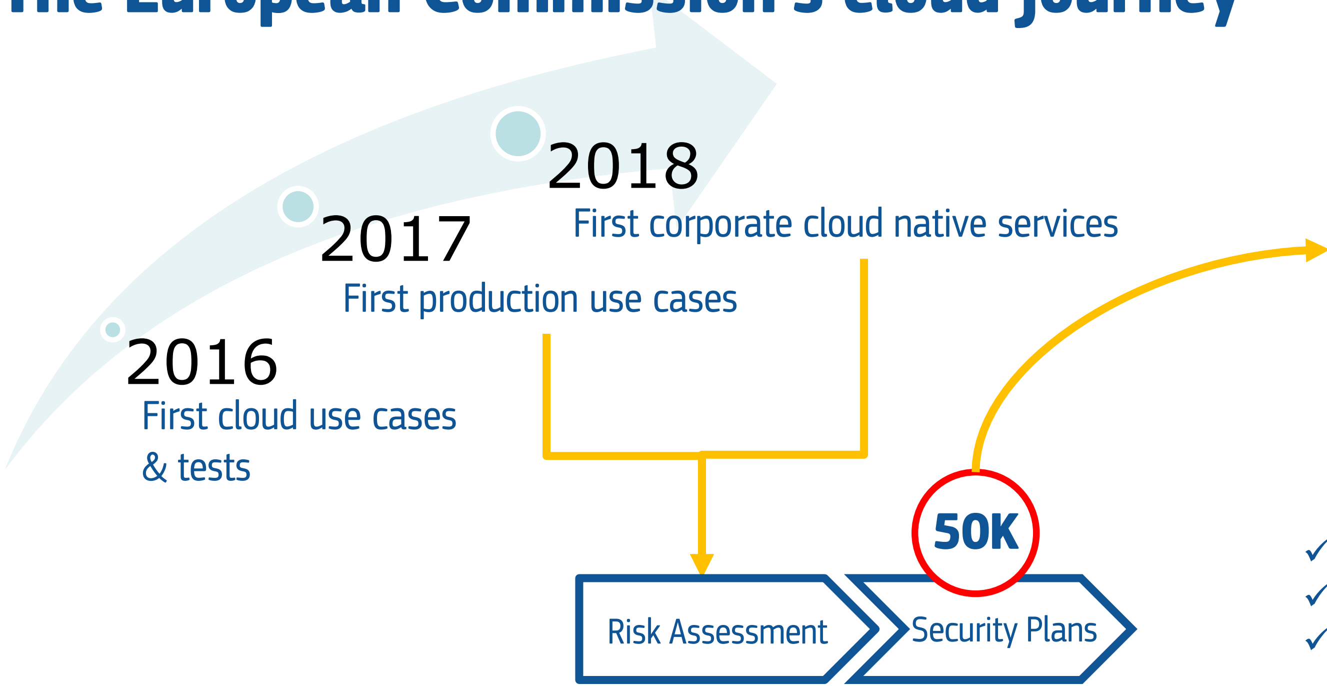
Cloud as an enabler for the European Commission Digital Strategy

16 May 2019

V.1.0.1

16th may 2019
2nd cloud strategy

The European Commission's cloud journey



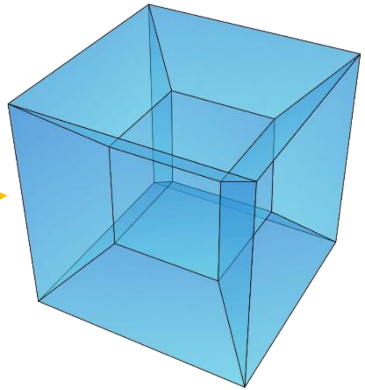
2016
First cloud use cases & tests

2017
First production use cases

2018
First corporate cloud native services

Risk Assessment → Security Plans

50K



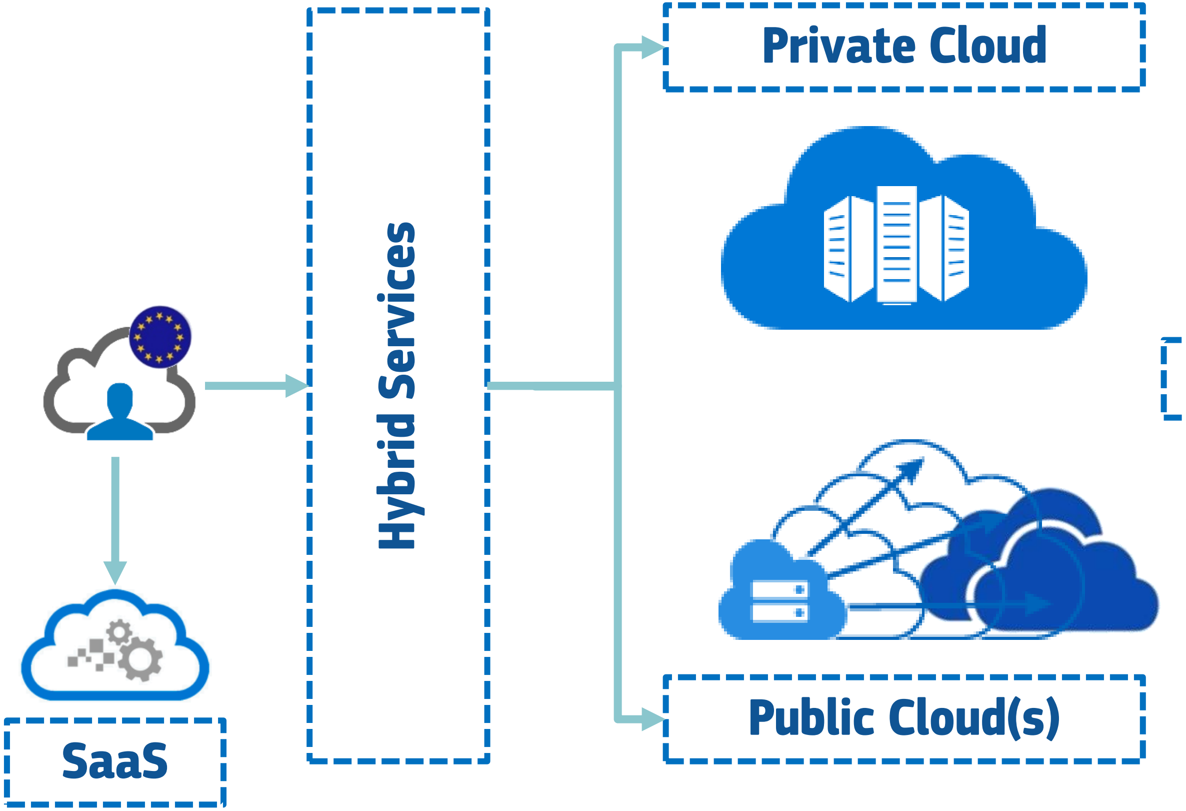
An hypercube

- ✓ Cloud services (many)
- ✓ Several options per service
- ✓ Standard control matrix

And even before… 50K x 1.500 systems = 75M€

We need to scale,
We could be smarter

On top, Hybrid Cloud



SaaS

Hybrid Services

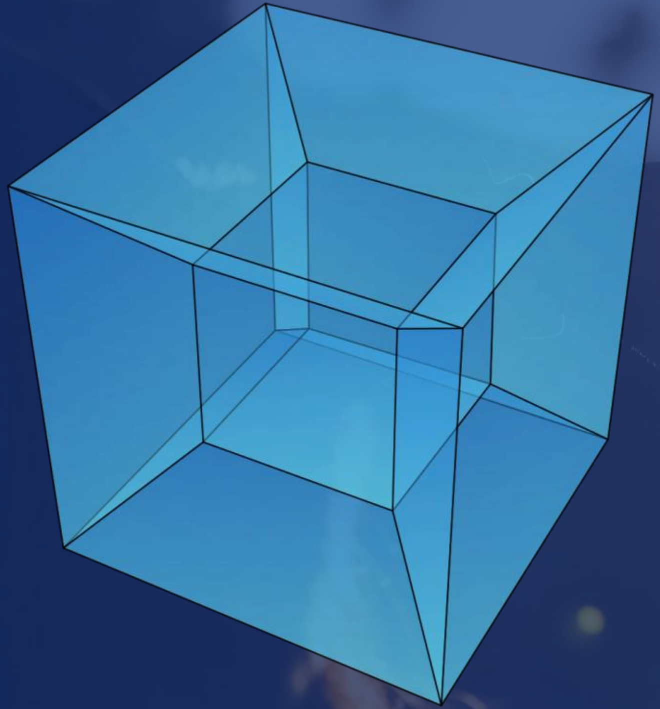
Private Cloud

Public Cloud(s)

- ✓ On **EC premises**
- ✓ Immunities and privileges protection
- ✓ High level of **control**
- ✓ Set of **core optimized services**
  - Self-service
  - For existing services
  - For new core services

Let’s not forget data protection

- ✓ Highly **scalable** and **elastic**
- ✓ Pay per use and on demand
- ✓ Fully automated (infra. as code)
- ✓ Vast variety of services
  - Reusable with reduced overhead
  - Follow market innovations
- ✓ High level of security



Our solution to the hypercube problem

Goal:

An industrial process!

We do not want to invent the art of making risk assessment, we want something practical that scales for our 1.500 information systems

So:

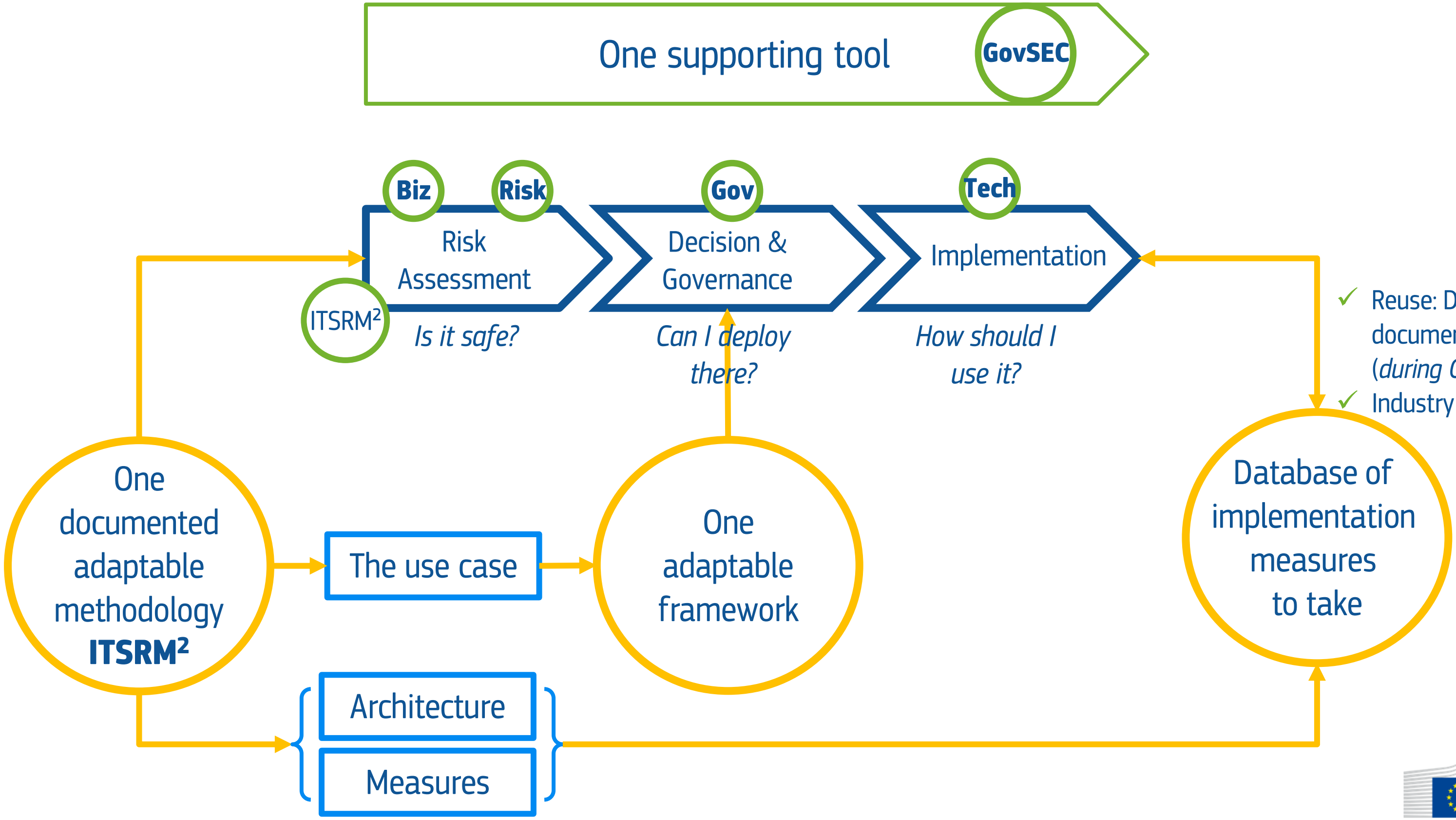
Risks assessment in less than a week

Not giving the feeling to *"go to the dentist"*

-end user quote-

GovSEC – **the concept**

An information system funded by **ISA**, to implement a methodology that proves the shared responsibility model is properly implemented



One supporting tool **GovSEC**

Biz **Risk** Risk Assessment

Gov Decision & Governance

Tech Implementation

ITSRM²

Is it safe?

Can I deploy there?

How should I use it?

One documented adaptable methodology **ITSRM²**

The use case

One adaptable framework

Architecture

Measures

Database of implementation measures to take

- ✓ Reuse: Dozens of services documented (*during Cloud I specific projects)*
- ✓ Industry best practices

Azure Microsoft

amazon web services

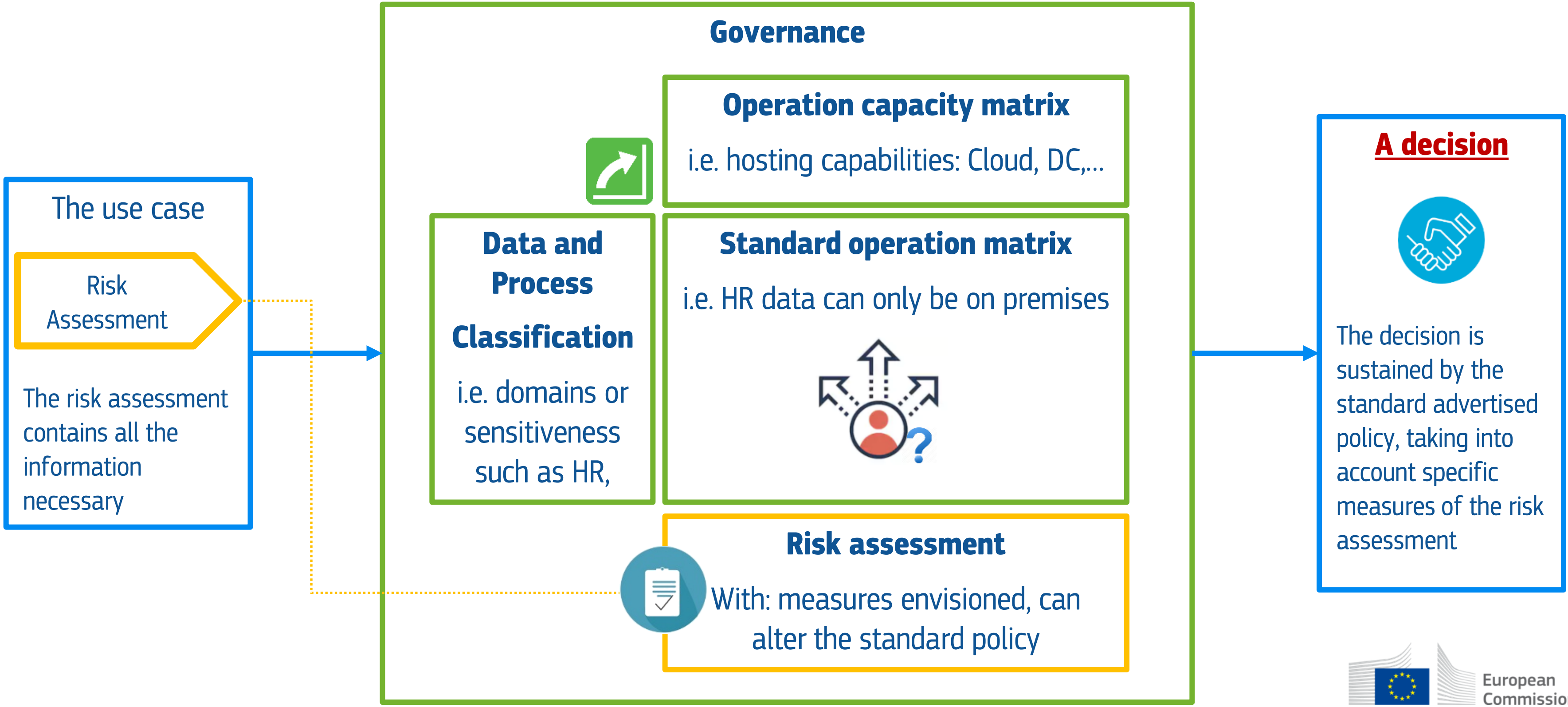
DIGIT Datacentre Services

European Commission

Governance module

Decision & Governance

Gov



The use case

Risk Assessment

The risk assessment contains all the information necessary

Governance

Operation capacity matrix

i.e. hosting capabilities: Cloud, DC,…

Data and Process

Classification

i.e. domains or sensitiveness such as HR,

Standard operation matrix

i.e. HR data can only be on premises

Risk assessment

With: measures envisioned, can alter the standard policy

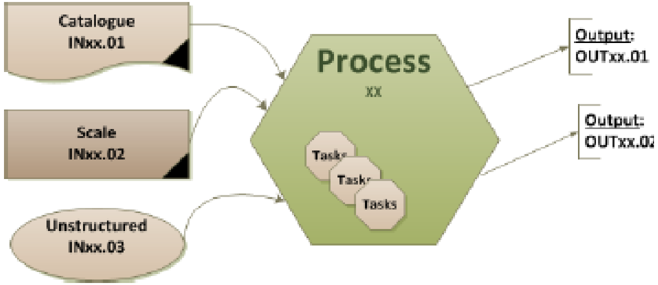
A decision

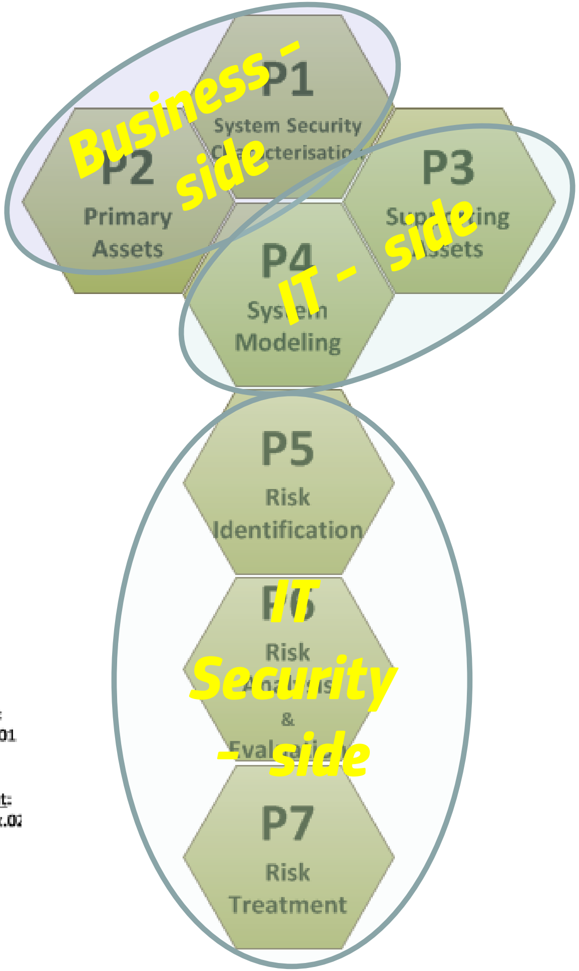
The decision is sustained by the standard advertised policy, taking into account specific measures of the risk assessment

ITSRM²

IT Security Risk Management Methodology

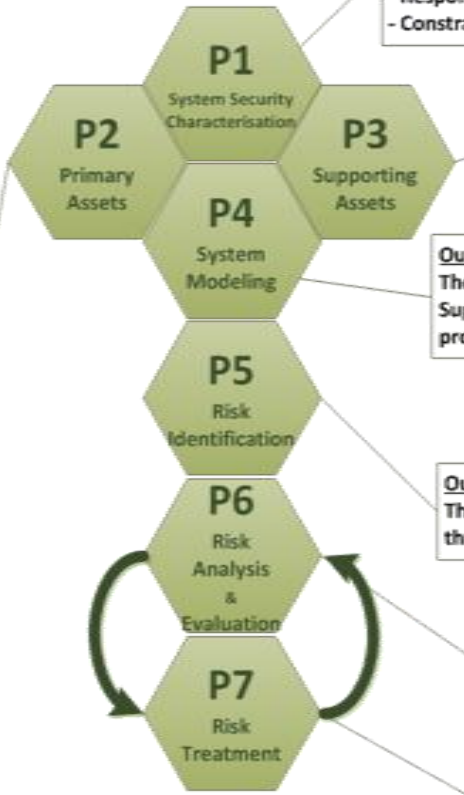
Output of a step
=
Input for next step





- ✓ Supports the Commission Decision 2017/46
- ✓ Complements the effort of the EC for the protection of the information systems
- ✓ Proposes practical choices of implementation of these processes:
  - Formulas
  - Actionable tasks and methods
  - Scales
  - Catalogues

ITSRM^2 Processes



Output:
- Identification and description of the system
- Information about the organisation
- Responsibles and contact points for Security Roles
- Constraints that may condition security

Output:
Inventory of Primary Assets with:
- Description
- Valuation
- Max Interest and Power of potential adversaries

Output:
The inventory of Supporting Assets with description

Output:
The System Model (Primary Assets with the Supporting Assets on which they are processed)

Output:
The register of Risks Identified (scenarios with threat)

Output:
The sorted register of Risks with their Residual Risk Level

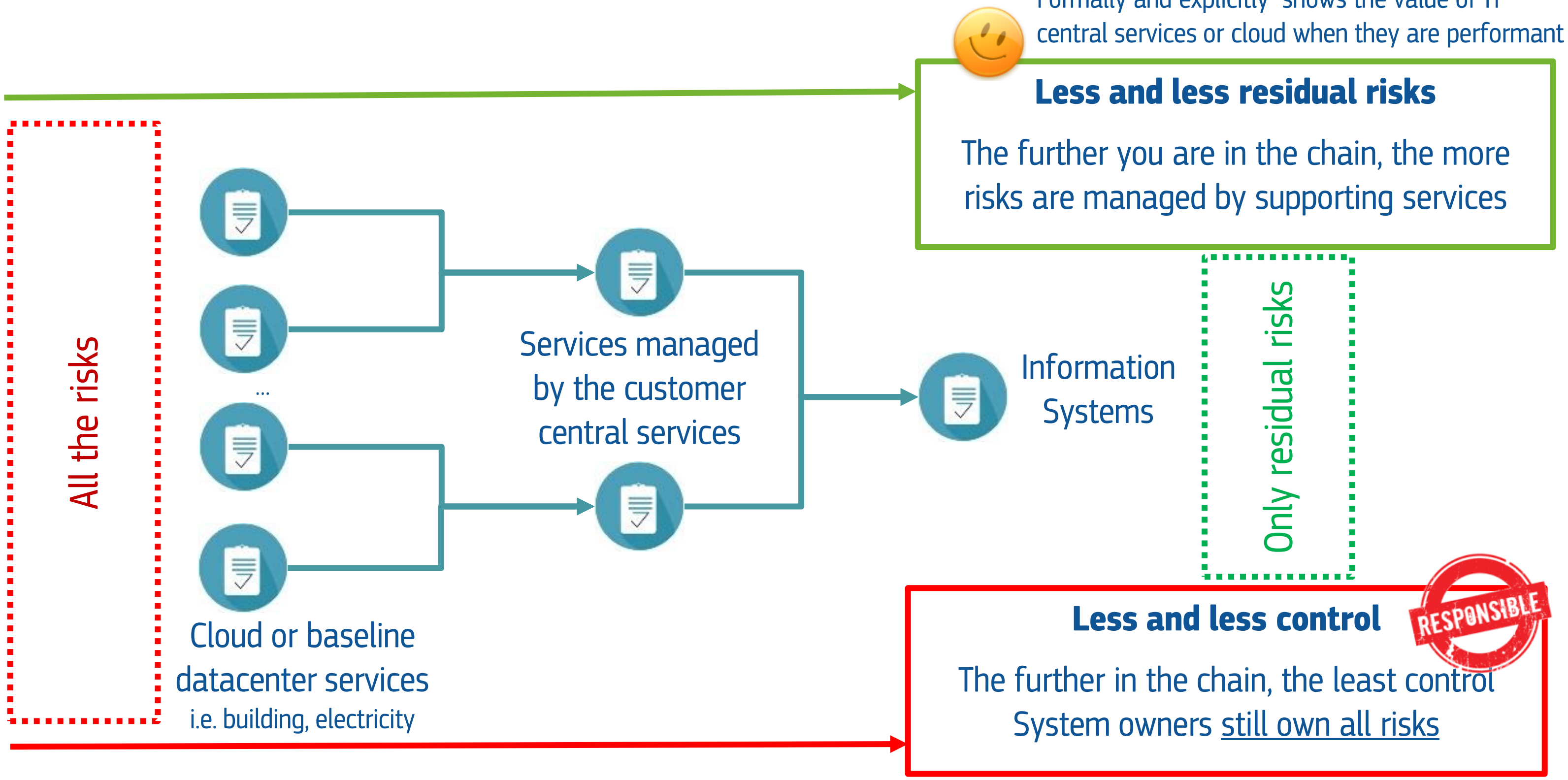
Output:
The list of chosen treatment of risks including mitigation measures

Everybody goes on missions

The trick: **shared responsibility model at scale**

When this becomes Easy

But keep focused



Formally and explicitly shows the value of IT central services or cloud when they are performant

Less and less residual risks

The further you are in the chain, the more risks are managed by supporting services

All the risks

…

Cloud or baseline datacenter services
i.e. building, electricity

Services managed by the customer central services

Information Systems

Only residual risks

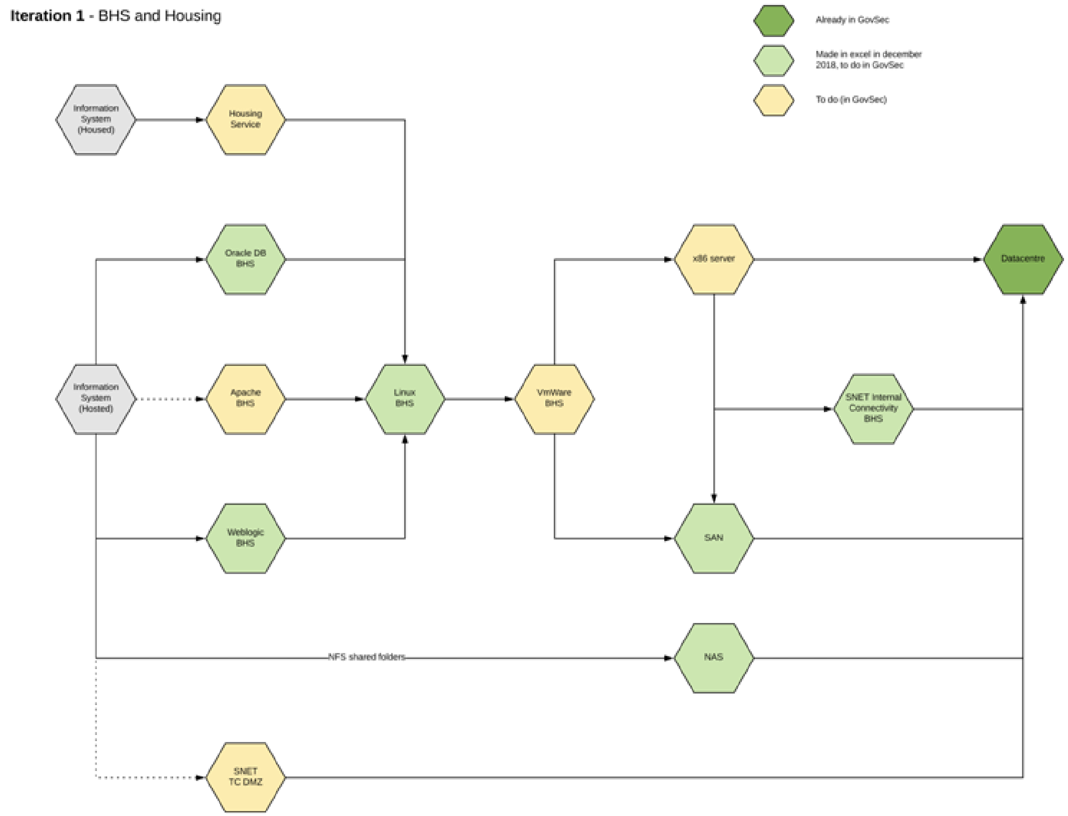
Less and less control

RESPONSIBLE

The further in the chain, the least control
System owners <u>still own all risks</u>

European Commission

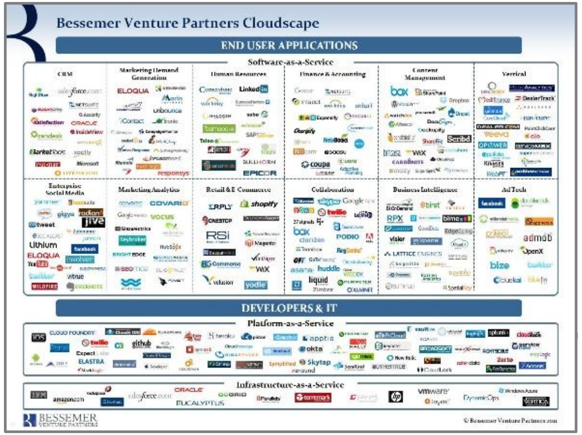
GovSec – Risk Assessments (and Security plans) for a **datacenter**


Iteration 1 - BHS and Housing
Already in GovSec
Made in excel in december 2018, to do in GovSec
To do (in GovSec)
Information System (Housed)
Housing Service
Oracle DB BHS
Information System (Hosted)
Apache BHS
Linux BHS
VmWare BHS
x86 server
Datacentre
SNET Internal Connectivity BHS
Weblogic BHS
SAN
NFS shared folders
NAS
SNET TC DMZ

Preparation the database of RA for IS that run in the datacenter?

GovSec – Risk Assessments (and Security plans) for the **Cloud**

Preparation the database of Risk Assessment for IS that run in the cloud?

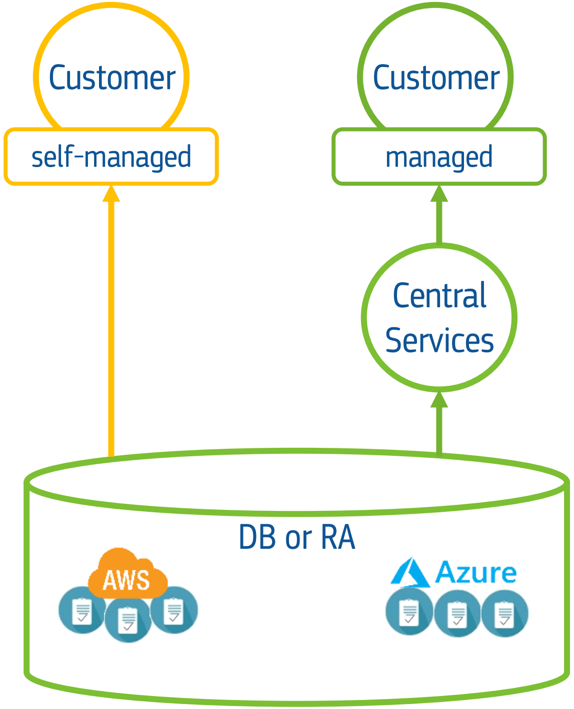


In the Cloud

A simple information system is using easily 15 basic provider services

(logs, authentication, storage, compute, console and API management, etc…)

Each of them need an individual Risk Assessment (lesson of Cloud I)



RA made by providers, list all options i.e. mitigations measures

Idea: mandatory for procurement
Would allow built-in security in tenders

People kind of liked it

✓ Commission datacenter fully modelled (in few weeks)

✓ Cloud providers are willing to play ball (or we do not use them)

✓ Agencies will adopt

Next steps

✓ Implementation of Data Protection Risk Assessment?

✓ Cloud systems being modelled with the same principle as the datacenter service

✓ Publication as open source, for both the methodology and the information system

✓ Awareness, awareness, awareness

European
Commission

Thank you