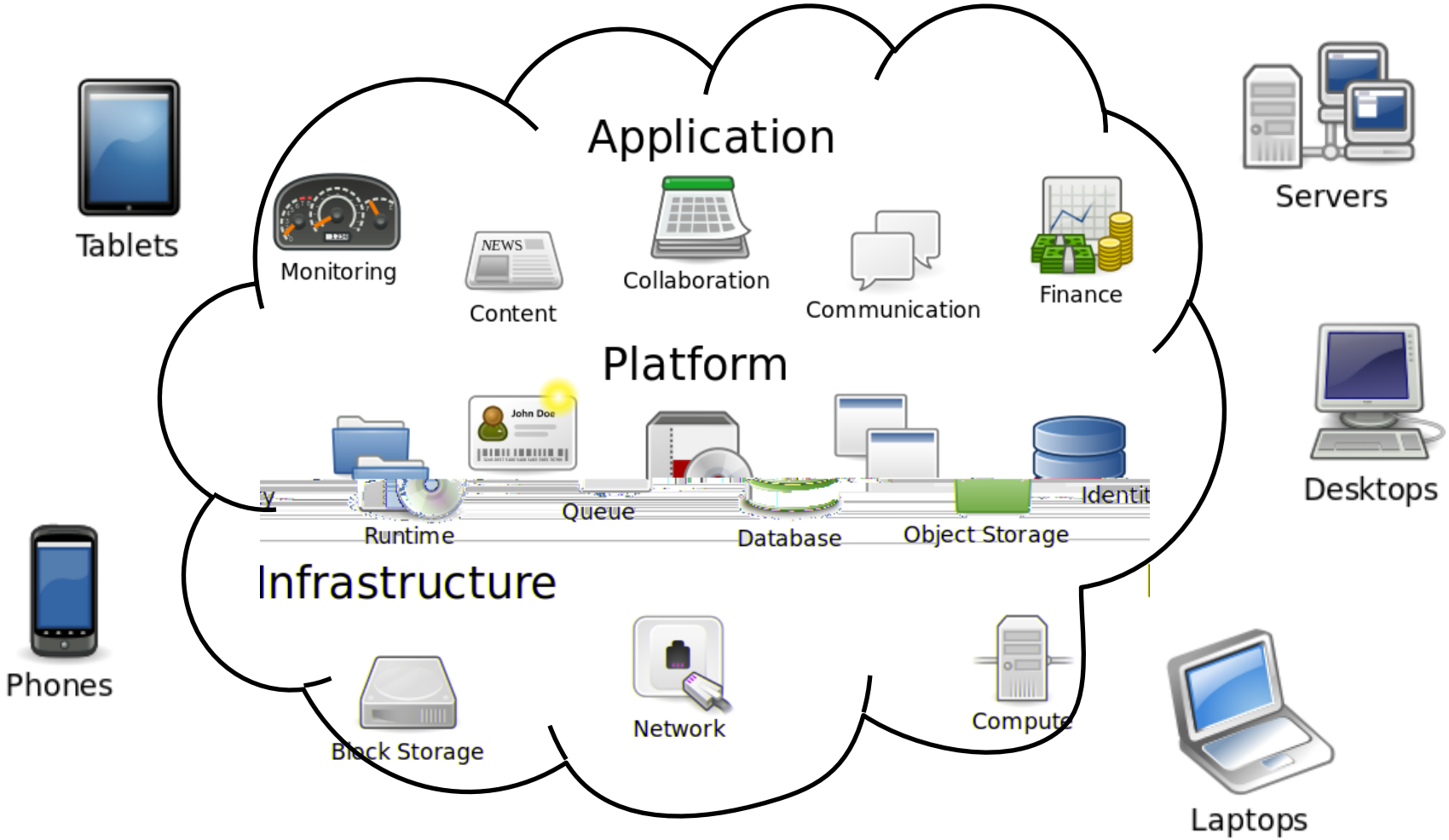

Smals
ICT for society

Overview of the cloud



What about the security of the cloud?

- garanteed by the cloud services
- Problematic for
  - ➢ Especially in our context « social security and eHealth»

Assess the security of a cloud service before using it

During this presentation…

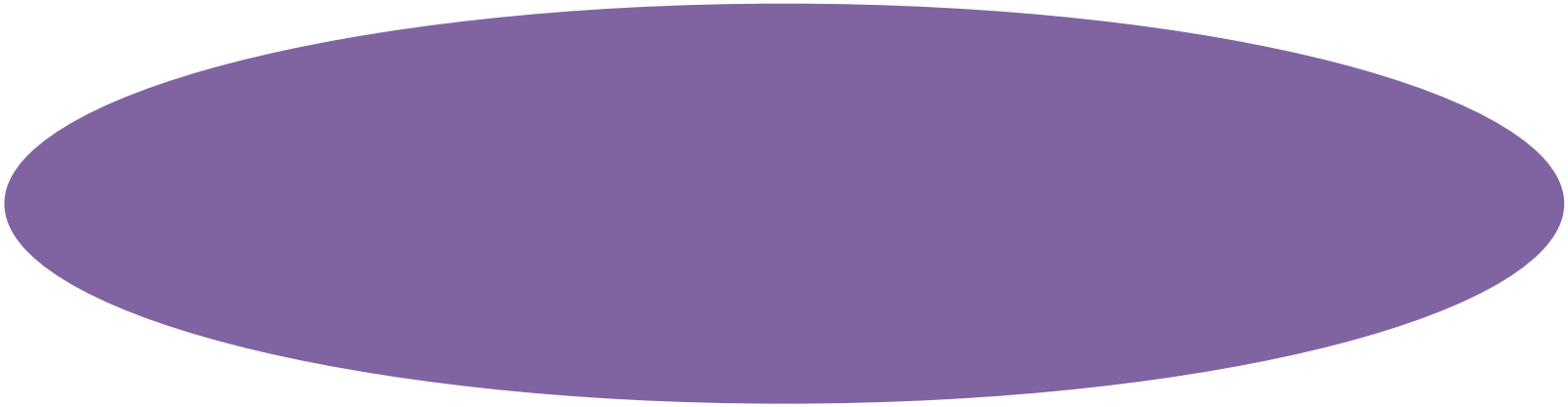
Look through the *Common thread* of cloud security

Agenda

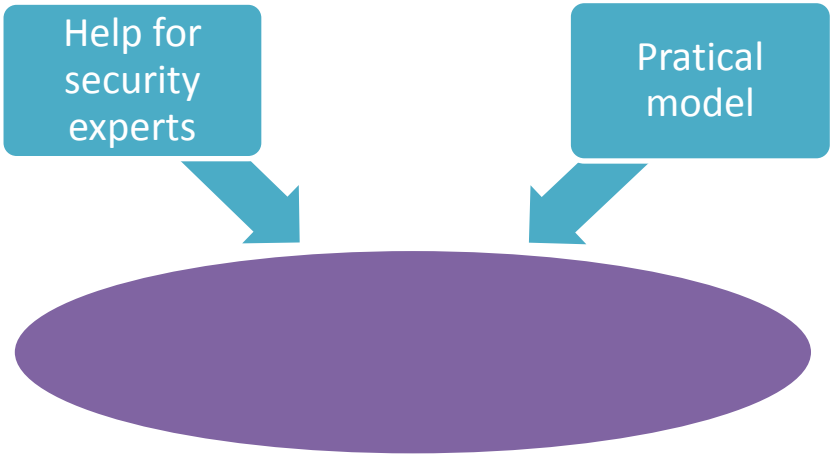
Goal of the model

Help for security experts

Practical model



Goal of the model



Eliminate/filter non fruitful tracks

Select potential candidates

Components of the model

4 major criteria

- Governance
- Identity and Access Management
- IT Security
- Operational Security

Cloud Policy of the Belgian social security

Type of data

2 evaluation forms

- Assess the security level of a cloud service
- Assess the possibility of using a cloud service

Components of the model

4 major criteria

- Governance
- Identity and Access Management
- IT Security
- Operational S

Cloud P
Belgi
ype of data

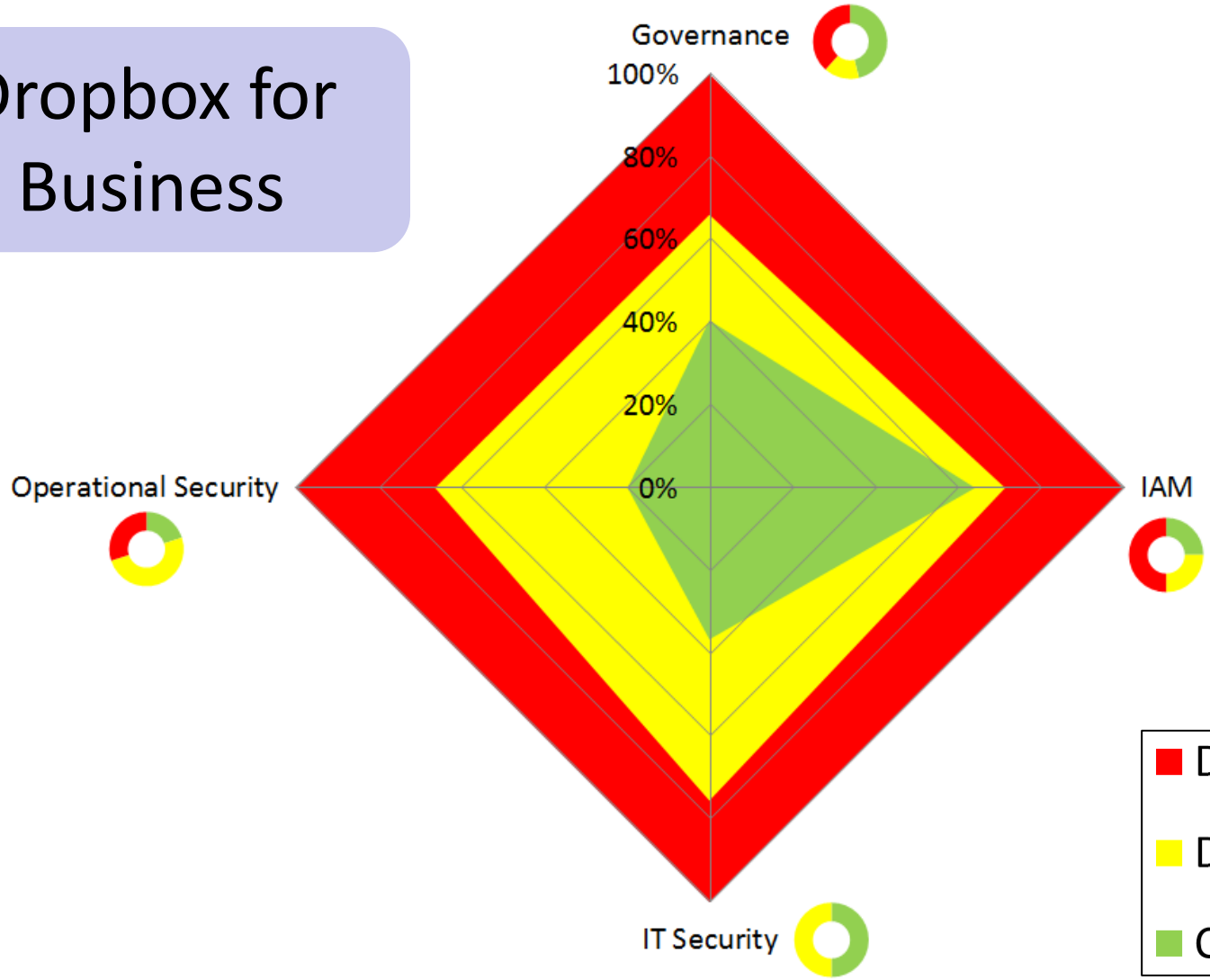
2 evaluation forms

- Assess the security level of a cloud service
- Assess the possibility of using a cloud service

Only a human expert must judge the result

What looks like the model?

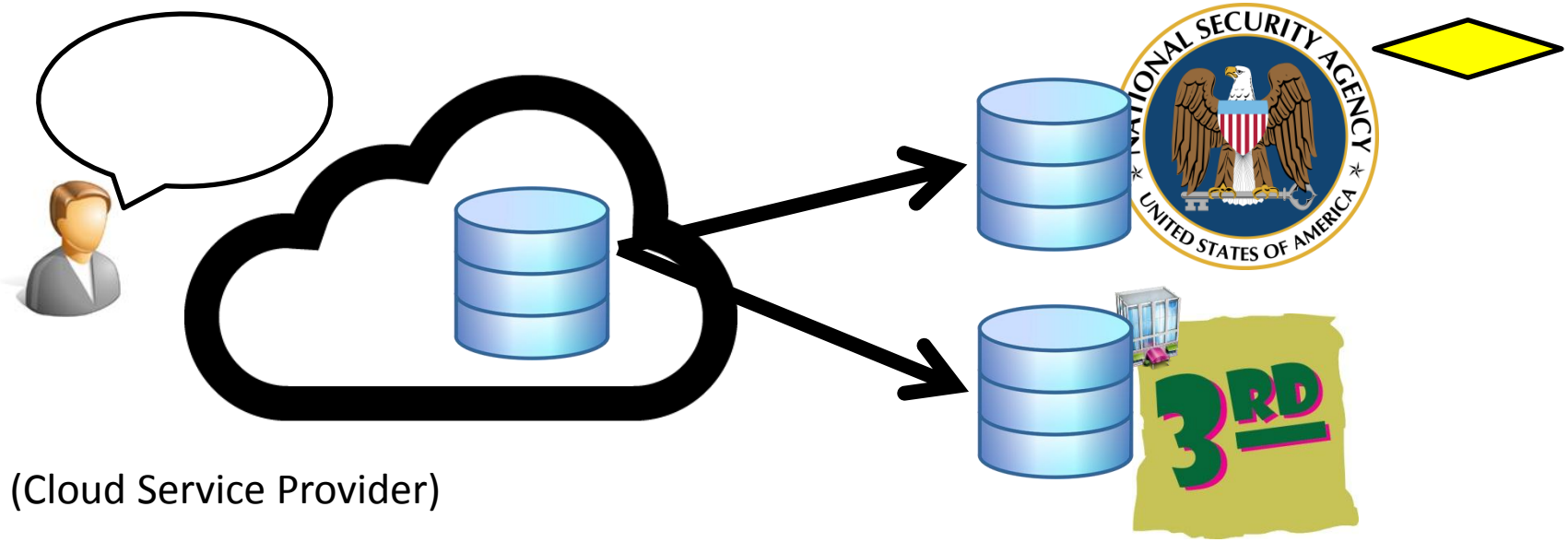
Dropbox for Business



Legal implications

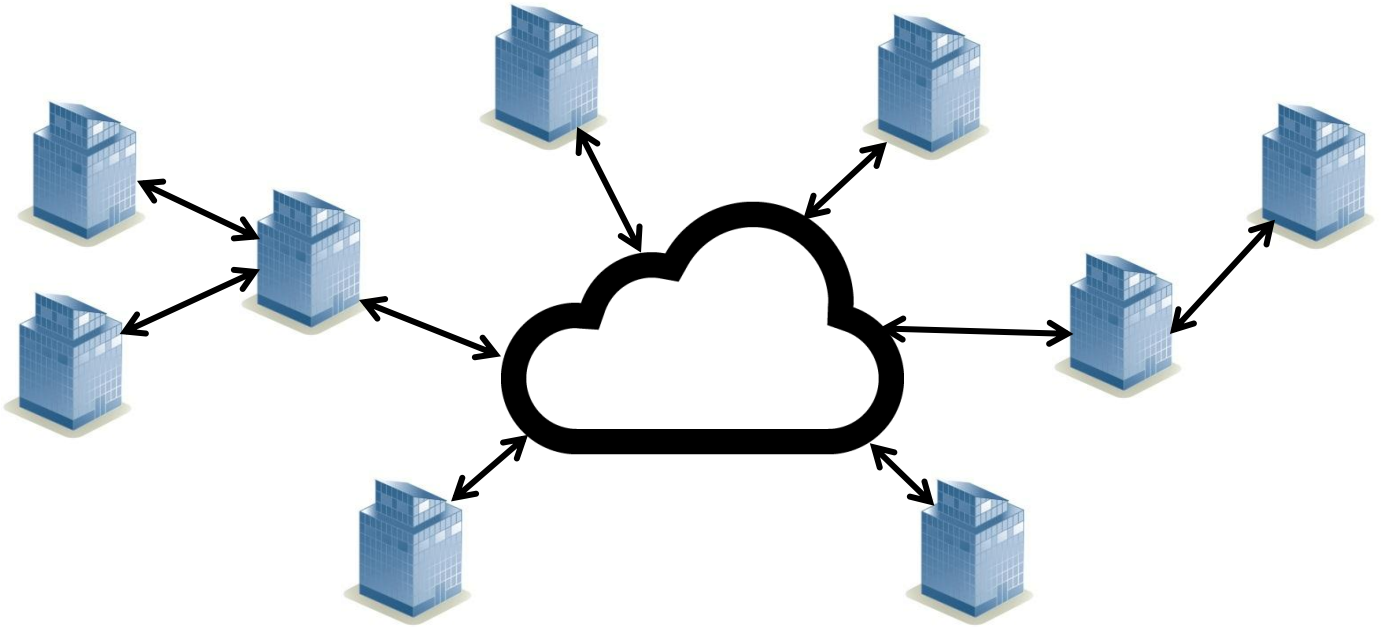
Which laws apply to the data?



Voc: CSP (Cloud Service Provider)

Supply chain management



CSP always responsible for its contractual commitments?

Audit

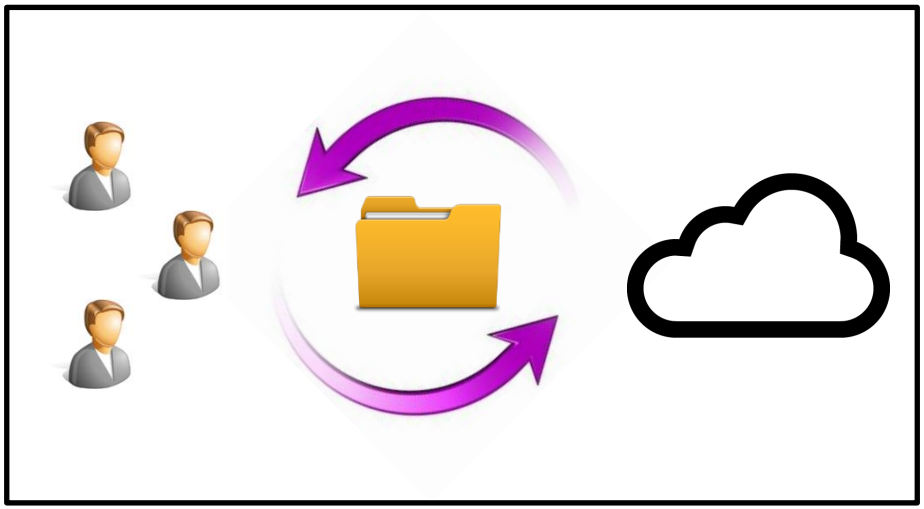
Every 6 months

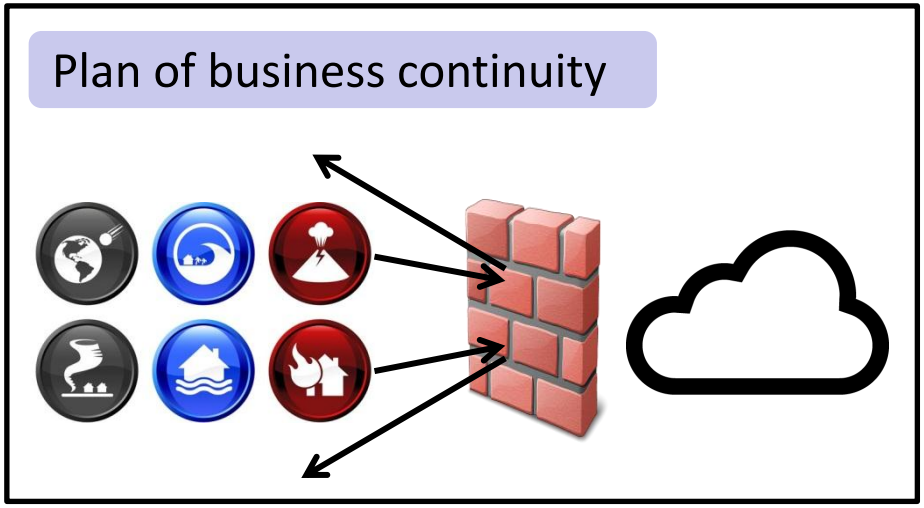
Every year

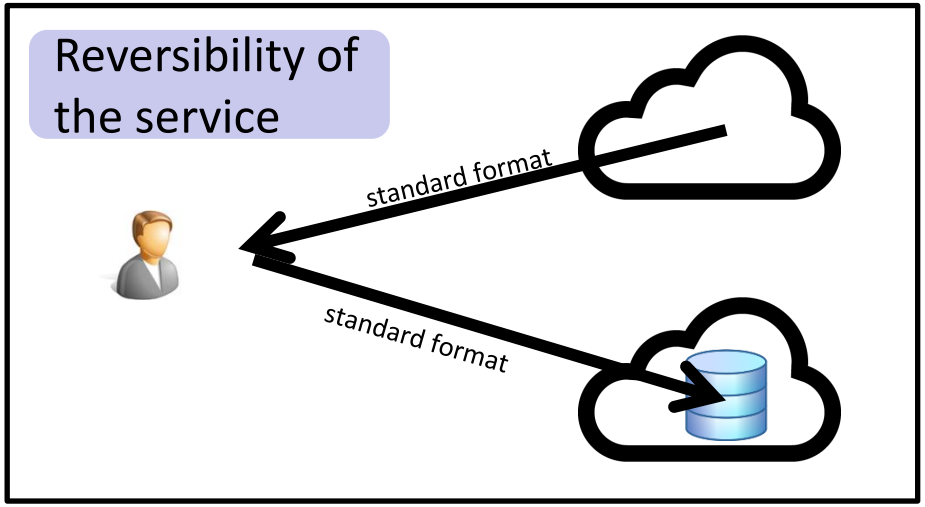
Meta-data

Meta-data only used for the cloud service?

Quality of the service







Governance: to remember

Which laws?

Reliable supply chain?

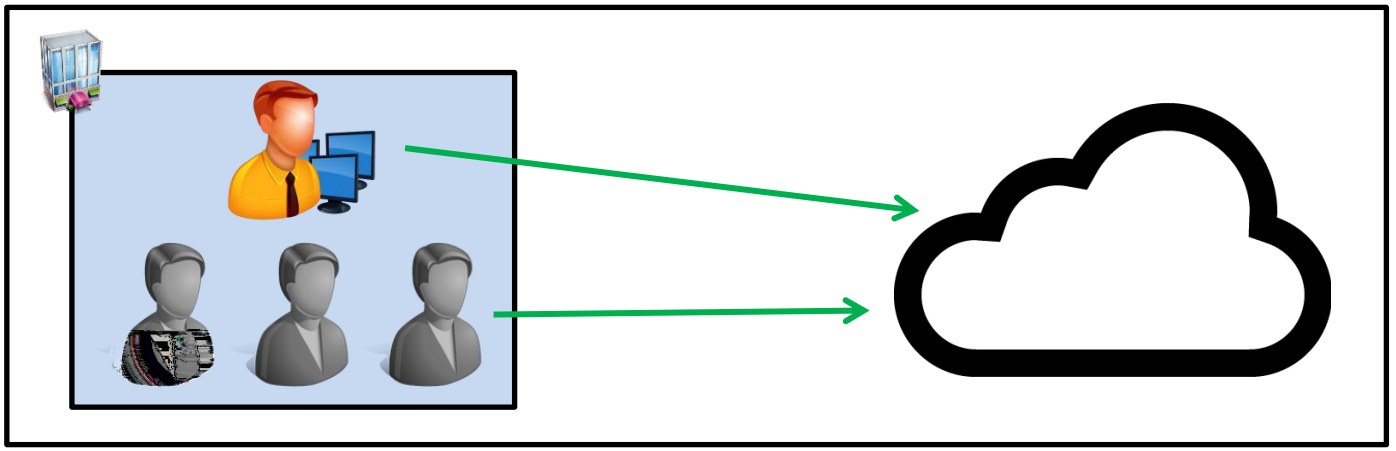
Regular audit?

No misuse of meta-data?

Good quality of service?


Island
ation
dge ending
Short Br

Authentication level



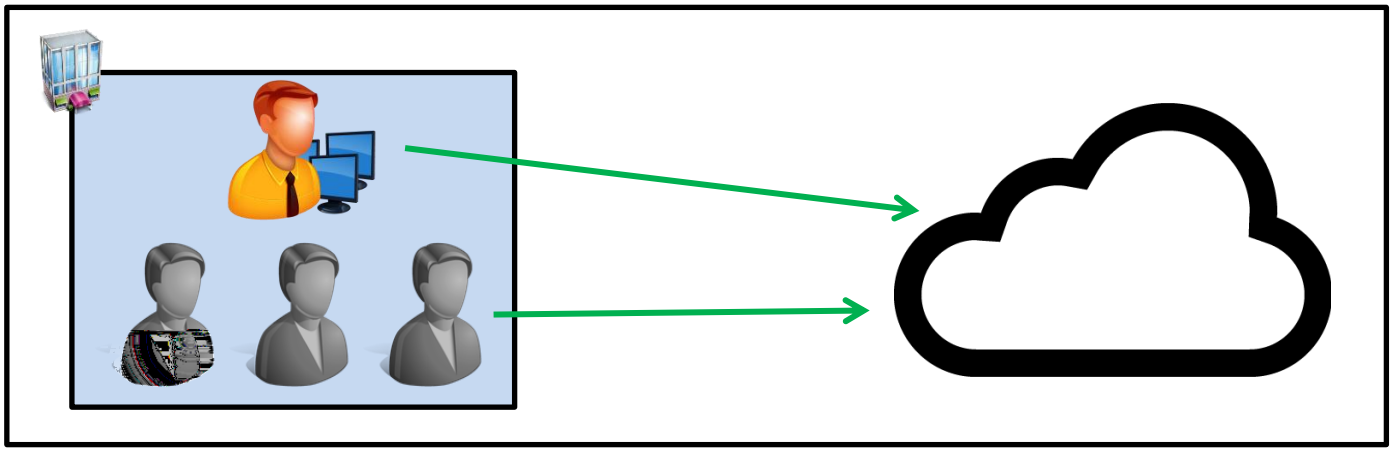
Username + Password

Username + Password + Token

Username + Password + Certificat

Username + Password + Certificat/Token + Location

Authentication level

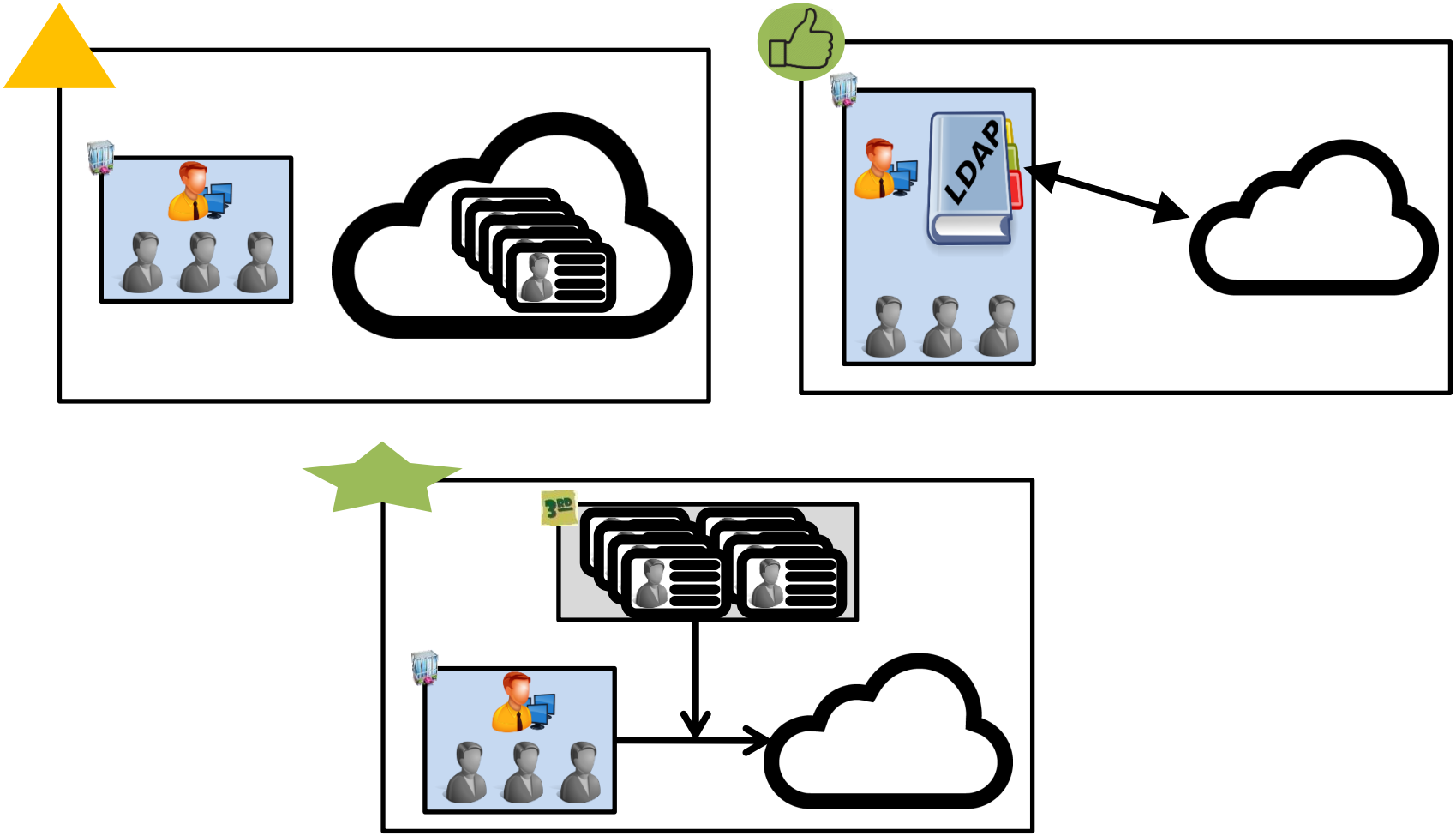


Username + Password + Token

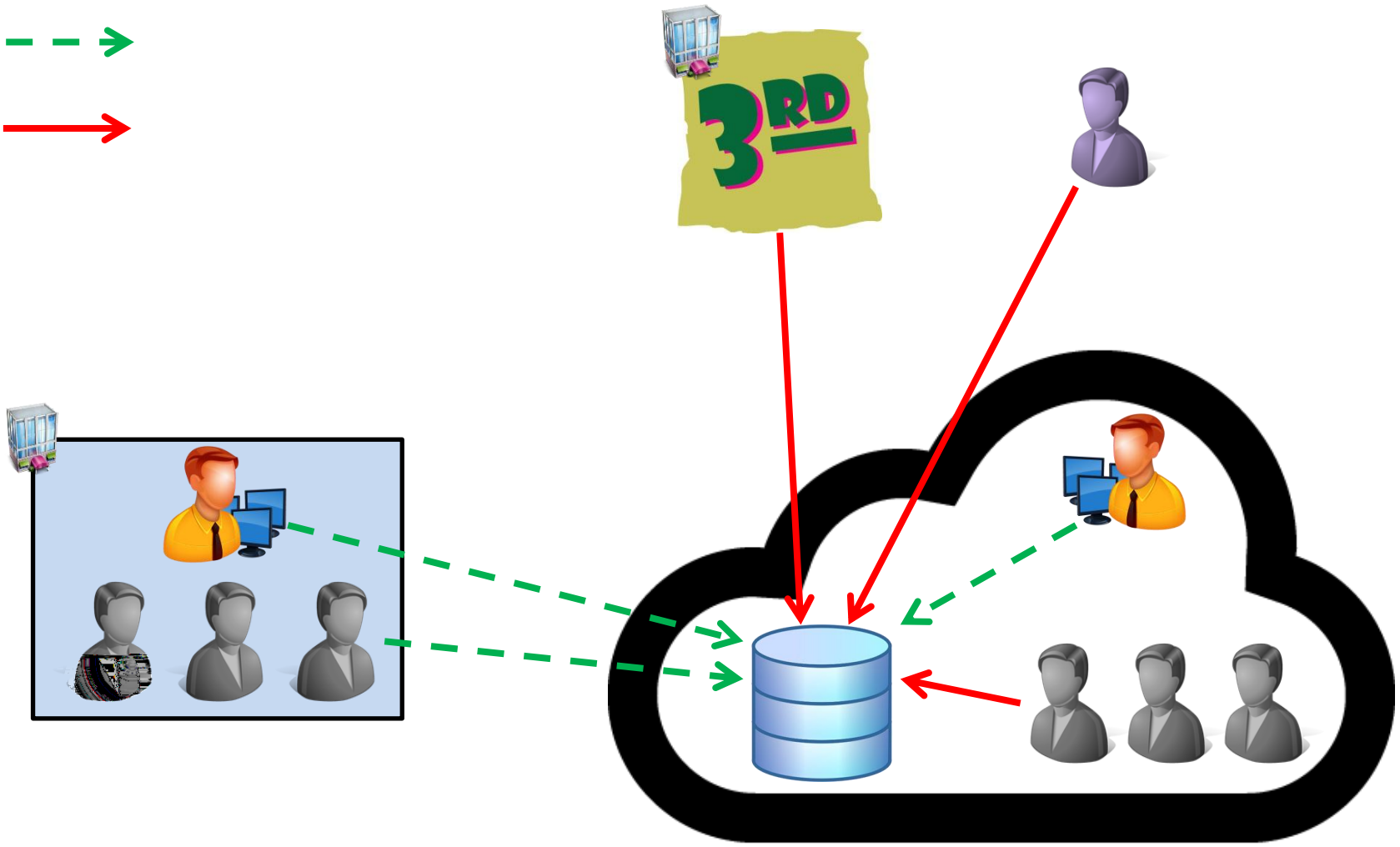
Username + Password + Certificat

Username + Password + Certificat/Token + Location

User management



Access management



IAM: to remember

2-factor authentication?

Controlled user management?

Well-defined access management?

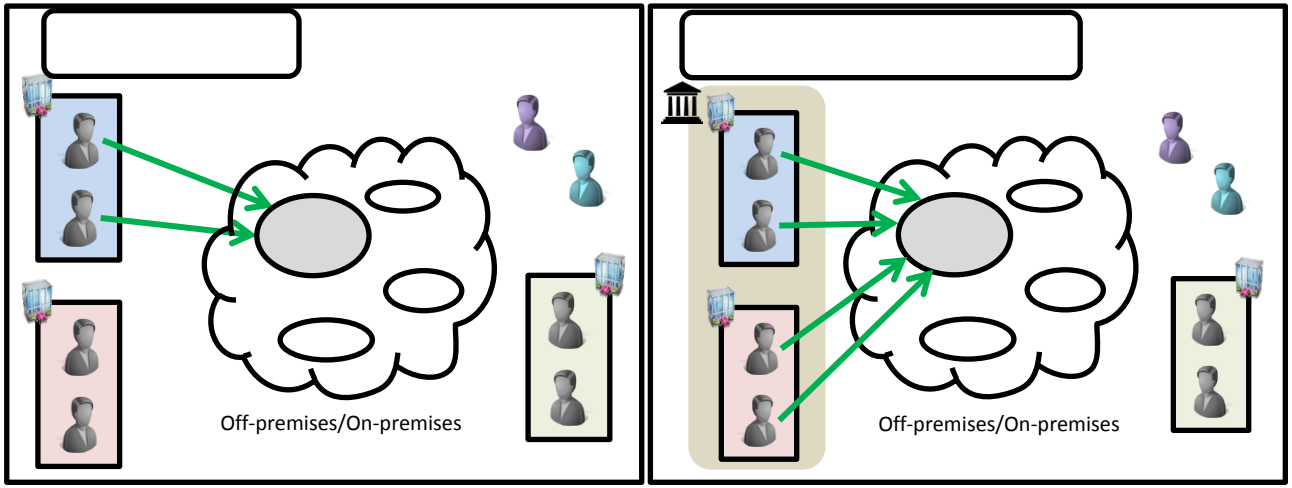
Security standards

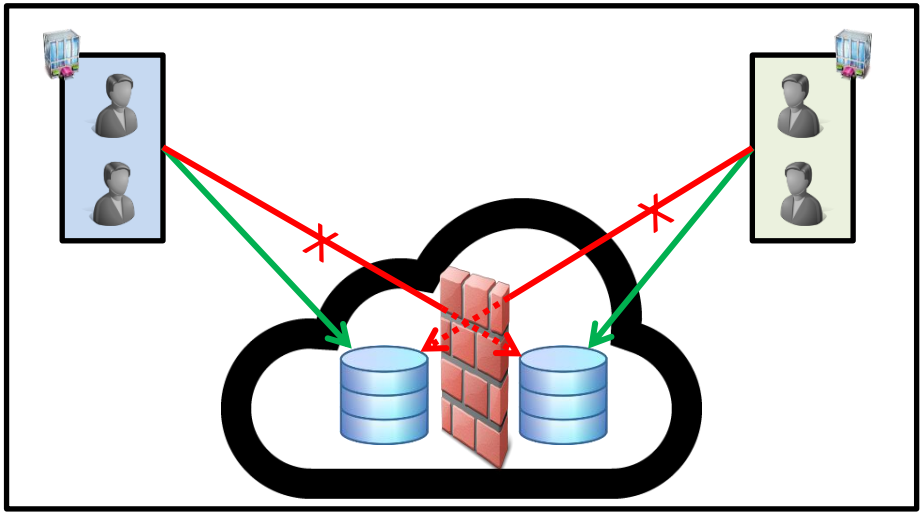
- Anti-virus, anti-malwares
- Patch management process
- Acceptance environments

- Network security: firewall, APT detection tools
- Monitoring: IDS/IPS, file integrity
- Data leak detection: DLP tools
- Protection of hypervisors and admin consoles
- Secure data deletion: crypto wiping, demagnetization

- Data integrity and security in input and output
- API developed according to standards (e.g. OWASP)

Segregation of data





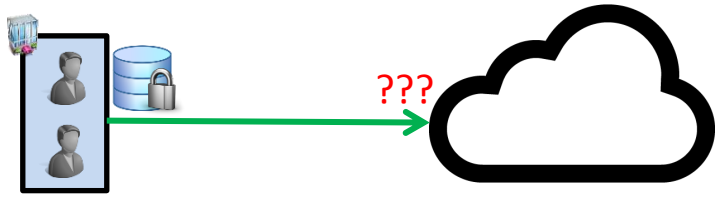
Very important point
BUT
often not documented

Cryptography

Strong crypto

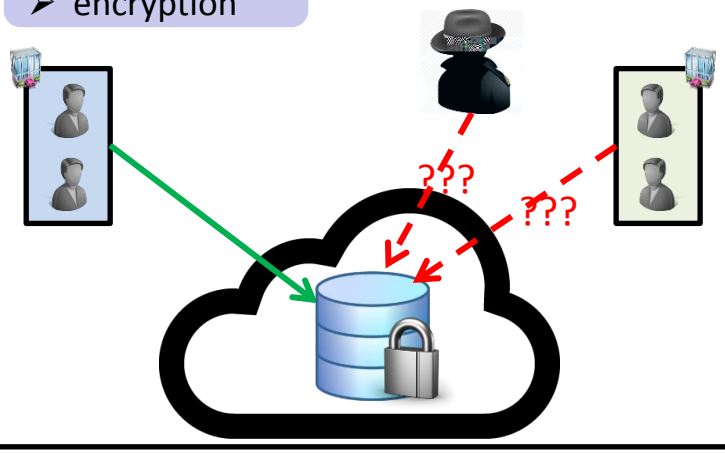
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Confidentiality towards the CSP
- encryption

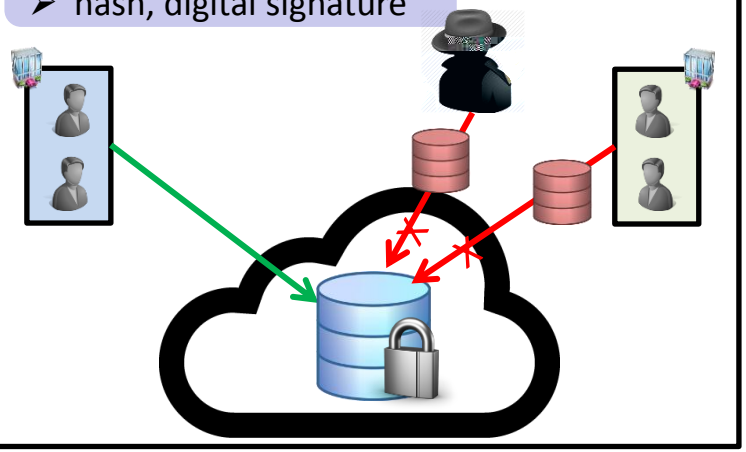


Outils: boxcryptor

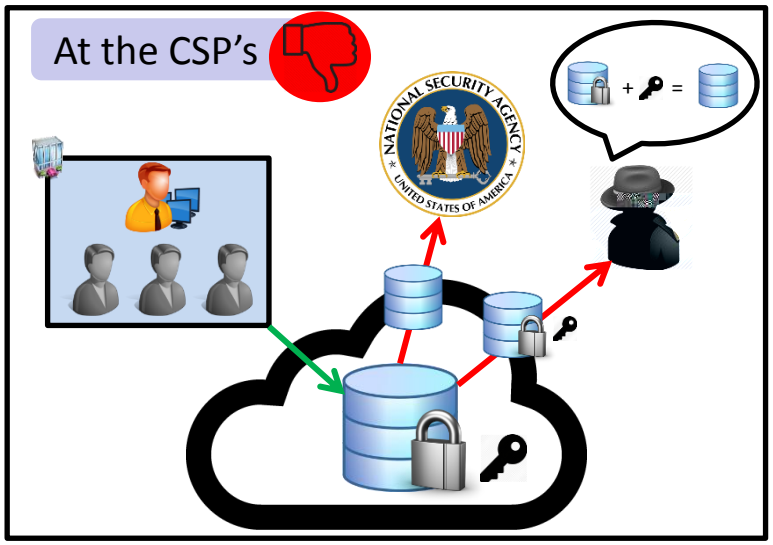
Confidentiality
- encryption

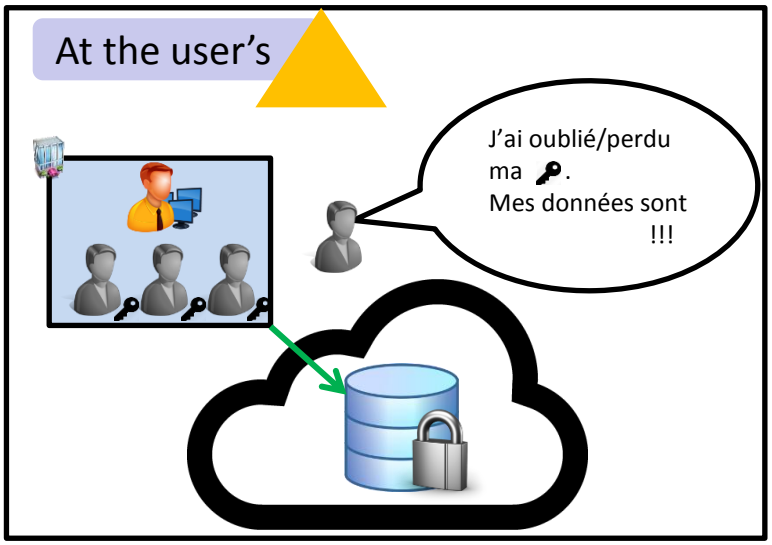


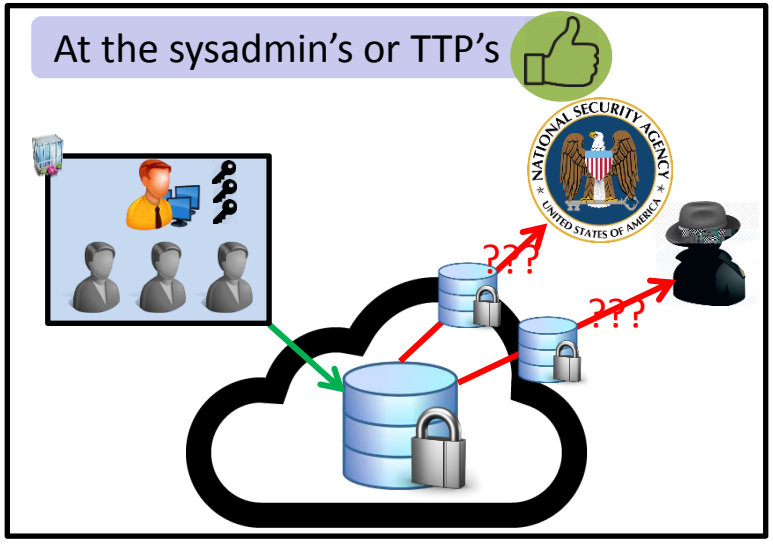
Integrity
- hash, digital signature



Key management







IT security: to remember

Security standards in place?

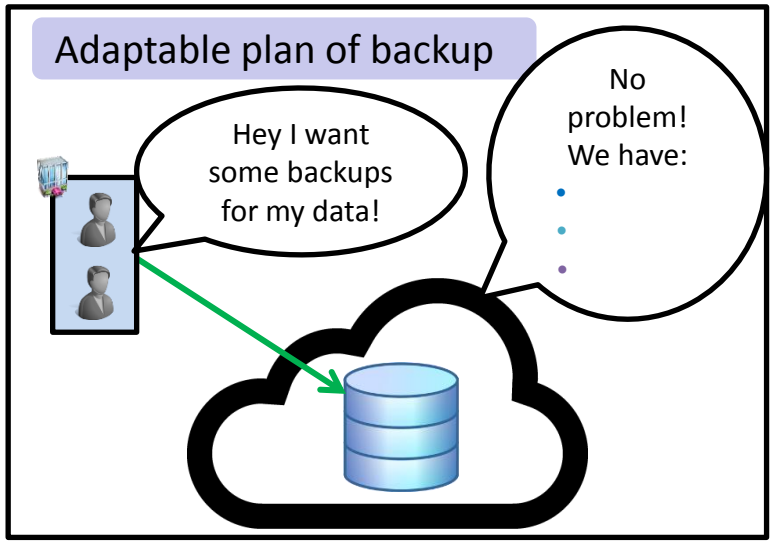
Segregation of data?

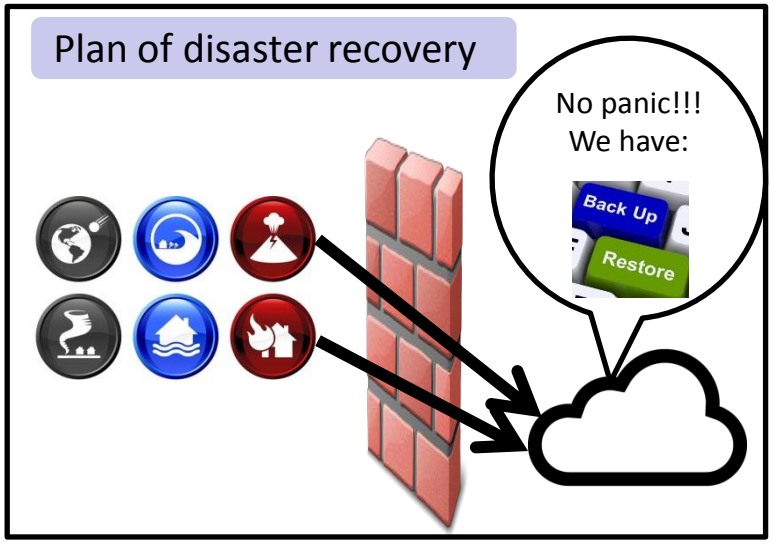
Cryptography standards used?

Data confidentiality and integrity?

Key management at the sysadmin's?

Backup and disaster recovery





Some values on the RTO and RPO

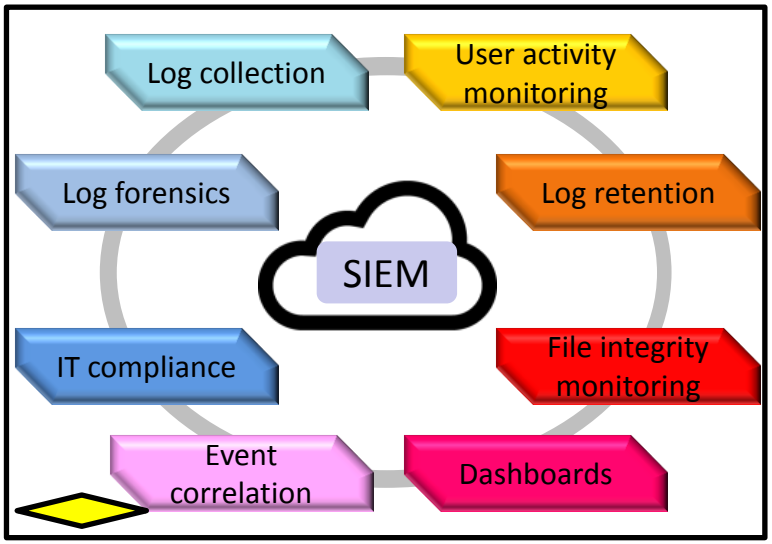
≈ 1 week

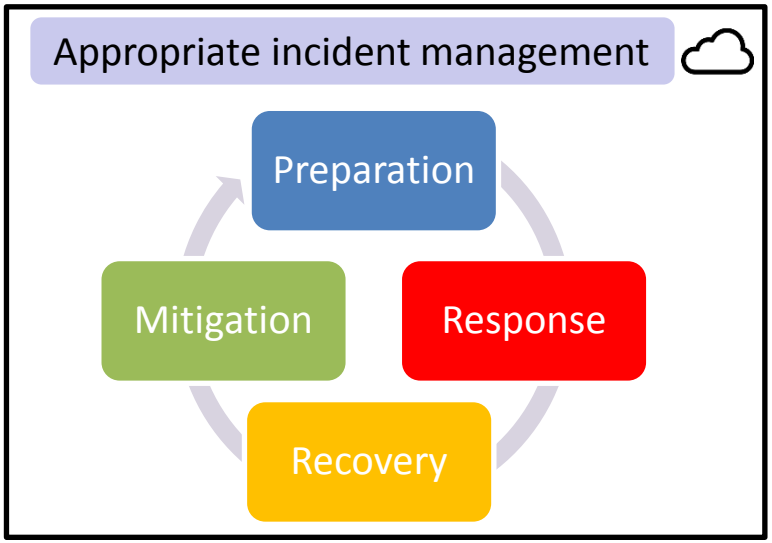
≈ 1 day

≈ 1 hour

Voc: RTO (Recovery Time Objective), RPO (Recovery Point Objective)

Incident management





Operational security: to remember

Adaptable plan of backup?

RTO and RPO < 1 day?

SIEM?

Appropriate incident management?

Security training of employees?


FILES
FILES

How works the model?

Result for the governance

	Category Title	Score	Minimal weighted score	Maximal weighted score
1.1	Legal implication		6%	11%
1.1.1	What is the physical location of data-at-rest?	Unknown	5,25	21
1.1.2	Which jurisdiction is the CSP subject to?	US	10,5	10,5
1.1.3	Can the CSP accomodate with the tenant's data retention requirements?	Unknown	0	8
1.1.4	Can the data be given to governments if requested for judicial requirements without informing the tenant or without constitutional guarantees?	Yes	0	0
1.1.5	Can the data be given to, shared with third parties, or used by the CSP for other purposes than the cloud service without the tenant's consent?	Yes	0	0
1.1.6	If the US-EU Safe Harbor applies, is the CSP registered?	Yes	8	8
1.2	Supply chain management		18%	22%
1.2.1	Does the CSP use subcontrators?	Yes	40	40
1.2.2	If so, will the CSP inform the tenant of the subcontractors hired to provide the cloud service?	Yes	20	20
1.2.3	If so, will the CSP inform the tenant of any change in the course of the contract?	Yes	20	20
1.2.4	If so, does the CSP guarantee contractually to remain fully responsible for his engagements, even with the hiring of subcontractors?	Unknown	0	20
1.3	Audit		10%	10%
1.3.1	At which time interval is the cloud service (including all its subcontractors) audited by a third party?	1 year	12,75	12,75
1.3.2	If the cloud service is audited, are the scopes of the audits accurately defined?	Yes	32	32
1.3.3	At which time interval is the cloud service (including all its subcontractors) pen-tested?	1 year	5,95	5,95
1.3.4	Did the cloud service define an ISP (Information Security Policy) and obtain a security-related certification?	Yes, ISP and certificate(s)	14	14
1.3.5	Is there a Tier certification of data centers (especially for physical availability and security) or equivalent certification?	No Tier certification or equivalent	0	0
1.4	Business continuity		0%	8%
1.4.1	Is the cloud service delivery managed under SLAs (Service Level Agreements)?	No	0	0
1.4.2	Does the CSP define and implement a business continuity plan?	Unknown	0	33
1.4.3	Is the reversibility of the cloud service provided?	No	0	0
1.5	Others		8%	15%
1.5.1	Does the CSP apply a segregation of duties in the CSP organization to protect the tenants?	Unknown	0	50
1.5.2	If meta-data are extracted by the CSP from the process of tenant's data, are they used for the cloud service only?	Yes	50	50

Worst case vs. Best case

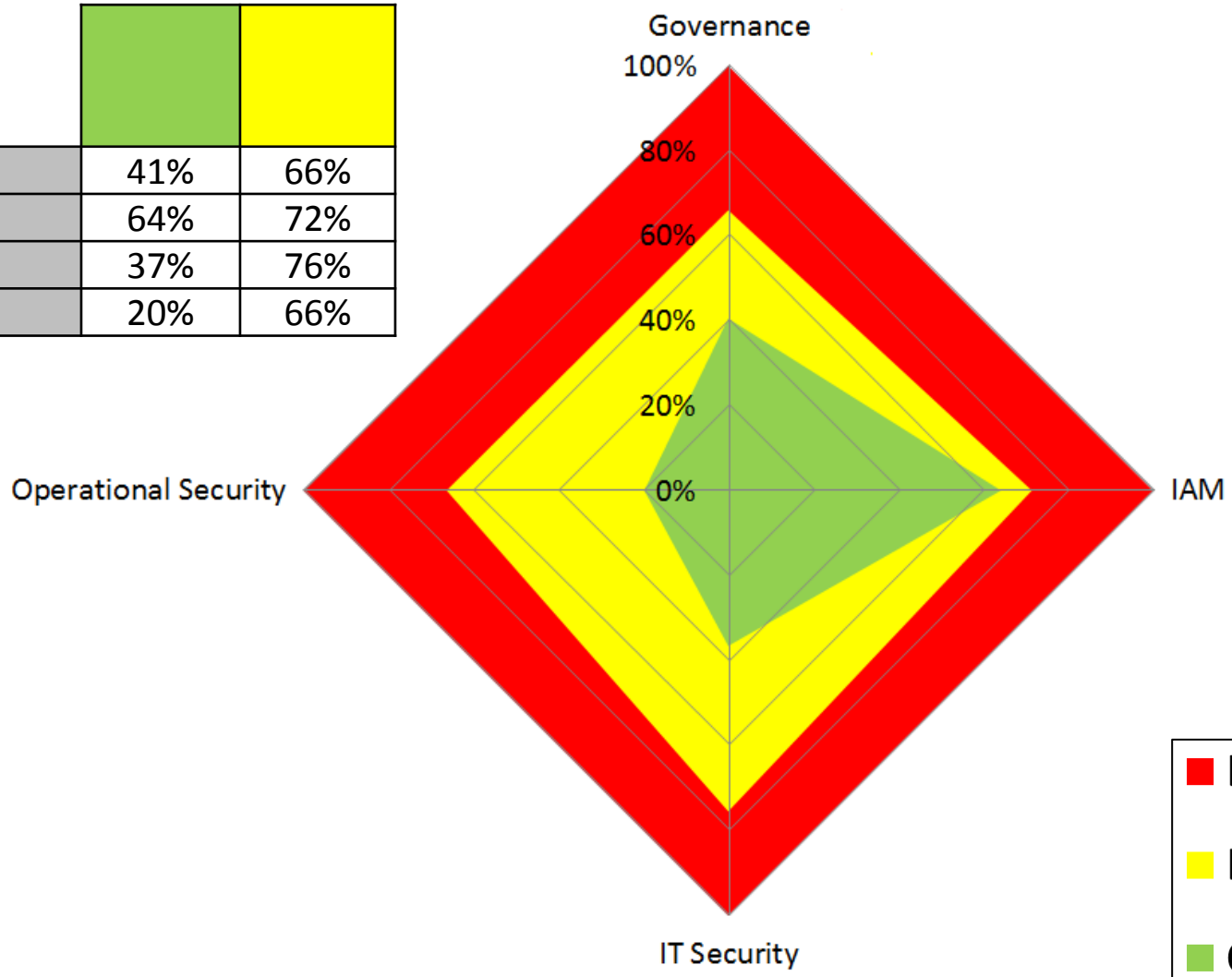
	Score	Minimal weighted score	Maximal weighted score
		41%	66%
		6%	11%
	Unknown	5,25	21
	US	10,5	10,5
	Unknown	0	8
nant or without constitutionalguarantees?	Yes	0	0
ud service without the tenant's consent?	Yes	0	0
	Yes	8	8
		18%	22%
	Yes	40	40
	Yes	20	20
	Yes	20	20
the hiring of subcontractors?	Unknown	0	20
		10%	10%

Result for the governance

	Score	Minimal weighted score	Maximal weighted score
		41%	66%
		6%	11%
	Unknown	5,25	21
	US	10,5	10,5
	Unknown	0	8
nant or without constitutionalguarantees?	Yes	0	0
oud service without the tenant's consent?	Yes	0	0
	Yes	8	8
		18%	22%
	Yes	40	40
	Yes	20	20
	Yes	20	20
the hiring of subcontractors?	Unknown	0	20
		10%	10%

Preliminary result of the analysis

	41%	66%
	64%	72%
	37%	76%
	20%	66%



Cloud policy of Belgian social security

Goal?

- Established the when an institution of the social security is considering using a cloud service

URL?

- QR code of the URL

Model?

- Each point is considered in the model
- But the model goes a bit further in the analysis

Smals
ICT for society

Cloud policy in the model

	Category Title	Score	Minimal weighted score	Maximal weighted score
1.1	Legal implication		6%	11%
1.1.1	What is the physical location of data-at-rest?	Unknown	5,25	21
1.1.2	Which jurisdiction is the CSP subject to?	US	10,5	10,5
1.1.3	Can the CSP accomodate with the tenant's data retention requirements?	Unknown	0	8
1.1.4	Can the data be given to governments if requested for judicial requirements without informing the tenant or without constitutional guarantees?	Yes	0	0
1.1.5	Can the data be given to, shared with third parties, or used by the CSP for other purposes than the cloud service without the tenant's consent?	Yes	0	0
1.1.6	If the US-EU Safe Harbor applies, is the CSP registered?	Yes	8	8
1.2	Supply chain management		18%	22%
1.2.1	Does the CSP use subcontrators?	Yes	40	40
1.2.2	If so, will the CSP inform the tenant of the subcontractors hired to provide the cloud service?	Yes	20	20
1.2.3	If so, will the CSP inform the tenant of any change in the course of the contract?	Yes	20	20
1.2.4	If so, does the CSP guarantee contractually to remain fully responsible for his engagements, even with the hiring of subcontractors?	Unknown	0	20
1.3	Audit		10%	10%
1.3.1	At which time interval is the cloud service (including all its subcontractors) audited by a third party?	1 year	12,75	12,75
1.3.2	If the cloud service is audited, are the scopes of the audits accurately defined?	Yes	32	32
1.3.3	At which time interval is the cloud service (including all its subcontractors) pen-tested?	1 year	5,95	5,95
1.3.4	Did the cloud service define an ISP (Information Security Policy) and obtain a security-related certification?	Yes, ISP and certificate(s)	14	14
1.3.5	Is there a Tier certification of data centers (especially for physical availability and security) or equivalent certification?	No Tier certification or equivalent	0	0
1.4	Business continuity		0%	8%
1.4.1	Is the cloud service delivery managed under SLAs (Service Level Agreements)?	No	0	0
1.4.2	Does the CSP define and implement a business continuity plan?	Unknown	0	33
1.4.3	Is the reversibility of the cloud service provided?	No	0	0
1.5	Others		8%	15%
1.5.1	Does the CSP apply a segregation of duties in the CSP organization to protect the tenants?	Unknown	0	50
1.5.2	If meta-data are extracted by the CSP from the process of tenant's data, are they used for the cloud service only?	Yes	50	50

Smals
ICT for society

Cloud policy in the model

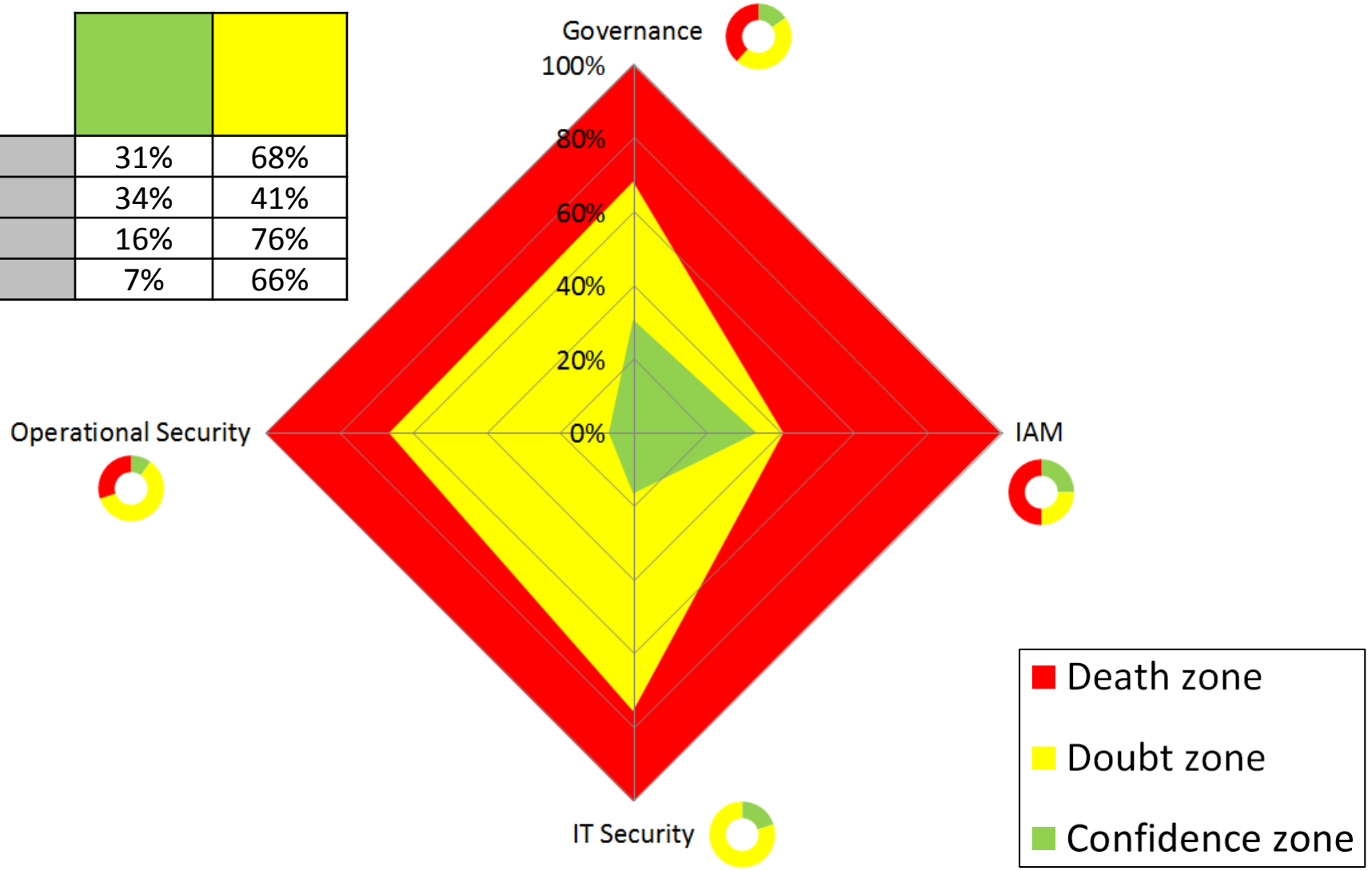
	Category Title	Score	Minimal weighted score	Maximal weighted score	Compliance with cloud policy
1.1	Legal implication		6%	11%	
1.1.1	What is the physical location of data-at-rest?	Unknown	5,25	21	
1.1.2	Which jurisdiction is the CSP subject to?	US	10,5	10,5	
1.1.3	Can the CSP accomodate with the tenant's data retention requirements?	Unknown	0	8	
1.1.4	Can the data be given to governments if requested for judicial requirements without informing the tenant or without constitutional guarantees?	Yes	0	0	
1.1.5	Can the data be given to, shared with third parties, or used by the CSP for other purposes than the cloud service without the tenant's consent?	Yes	0	0	
1.1.6	If the US-EU Safe Harbor applies, is the CSP registered?	Yes	8	8	
1.2	Supply chain management		18%	22%	
1.2.1	Does the CSP use subcontrators?	Yes	40	40	
1.2.2	If so, will the CSP inform the tenant of the subcontractors hired to provide the cloud service?	Yes	20	20	
1.2.3	If so, will the CSP inform the tenant of any change in the course of the contract?	Yes	20	20	
1.2.4	If so, does the CSP guarantee contractually to remain fully responsible for his engagements, even with the hiring of subcontractors?	Unknown	0	20	
1.3	Audit		10%	10%	
1.3.1	At which time interval is the cloud service (including all its subcontractors) audited by a third party?	1 year	12,75	12,75	
1.3.2	If the cloud service is audited, are the scopes of the audits accurately defined?	Yes	32	32	
1.3.3	At which time interval is the cloud service (including all its subcontractors) pen-tested?	1 year	5,95	5,95	
1.3.4	Did the cloud service define an ISP (Information Security Policy) and obtain a security-related certification?	Yes, ISP and certificate(s)	14	14	
1.3.5	Is there a Tier certification of data centers (especially for physical availability and security) or equivalent certification?	No Tier certification or equivalent	0	0	
1.4	Business continuity		0%	8%	
1.4.1	Is the cloud service delivery managed under SLAs (Service Level Agreements)?	No	0	0	
1.4.2	Does the CSP define and implement a business continuity plan?	Unknown	0	33	
1.4.3	Is the reversibility of the cloud service provided?	No	0	0	
1.5	Others		8%	15%	
1.5.1	Does the CSP apply a segregation of duties in the CSP organization to protect the tenants?	Unknown	0	50	
1.5.2	If meta-data are extracted by the CSP from the process of tenant's data, are they used for the cloud service only?	Yes	50	50	

Compliance display in the model

	41%	66%	
	64%	72%	
	37%	76%	
	20%	66%	

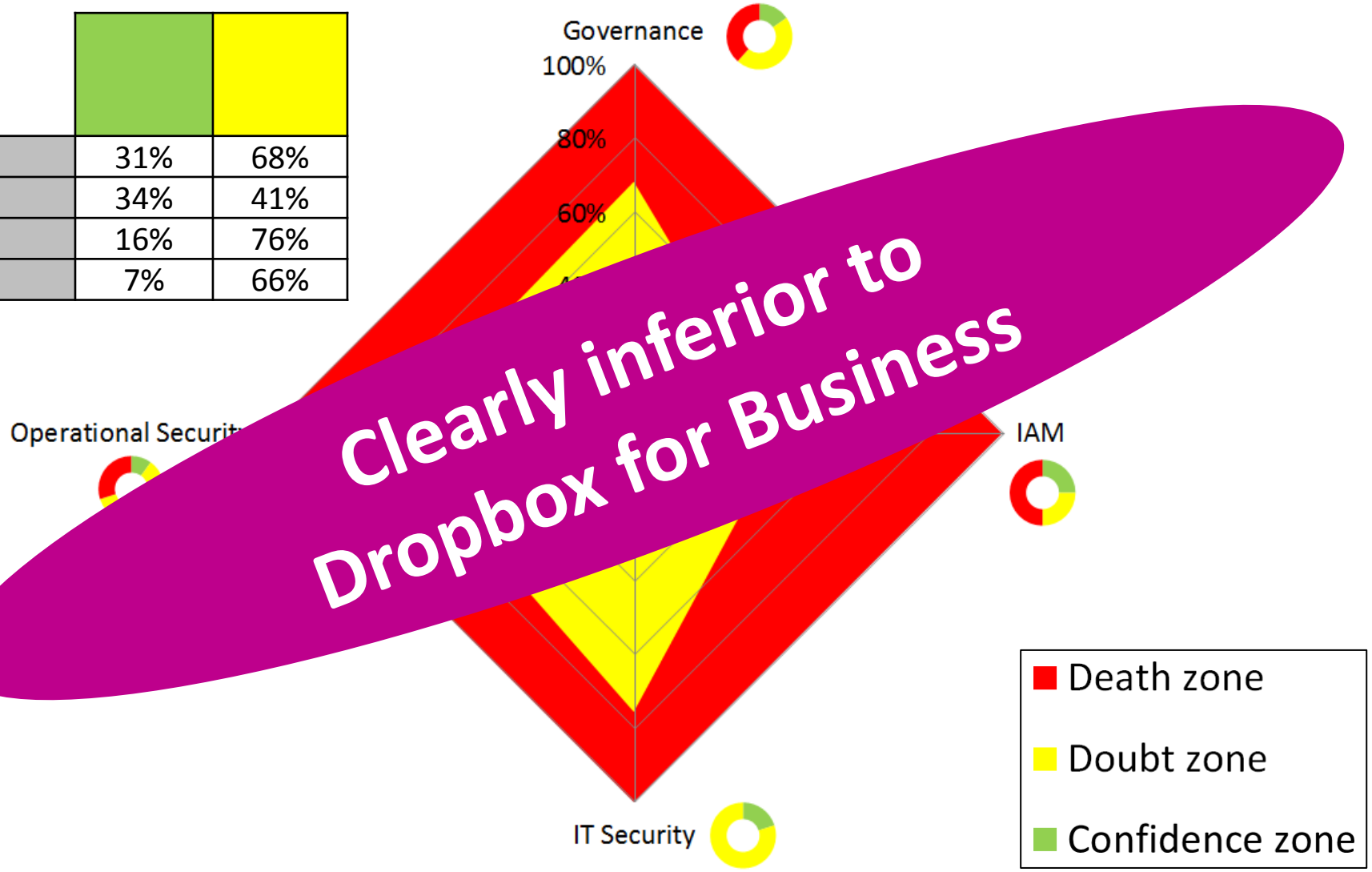
What about Dropbox Free?

	31%	68%
	34%	41%
	16%	76%
	7%	66%



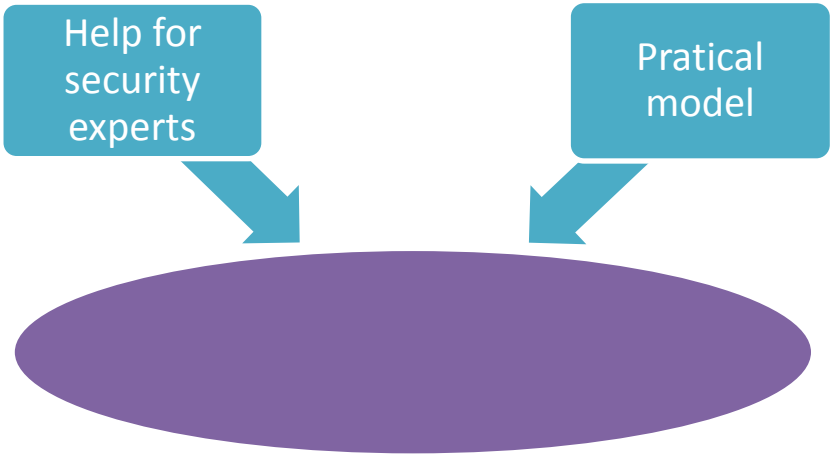
What about Dropbox Free?

	31%	68%
	34%	41%
	16%	76%
	7%	66%



Clearly inferior to Dropbox for Business

Goal of the model



Eliminate/filter non fruitful tracks

Select potential candidates

How to choose a good candidate?

- Experts analyze cloud services
- Results are published

- Client makes a self-assessment of his needs/requirements

- Client compares:

Self-assessment

Which type of data?

Which security level?

Self-assess: which type of data?

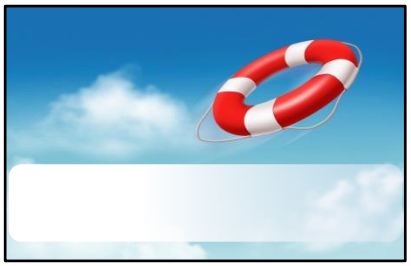
Ref: Data classification policy of the Belgian social security

Self-assess: which security level?

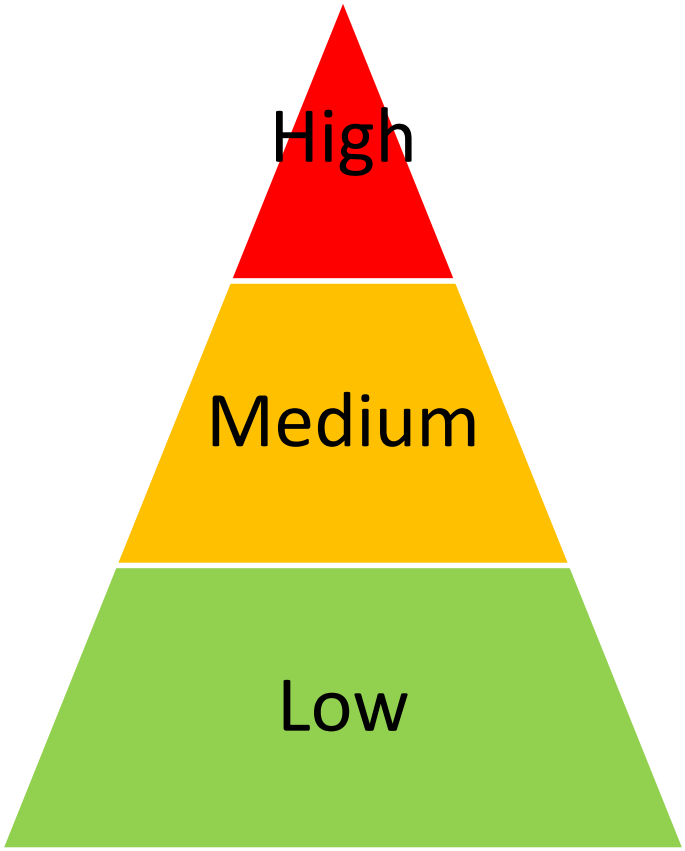
- Question 1?
- Question 2?
- …

- Question 1?
- Question 2?
- …

- Question 1?
- Question 2?
- …



- Question 1?
- Question 2?
- …

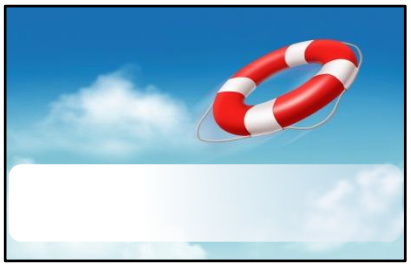


Self-assess: which security level?

- Question 1?
- Question 2?
- …

- Question 1?
- Question 2?
- …

- Question 1?
- Question 2?
- …



- Question 1?
- Question 2?
- …

Example: pay slip storage

	Category Title		Score	Required score
0.1	What type of data is intended to be moved to a cloud service?		Personal	
	Explanations / Examples			
	The choices of data type are extracted from the Data Classification Policy of the Social Security.			
	Score specification			
	Public	e.g. web site of BCSS/KSZ		
	Internal to the company	e.g. internal strategy, agenda, contact, email		
	Confidential of the company	e.g. financial roadmap		
	Personal	e.g. HR personal folder		
	Personal and social	e.g. National register data		
	Medical	e.g. medical record		
1.1	Which level of governance must be attained by the cloud service?		High	75
2.1	Which level of authentication must be offered by the cloud service?		High	28,9
2.2	Which level of control on the user management must be proposed by the cloud service?		High	24,75
2.3	Which level of access management must be provided by the cloud service?		High	24,75
3.1	Which deployment model must be provided by the cloud service?		Community cloud	16,5
3.2	Which level of interface security must be provided by the cloud service?		High	12
3.3	Which level of infrastructure and virtualization security must be achieved by the cloud service?		High	22,5
3.4	Which level of cryptography must be provided by the cloud service?		High	16,8
4.1	Which level of backup and disaster recovery must be provided by the cloud service?		High	37,5
4.2	Which level of incident management must be provided by the cloud service?		High	37,5

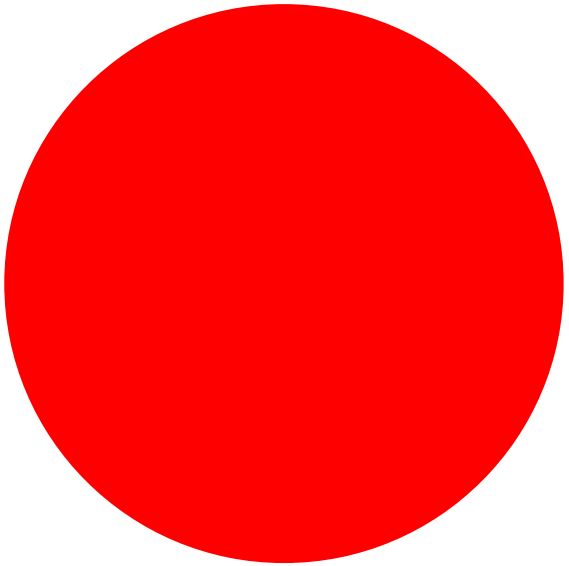
Smals
ICT for society

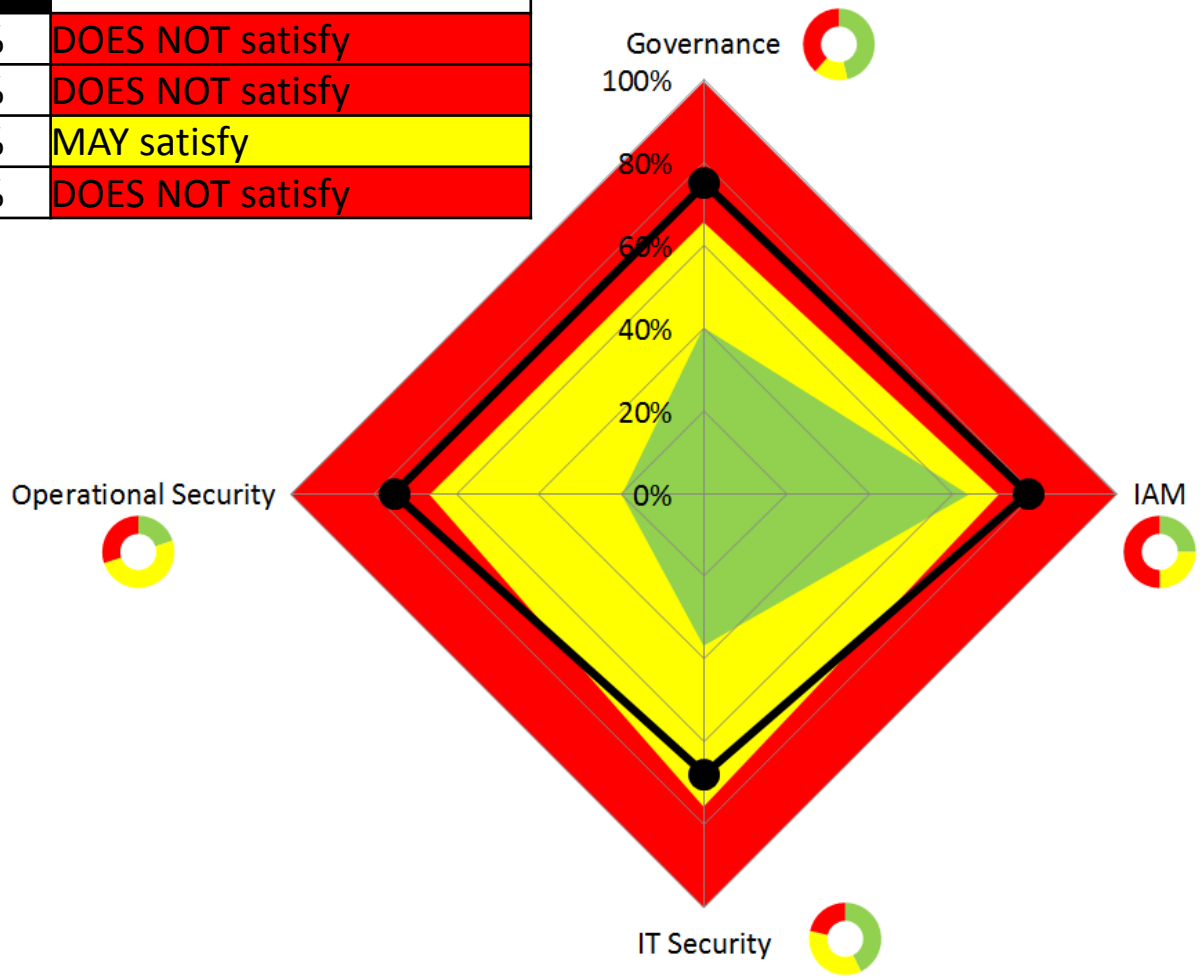
Example: pay slip storage

	Category Title	Score
	Data Type	
.1	What type of data is intended to be moved to a cloud service?	Personal
	Explanations / Examples	
	The choices of data type are extracted from the Data Classification Policy of the Social Security.	
	Score specification	
	Public	e.g. web site of BCSS/KSZ
	Internal to the company	e.g. internal strategy, agenda, contact, email
	Confidential of the company	e.g. financial roadmap
	Personal	e.g. HR personal folder
	Personal and social	e.g. National register data
	Medical	e.g. medical record
	Governance	
1	Which level of governance must be attained by the cloud service?	High
	Identity and Access Management (IAM)	
	Which level of authentication must be offered by the cloud service?	High
	the user management must be proposed by the cloud service?	High

Example: pay slip storage

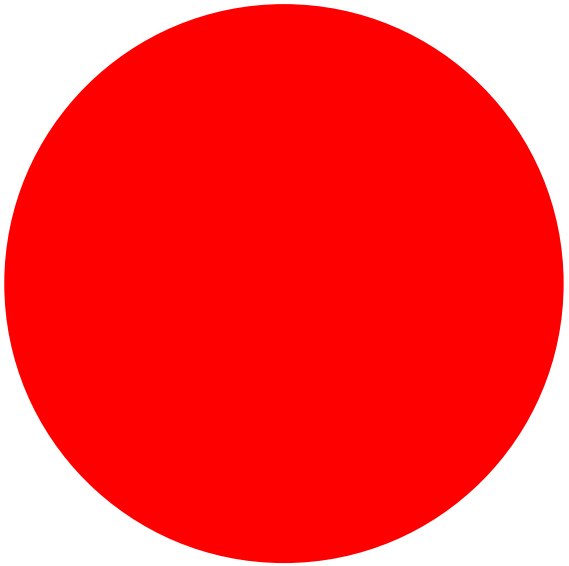
				Dropbox for Business
	41%	66%	75%	DOES NOT satisfy
	64%	72%	78%	DOES NOT satisfy
	37%	76%	68%	MAY satisfy
	20%	66%	75%	DOES NOT satisfy

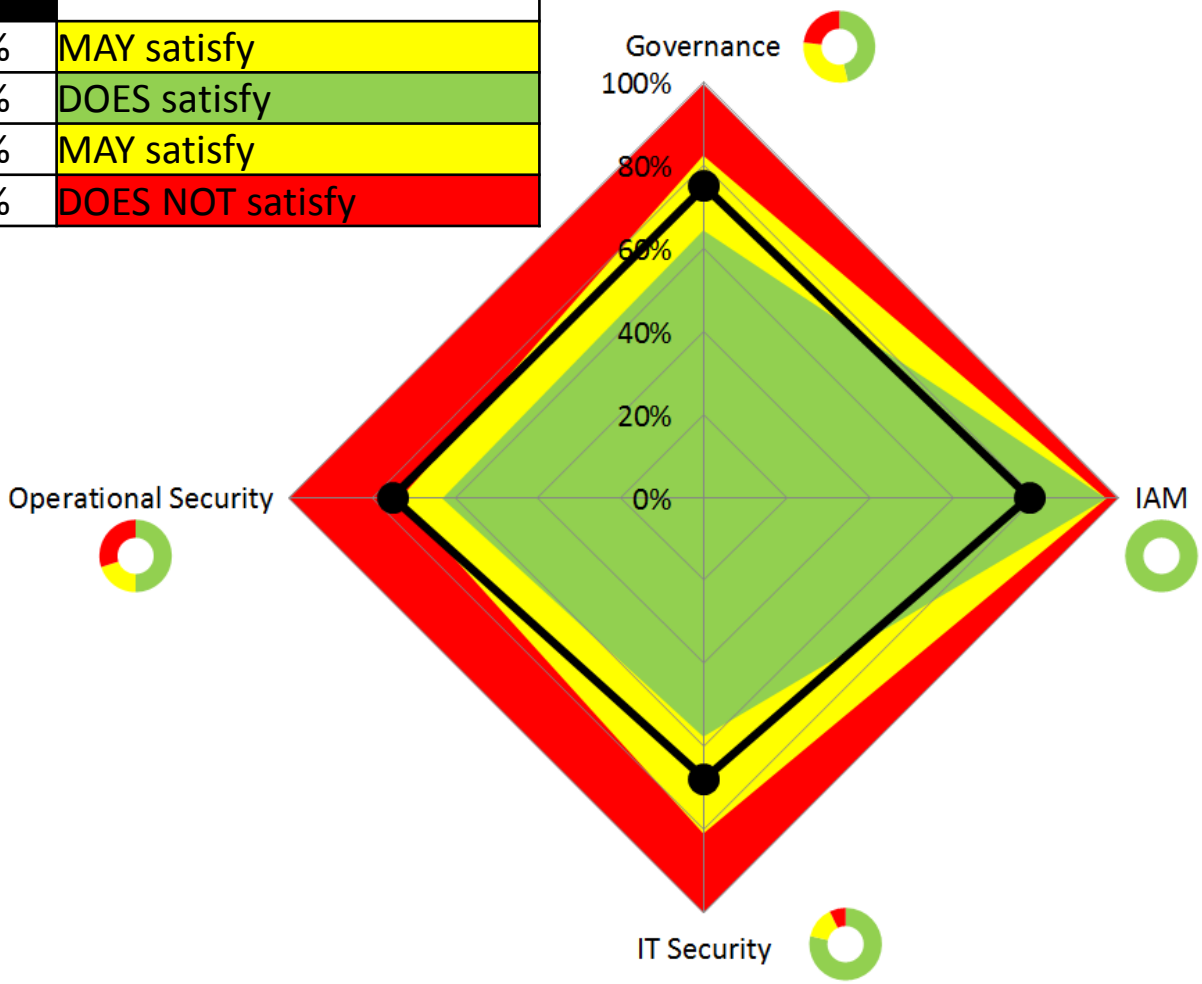




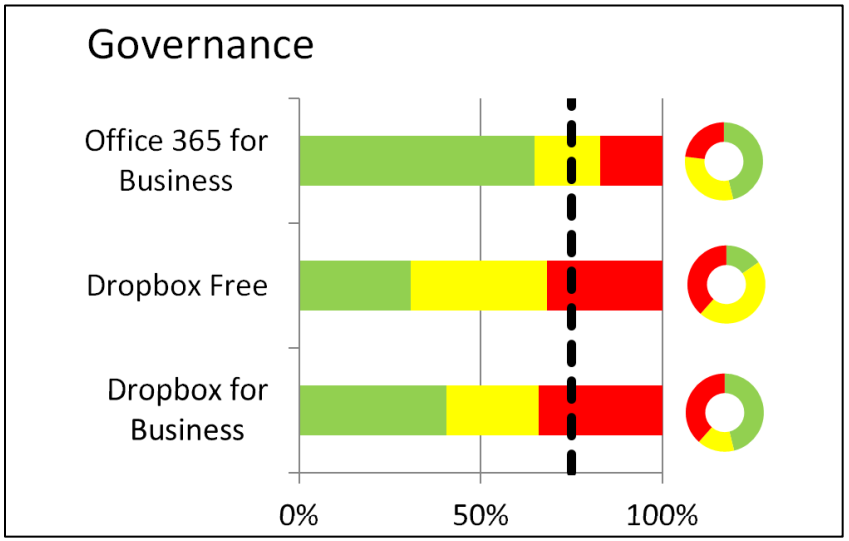
Example: pay slip storage

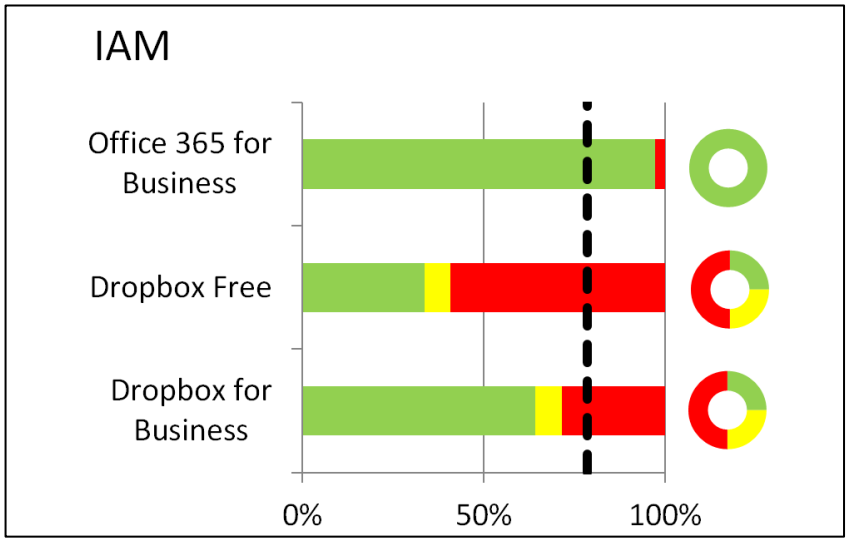
				Office 365 for Business
	65%	83%	75%	MAY satisfy
	97%	97%	78%	DOES satisfy
	58%	81%	68%	MAY satisfy
	63%	73%	75%	DOES NOT satisfy

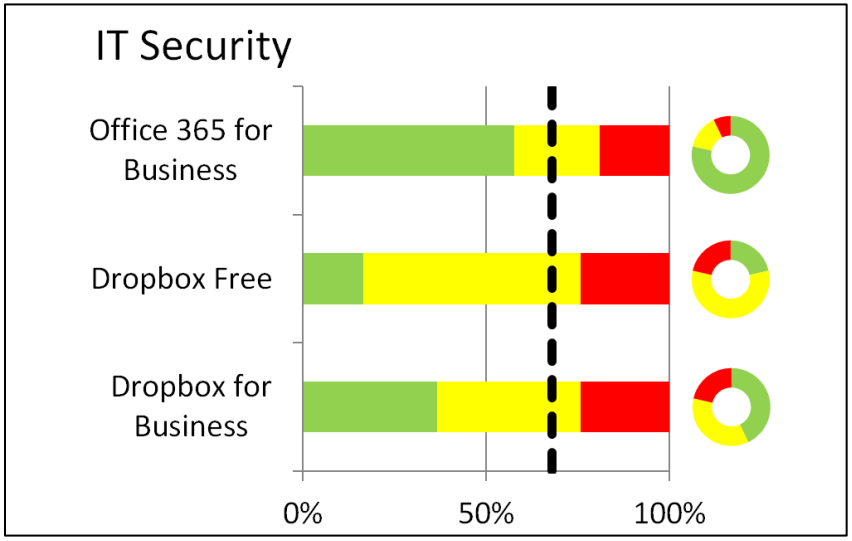


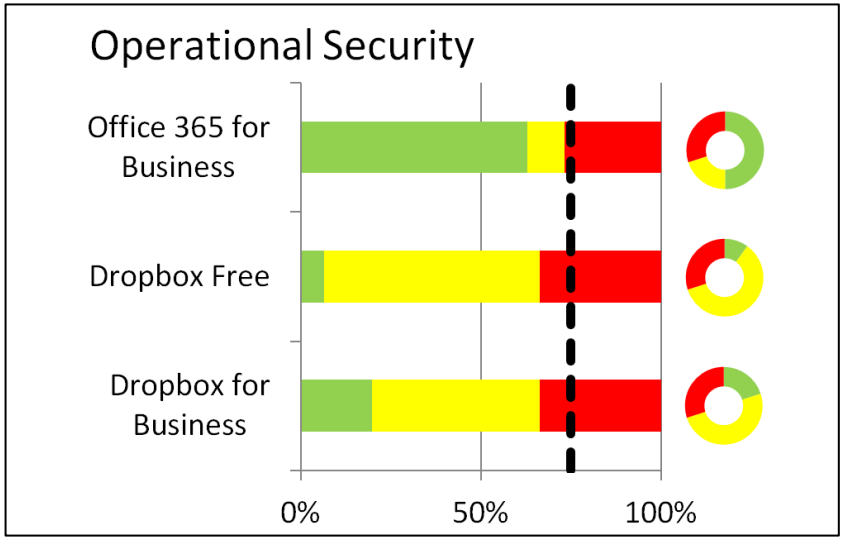


Example: pay slip storage

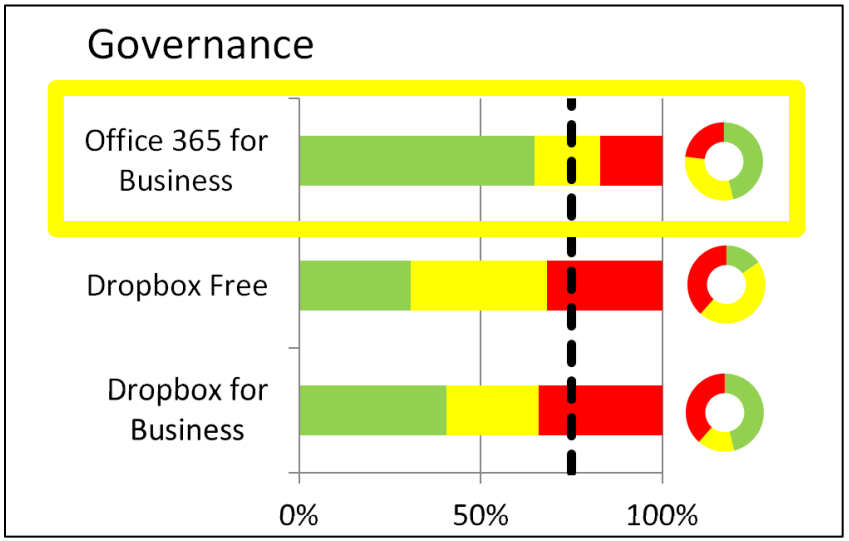


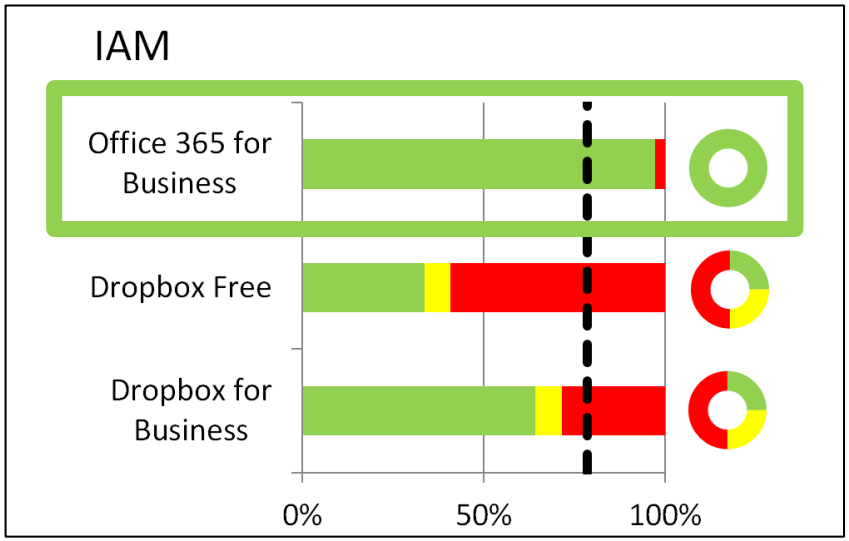


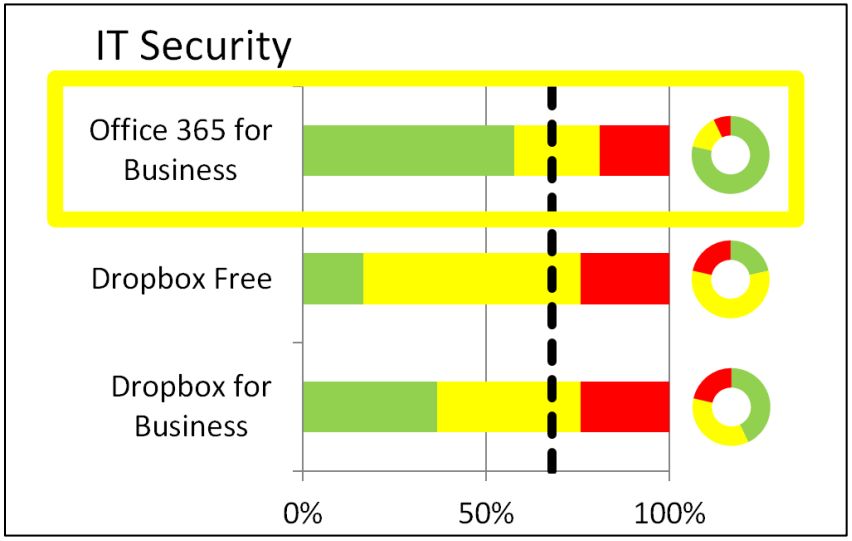


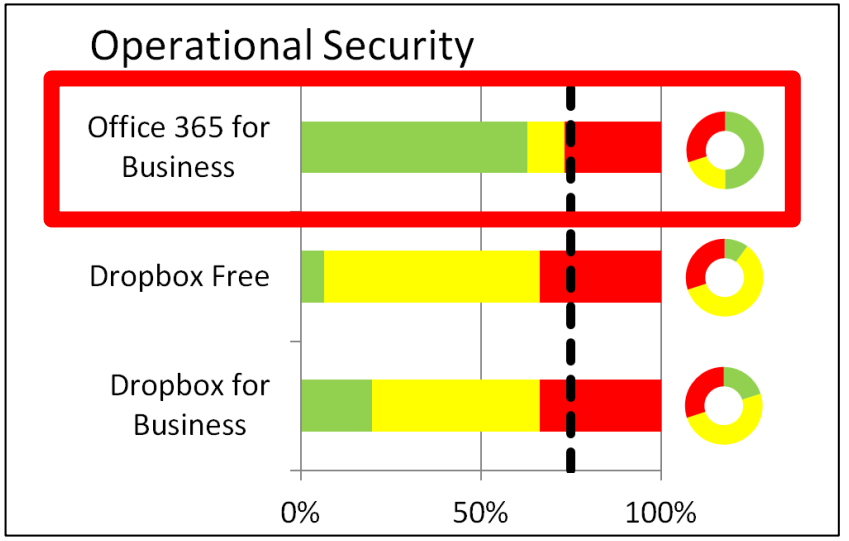


Example: pay slip storage

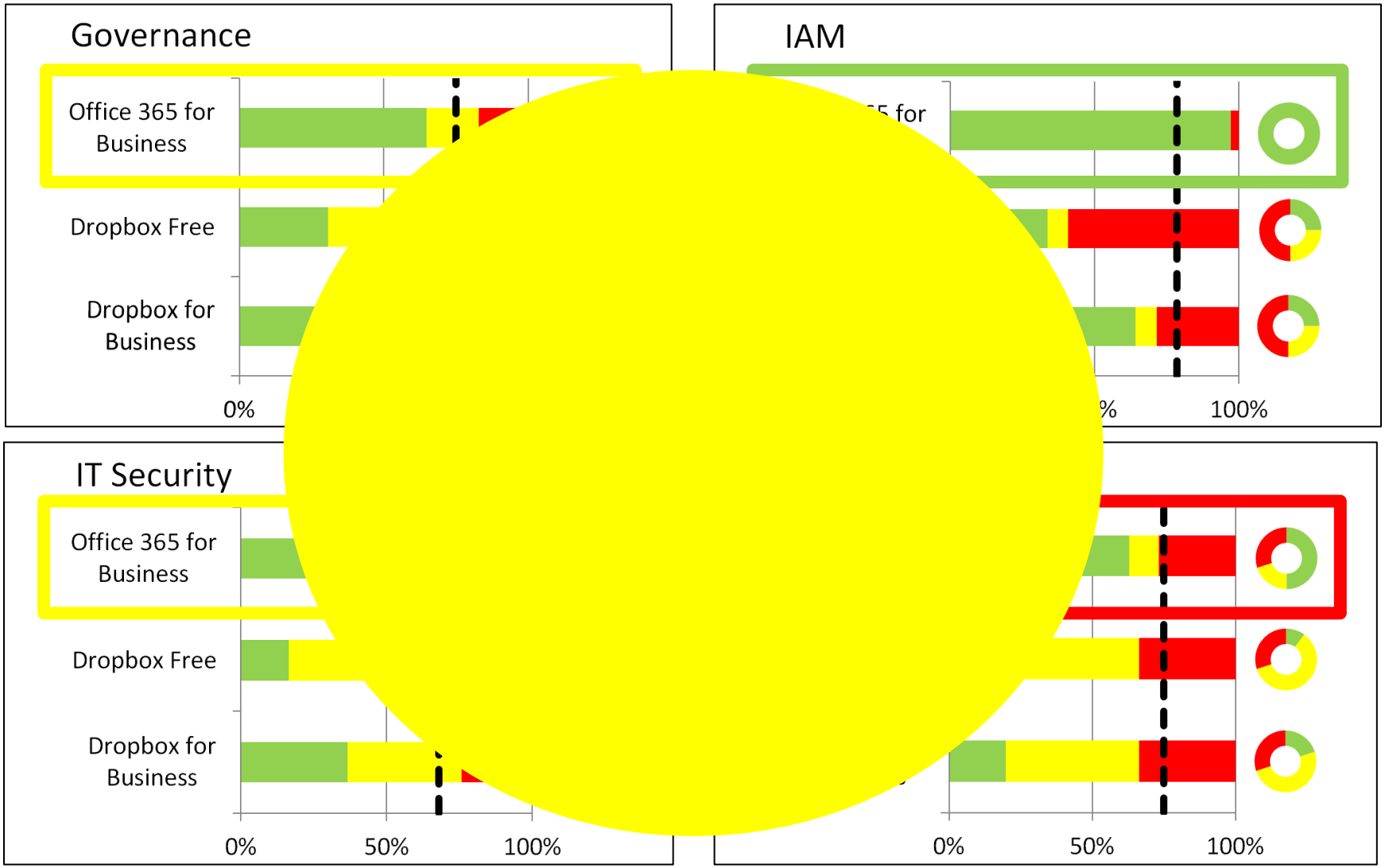








Example: pay slip storage



Conclusion

Cloud security is

Especially if we want to send there data

Importance of the security of a cloud service

Proposition of such an assessment tool:

A human expert is the only true judge of the result

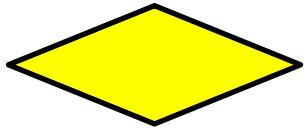
Where is the model?

URL?

- Version FR
- Version NL

For who?

- Security experts and counsellors

Some interesting 

- U.S. Government, "The PATRIOT Act"
- Tania Martin, "Research Note 32: Advanced Persistent Threats - Etat de l'Art"
- OWASP, "The OWASP Project"
- Kristof Verslype, "Quick Review 65: BoxCryptor - Client-side encryptie voor FSS"
- Kristof Verslype, "Research Note 26: Security Information & Event Management (SIEM)"
- Tania Martin, "Social engineering : watch out because there is no patch for human stupidity"
- Belgian social security, "Politique de sécurité relative à des services de Cloud Computing"
- Belgian social security, "Policy dataclassification"
- Smals Research, "Modèle d'évaluation de sécurité cloud"
- Smals Research, "Cloud security evaluatiemodel"

☎ 02 787 56 05
✉ tania.martin@smals.be

www.smals.be
@Smals_ICT
www.smalsresearch.be
@SmalsResearch