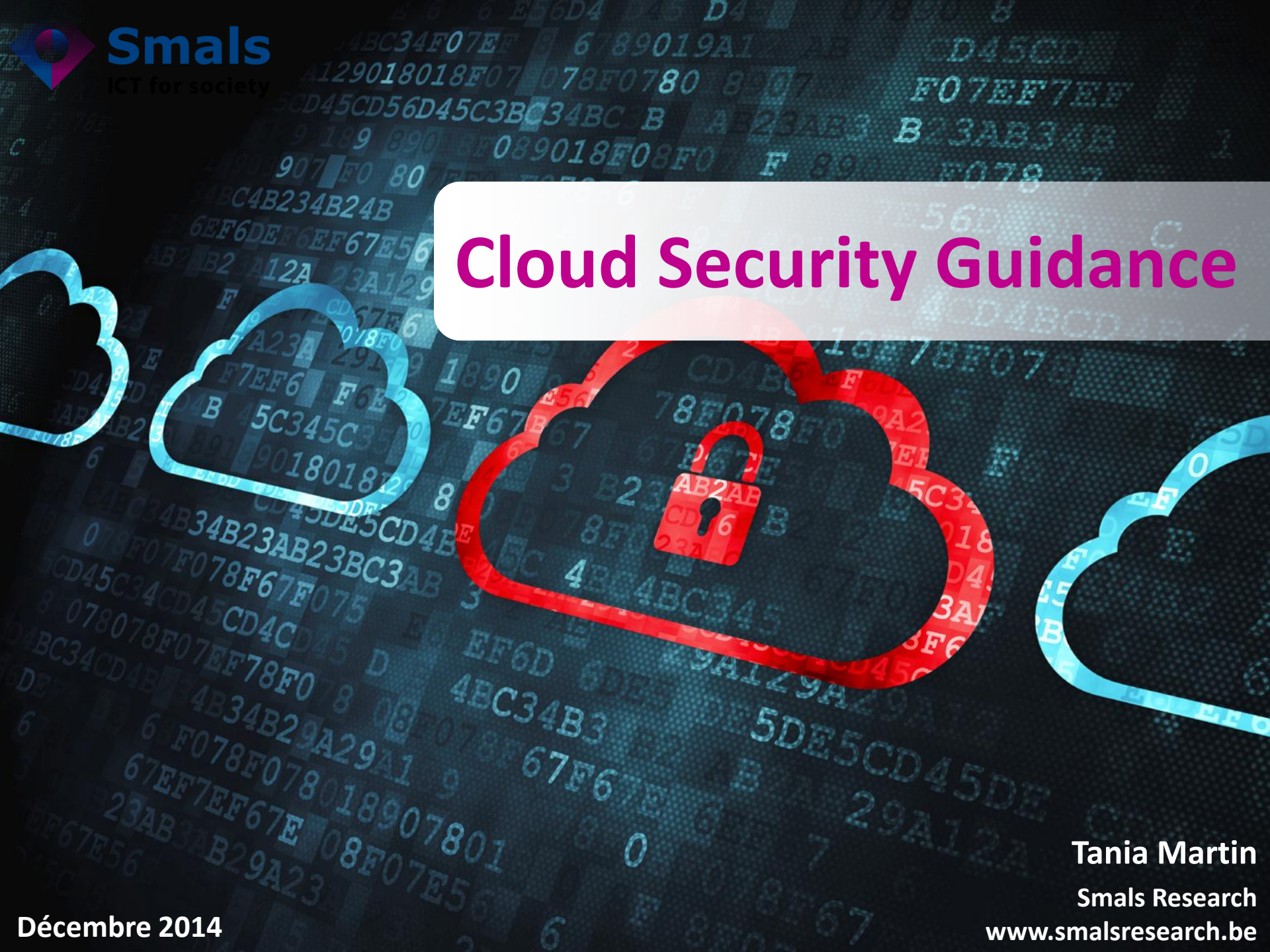


Cloud Security Guidance

Tania Martin
Smals Research
www.smalsresearch.be

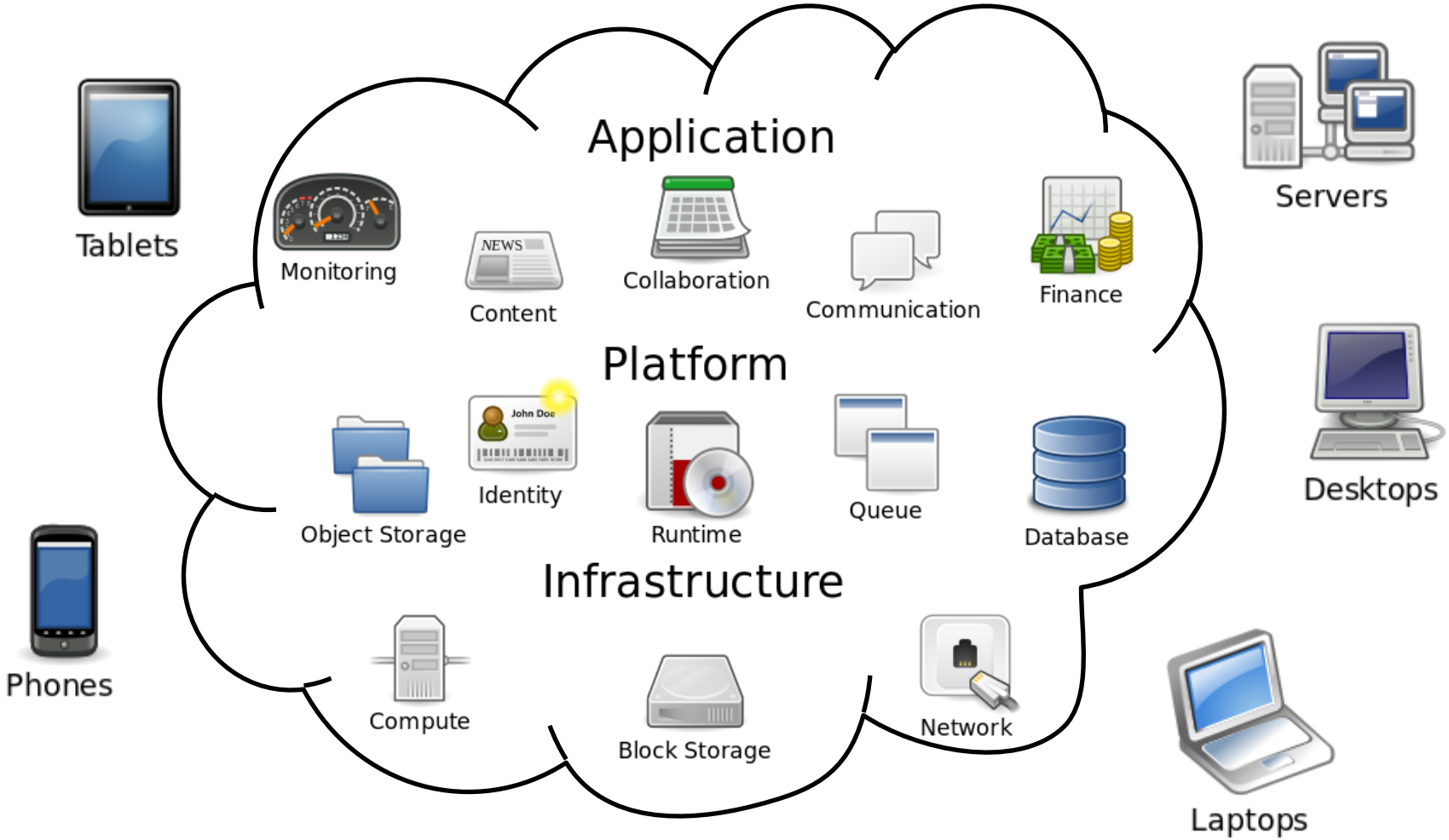
Décembre 2014

Agenda

1. Le cloud et sa sécurité
2. Modèle d'évaluation
   - Governance
   - Identity and access management
   - IT security
   - Operational security
3. Exemple: Dropbox for Business
4. Choisir un service cloud
5. Conclusion

Le cloud et sa sécurité

Aperçu du cloud



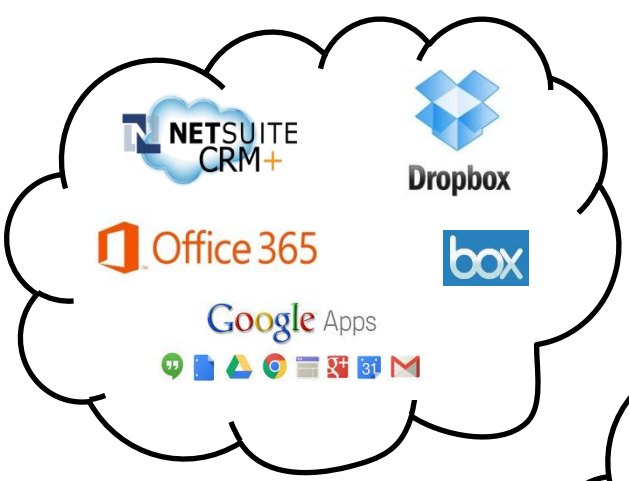
Modèles de service cloud

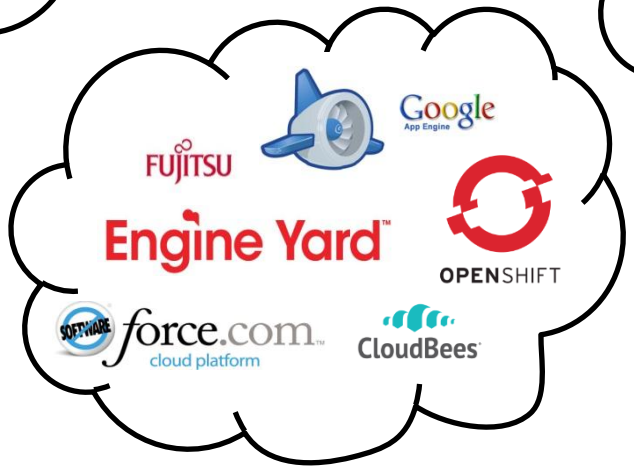
SaaS

PaaS

IaaS

REF





Voc: CSP (Cloud Service Provider)

5 caractéristiques essentielles

broad network access	**rapid elasticity**	**measured service**	**on-demand self-service**	**resource pooling**

- Accès au service via tout type de machine
- Service quasi-automatiquement approvisionné
- Optimisation automatique des ressources
- Self-service de l'utilisateur
- Ressources partagées par plusieurs tenants

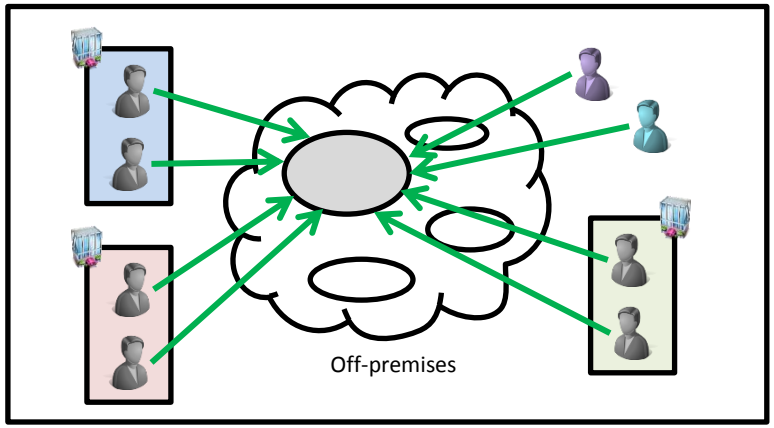
Voc: *tenant* = client (entreprise/particulier)
Ref: NIST Special Publication 800-145 REF

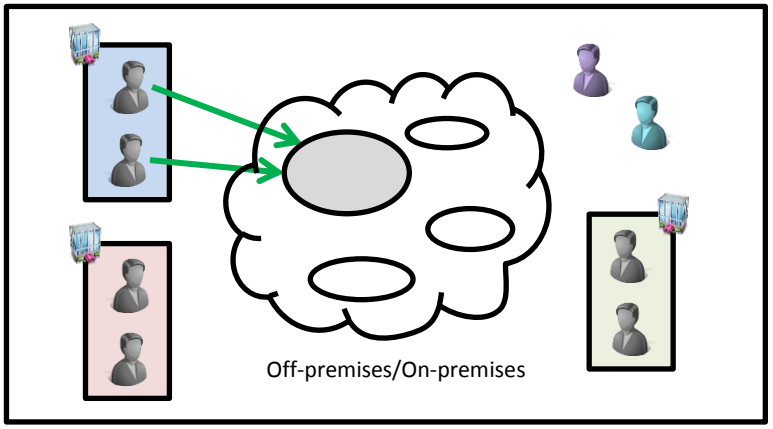
Modèles de déploiement

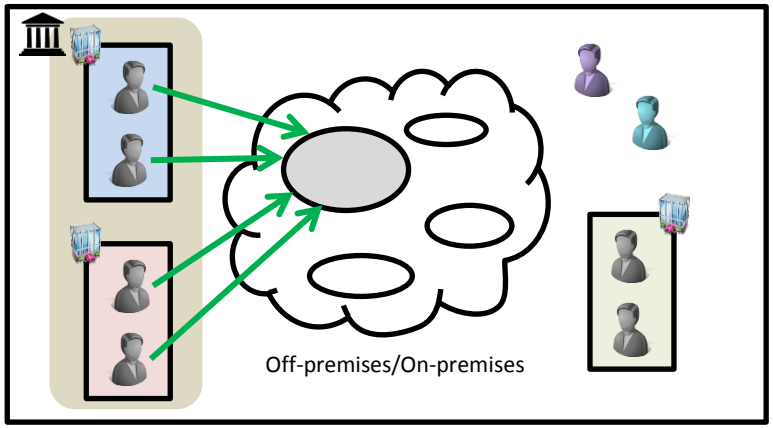
Public

Community

Private







Voc: *off-premises* = hors-site
on-premises = sur-site

Et la sécurité du cloud dans tout ça?

Le cloud: safe & secure?

Usage

- Stockage de codes source

Attaque

- Prise de contrôle de l'interface admin (sous Amazon WS)
- Effacement des données (backup compris)

A retenir

- Contrôler la chaine de sous-traitance
- Bonne séparation des rôles/pouvoirs

Le cloud: safe & secure?

amazon web services™ | EC2

Usage

- Location de serveur
- Création de machines virtuelles

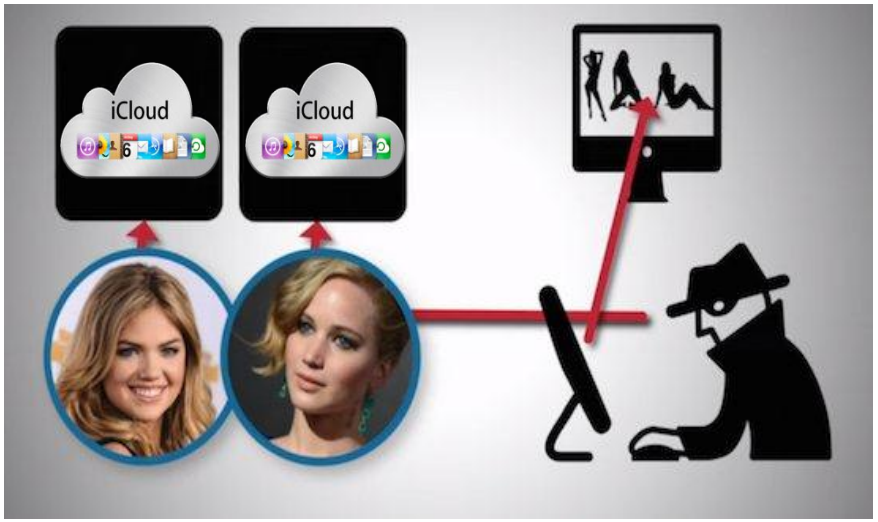
Attaque

- Auto update des nouveaux serveurs est **DESACTIVEE** par défaut
- Image serveur de Windows 2003 date d'octobre 2009

A retenir

- Produits toujours up-to-date
- Security-by-design

Le cloud: safe & secure?



Usage

- Stockage de données
- Email + agenda

Attaque

- Faille de conception dans « Find my iPhone »
- Brute force sur les passwords
  (sans alerte ni lockout)

A retenir

- Authentification 2-factor indispensable pour des données sensibles
- Avoir un bon mot de passe

Et la sécurité du cloud dans tout ça?

- **Pas 100%** assurée par les services cloud
- Problématique pour des **données sensibles**
  - ➢ Surtout dans notre contexte « sécurité sociale et eHealth»

Evaluer la sécurité d'un service cloud avant utilisation

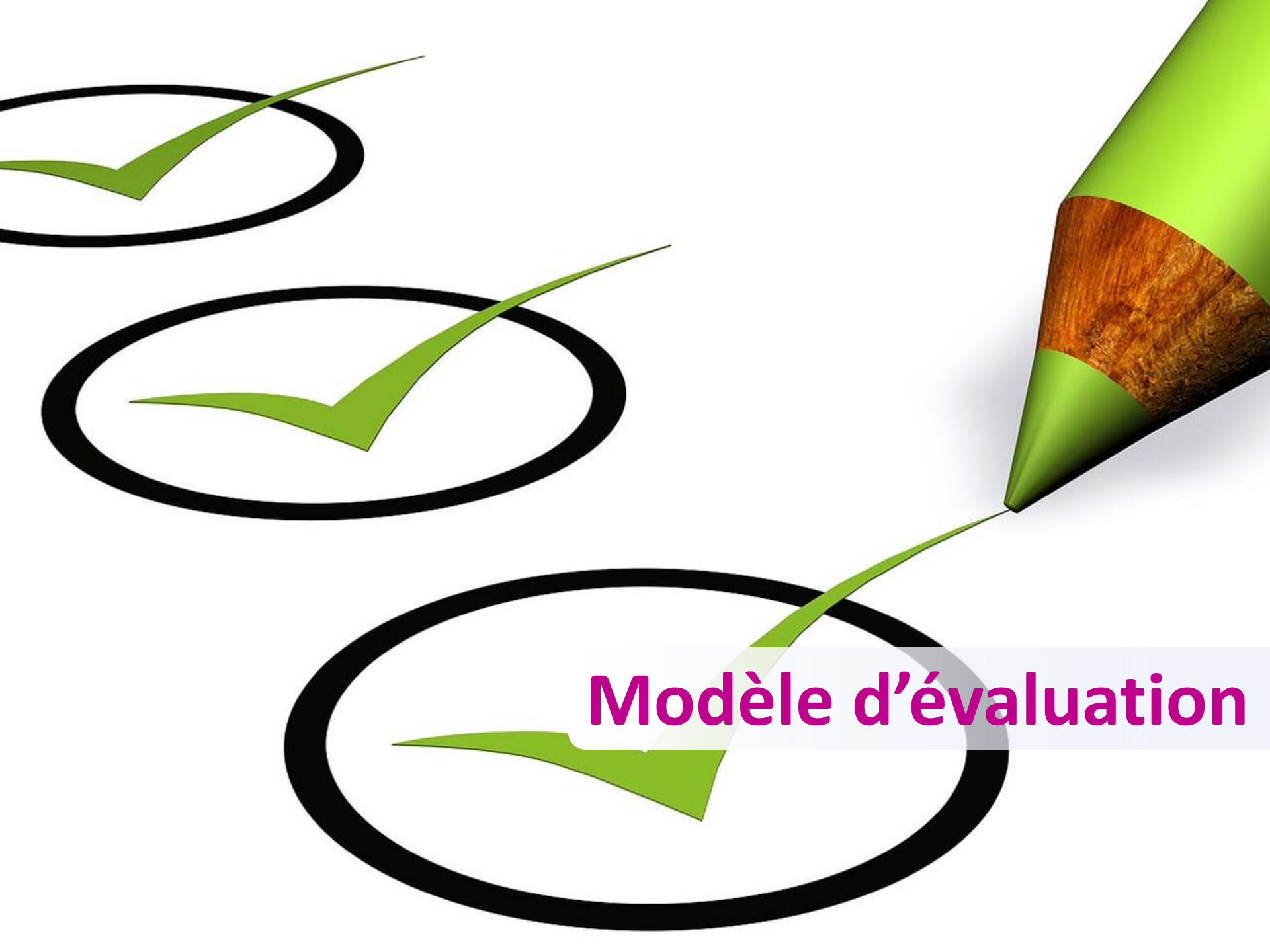
Durant cette présentation…

Parcourir les **points-clé** de la sécurité du cloud

Modèle d'évaluation de sécurité des services cloud

+

Dropbox for Business



Modèle d’évaluation

But du modèle

Aide pour les experts en sécurité

Modèle pratique

« Quel service cloud puis-je utiliser si je souhaite y mettre un type X de données ? »

But du modèle

Aide pour les experts en sécurité

Modèle pratique

« Quel service cloud puis-je utiliser si je souhaite y mettre un type X de données ? »

Eliminer/filtrer les pistes non fructueuses

Sélectionner les candidats potentiels

Composantes du modèle

4 critères majeurs

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

Cloud Policy de la sécurité sociale

Type de données

2 questionnaires

- Evalue le niveau de sécurité d'un service cloud
- Evalue la possibilité d'utiliser un service cloud

Composantes du modèle

4 critères majeurs

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

Cloud P
sé
pe de données

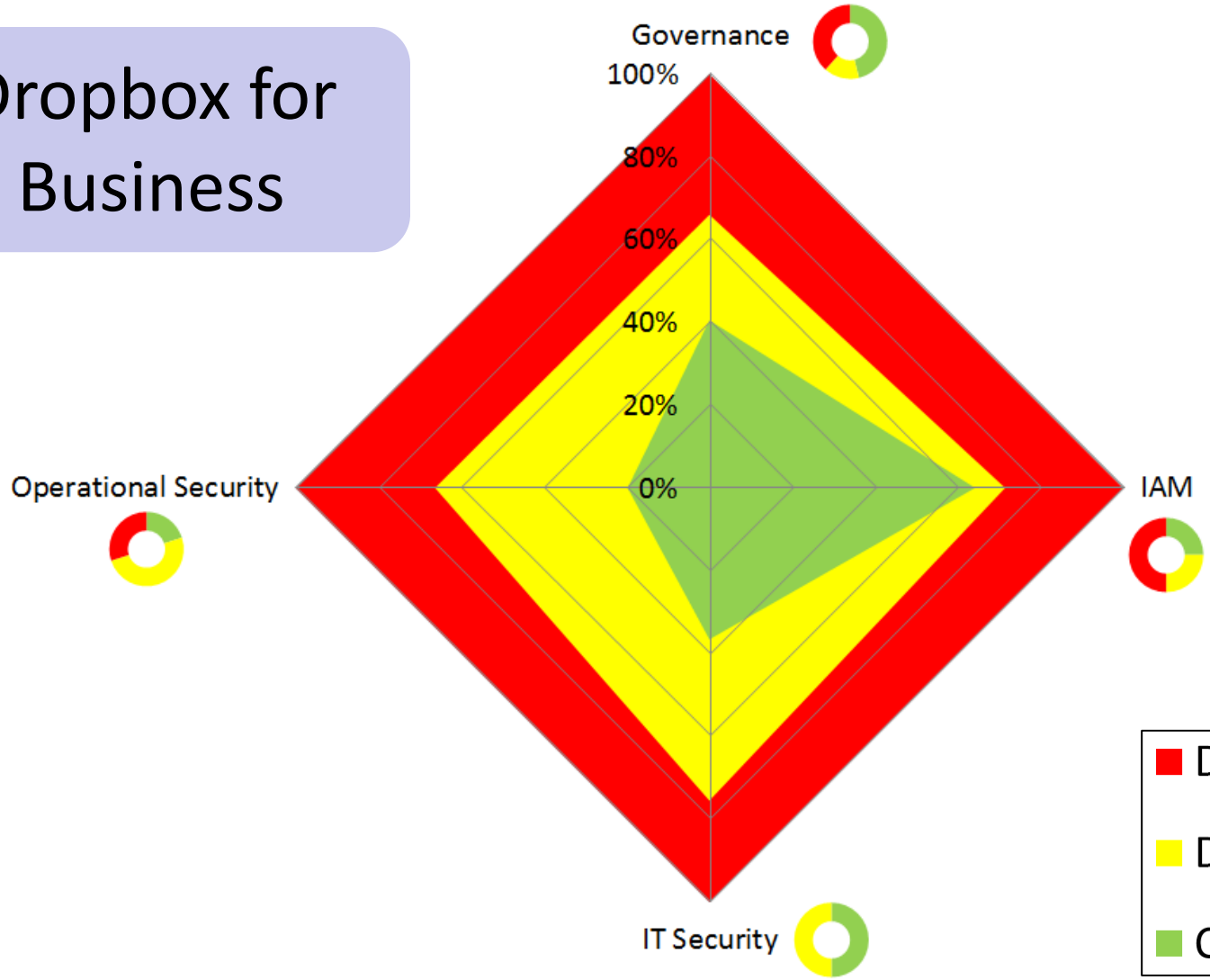
Seul un expert humain doit juger du résultat

2 questionnaires

- Evalue le niveau de sécurité d'un service cloud
- Evalue la possibilité d'utiliser un service cloud

A quoi ressemble le modèle?

Dropbox for Business

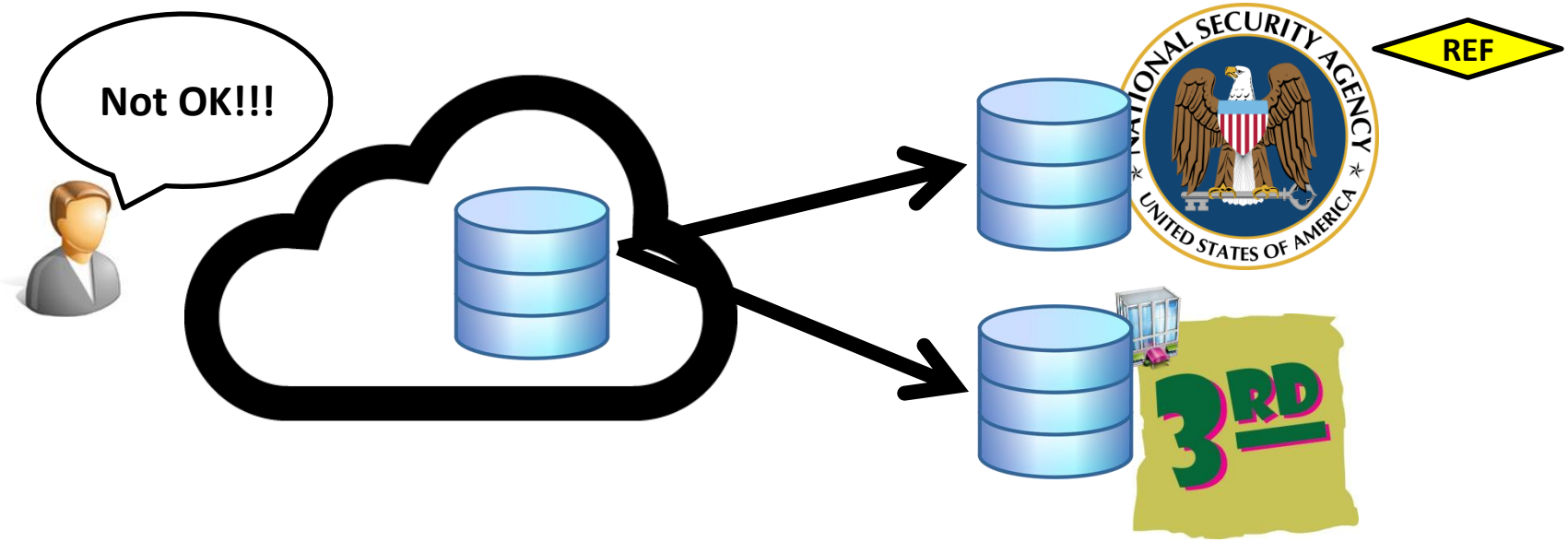


Governance

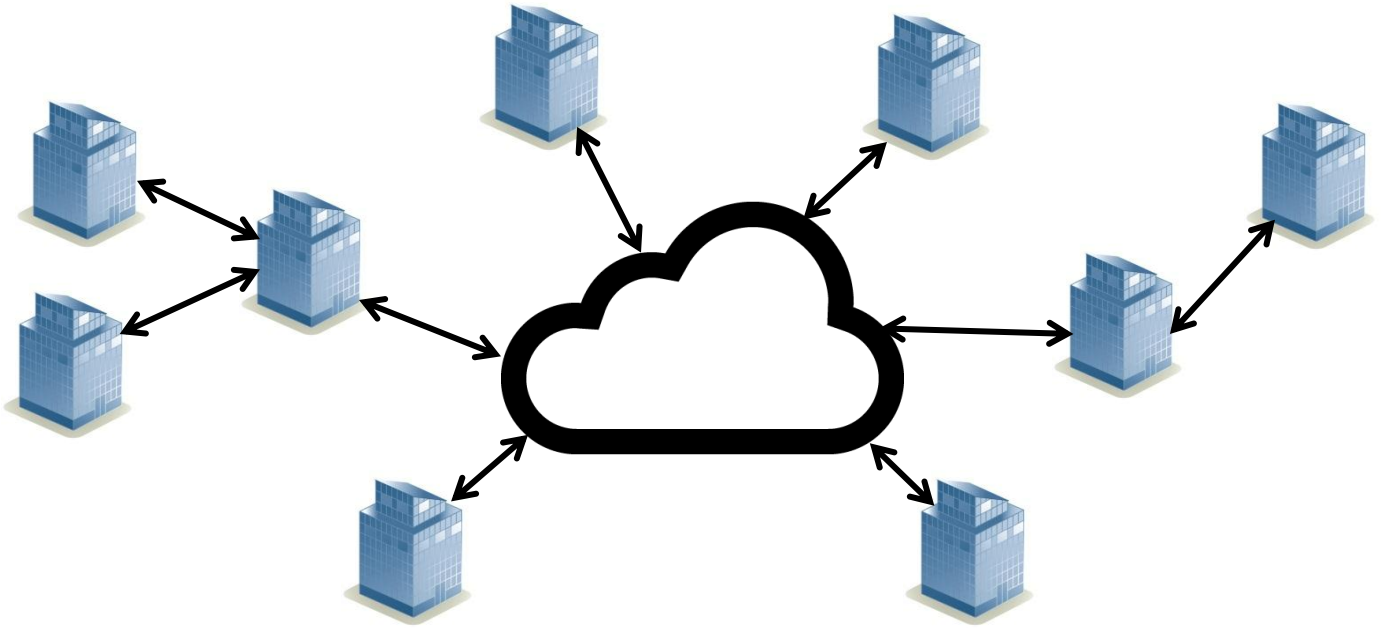
Implications légales

Quelles lois appliquent sur les données?



Chaine de sous-traitance

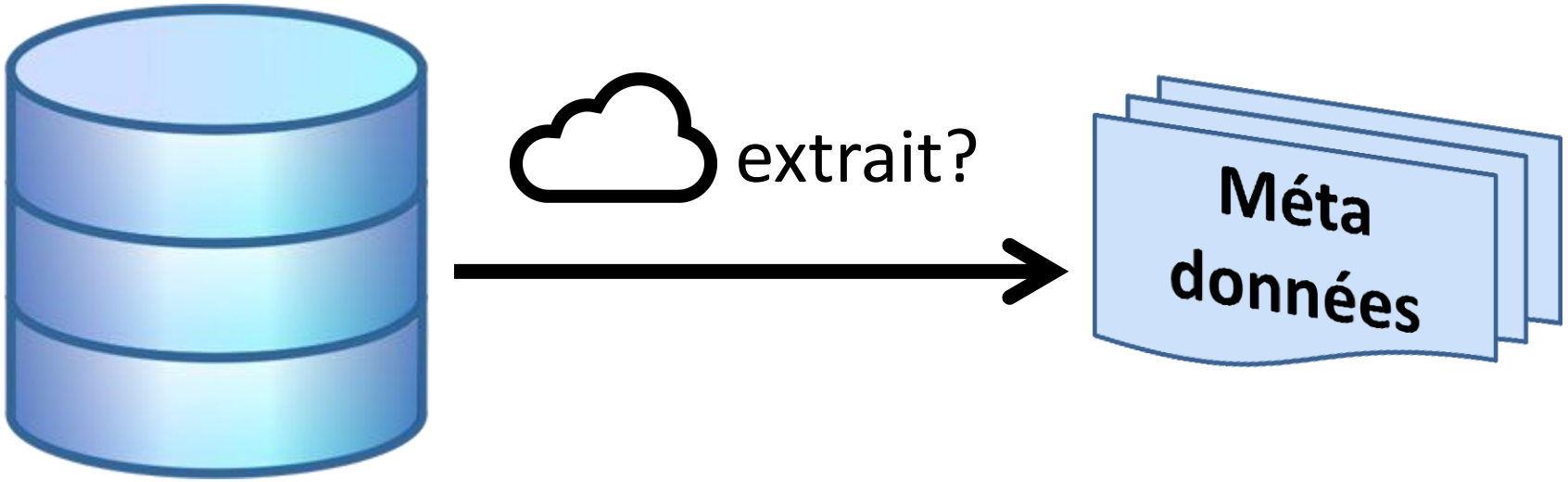


CSP toujours responsable de ses engagements contractuels?

Audit

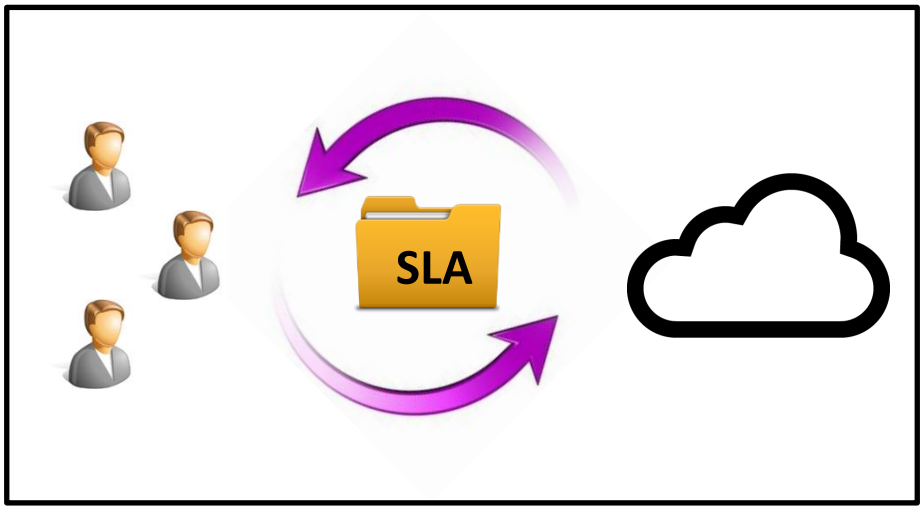
Tous les 6 mois **10 /10** Tous les ans

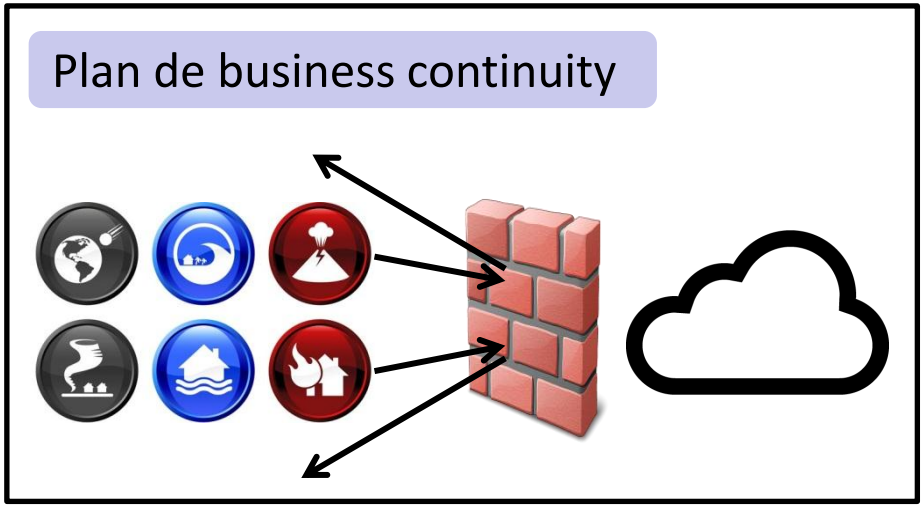
Méta-données

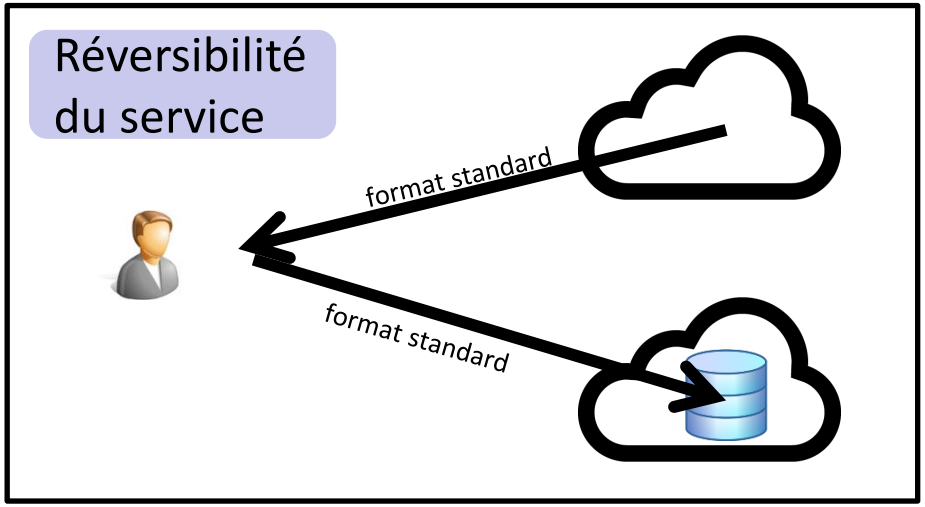


Méta-données utilisées seulement pour le service cloud?

Qualité du service







Exemple: Dropbox for Business

Exemple: Dropbox for Business

	Category Title	Score	Minimal weighted score	Maximal weighted score
1	**Governance**		**41%**	**66%**
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

Exemple: Dropbox for Business

Worst case **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%

Exemple: Dropbox for Business

	Score	Minimal weighted score	Maximal weighted score
		41%	66%
		6%	11%
	Unknown	5,25	21
	US	10,5	10,5
	Unknown	0	8
	Yes	0	0
	Yes	0	0
	Yes	8	8

Exemple: Dropbox for Business

	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%

Governance: à retenir

Quelles lois?

Sous-traitance fiable?

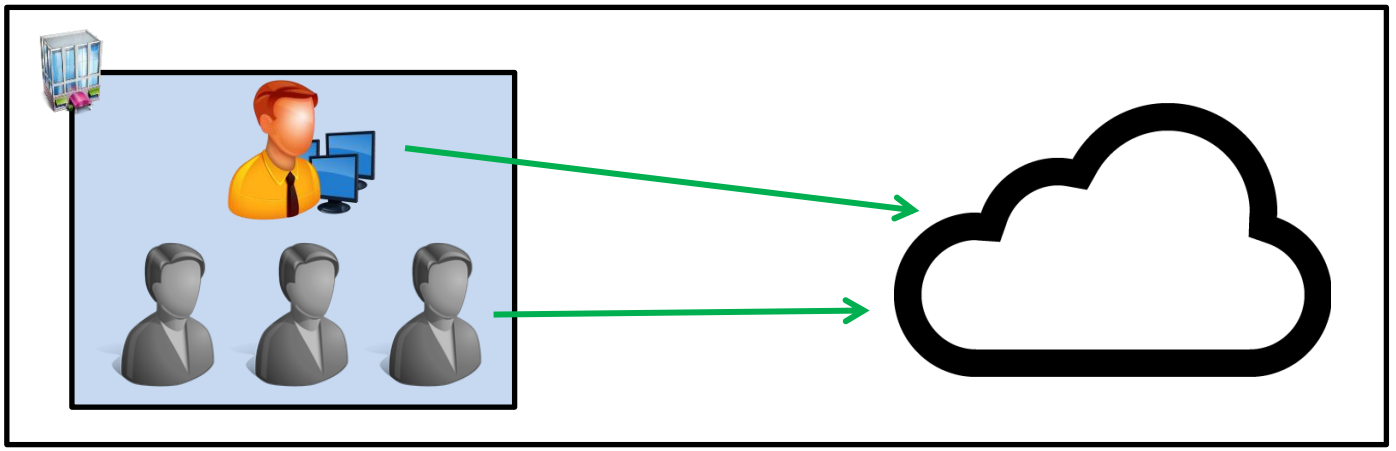
Audit régulier?

Non abus des méta données?

Bonne qualité du service?

Identity and Access Management

Niveau d'authentification



Username + Password

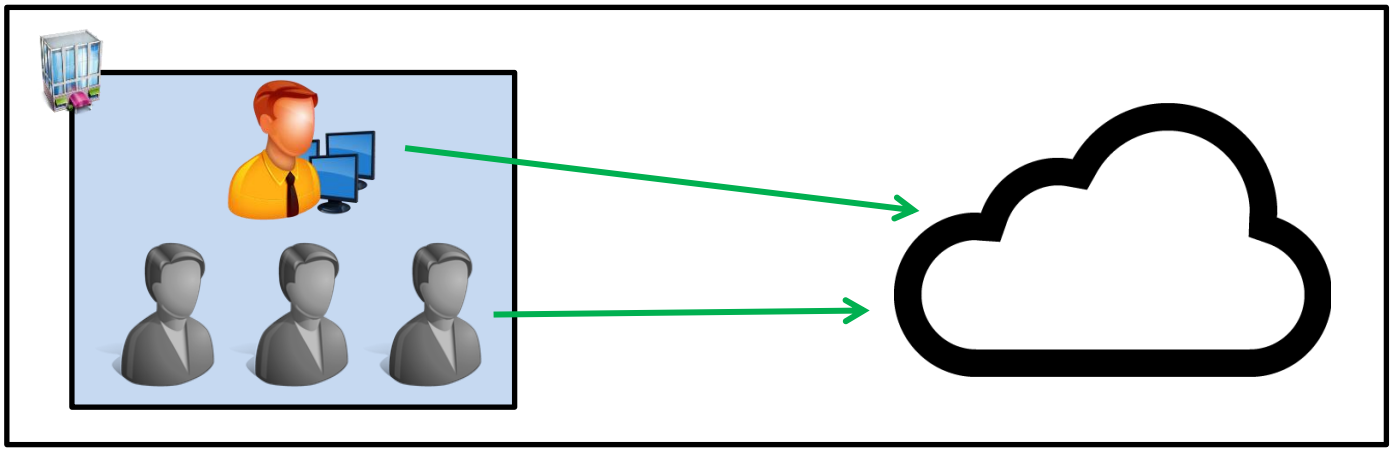
Username + Password + Token

Username + Password + Certificat

Username + Password + Certificat/Token + Location

10 /10

Niveau d'authentification



Authentification « 2-factor »

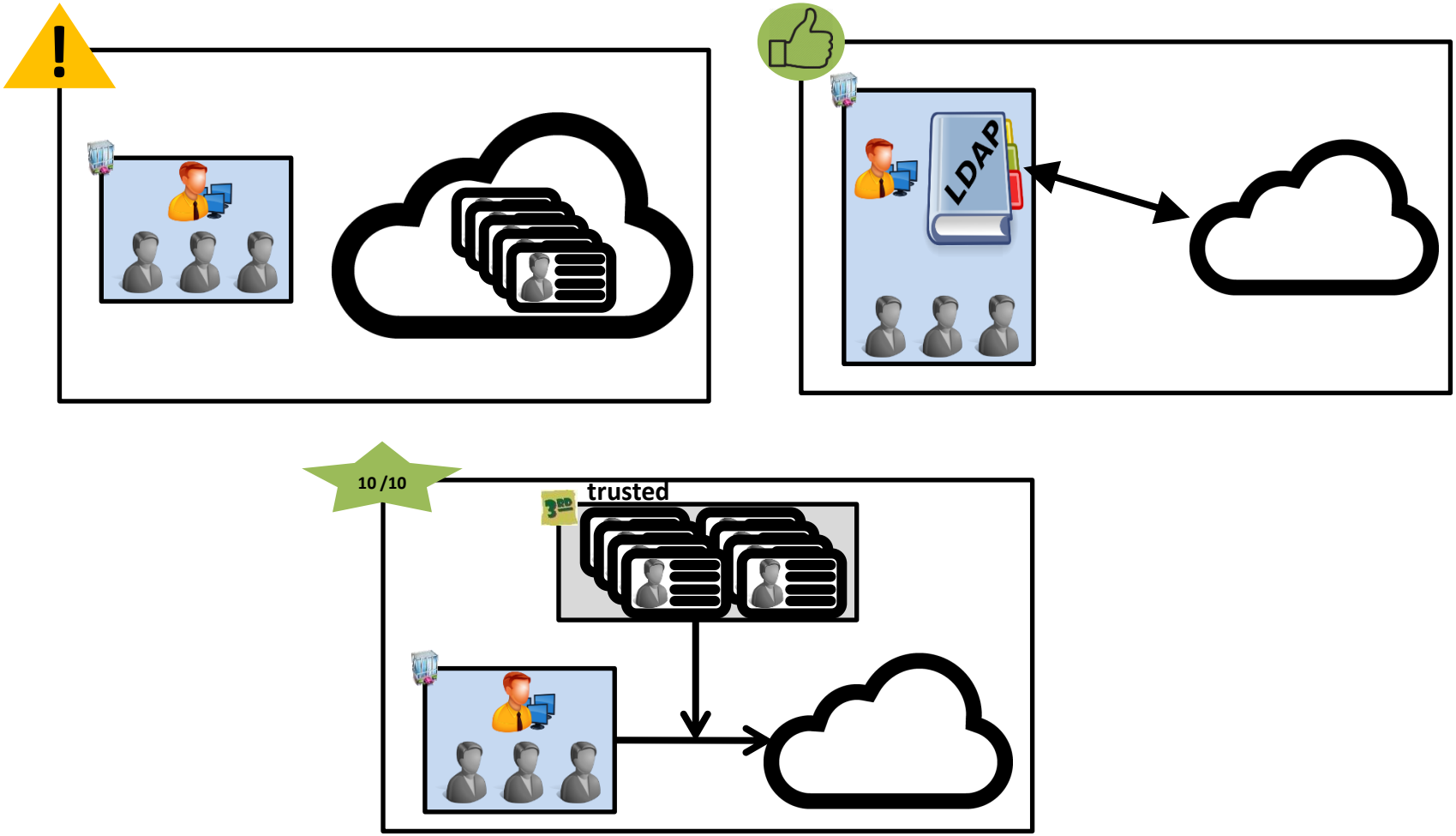
Username + Password + Token

Username + Password + Certificat

Username + Password + Certificat/Token + Location

10 /10

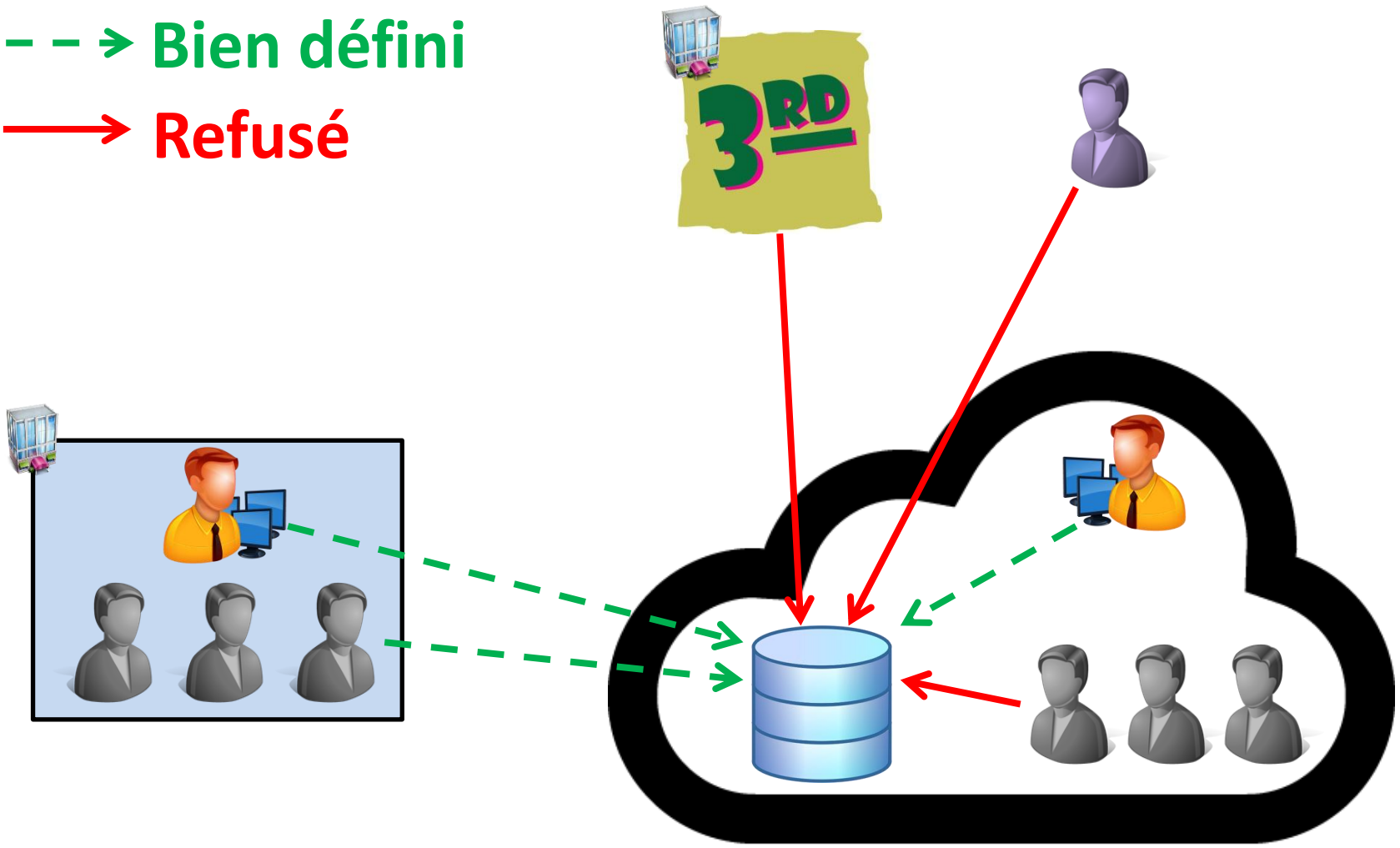
Gestion des utilisateurs



Accès aux données

- - → Bien défini

⟶ Refusé



Exemple: Dropbox for Business

	Category Title	Score	Minimal weighted score	Maximal weighted score
2	**Identity and Access Management (IAM)**		**64%**	**72%**
2.1	Authentication level		31%	31%
2.1.1	Are the different authentication mechanisms to access the cloud service documented?	Yes	36	36
2.1.2	What is the strongest authentication mechanism to access the cloud service as a tenant system administrator offered by the CSP?	Username + password + token (e.g. with SMS)	12	12
2.1.3	What is the strongest authentication mechanism to access the cloud service as a tenant user offered by the CSP?	Username + password + token (e.g. with SMS)	12	12
2.1.4	Are password policy enforcements well-defined and implemented?	Yes	16	16
2.1.5	Are secure password reset procedures well-defined and implemented?	Yes	16	16
2.2	User management		33%	33%
2.2.1	Who performs the tenants' user management?	Tenant system administrator	22	22
2.2.2	Is the integration with the IAM of the tenant possible?	Yes	35	35
2.2.3	Is the integration with an ID-provider possible?	Yes	28	28
2.2.4	Are the identification and/or authentication of the devices used to access the cloud service possible as additional enforcement of the IAM?	Yes	15	15
2.3	Access management		0%	7%
2.3.1	Does the CSP document how the IAM of its employees related to the tenants' assets is performed?	No	0	0
2.3.2	Is data access of {tenant user, tenant system administrator, CSP system administrator} clearly defined?	No	0	0
2.3.3	Is data access of {CSP employees, third party, other tenants} denied?	No	0	0
2.3.4	Is IAM management and data access logging clearly defined and available?	Unknown	0	22

Exemple: Dropbox for Business

	Score	Minimal weighted score	Maximal weighted score
nt (IAM)		64%	72%
		31%	31%
ented?	Yes	36	36
tenant system	Username + password + token (e.g. with SMS)	12	12
tenant user offered	Username + password + token (e.g. with SMS)	12	12
	Yes	16	16
	Yes	16	16
		33%	33%
	Tenant system administrator	22	22

IAM: à retenir

Authentification « 2-factor »?

Gestion des utilisateurs controlée?

Accès aux données bien défini?

Pause

Agenda

1 Le cloud et sa sécurité

2 Modèle d'évaluation

- Governance
- Identity and access management
- IT security
- Operational security

3 Exemple: Dropbox for Business

4 Choisir un service cloud

5 Conclusion


IT Security

Standards de sécurité

OS

- Anti-virus, anti-malwares
- Patch management process
- Environnement d'acceptation

Infra

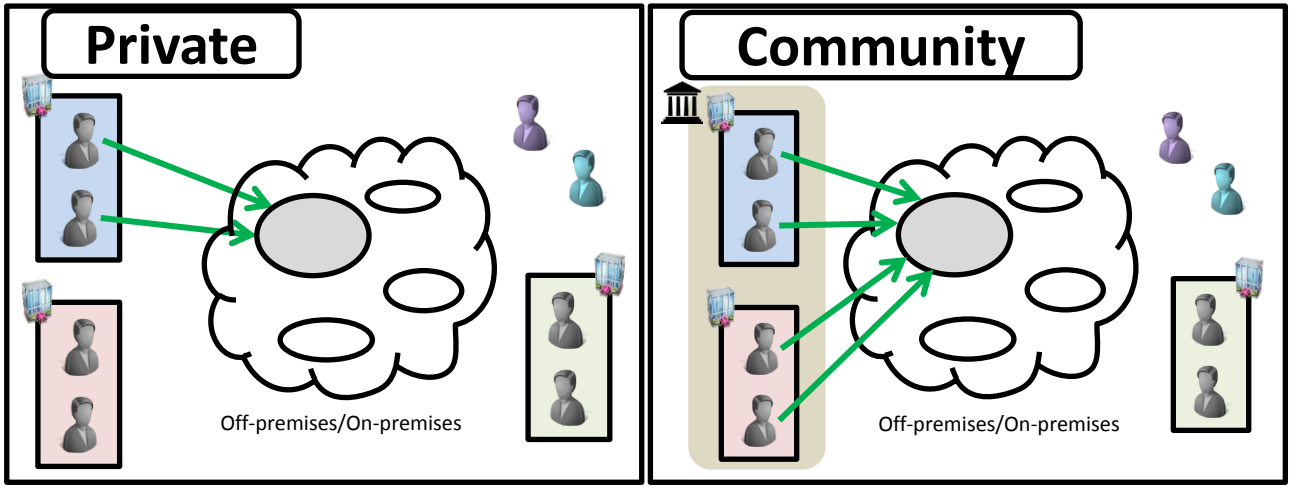
physique + virtuelle

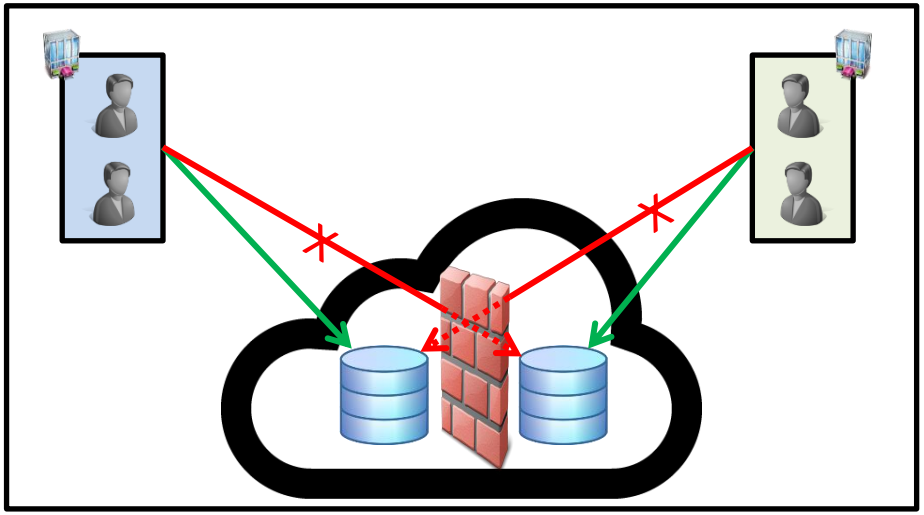
- Sécurité réseau: firewall, APT detection tools REF
- Monitoring: IDS/IPS, file integrity
- Détection des fuites: DLP
- Protection des hyperviseurs et consoles d'administration
- Effacement securisé des données: crypto wiping, démagnétisation

Interface

- Intégrité et sécurité des données en input et output
- API développées en suivant les standards (e.g. OWASP) REF

Ségrégation des données





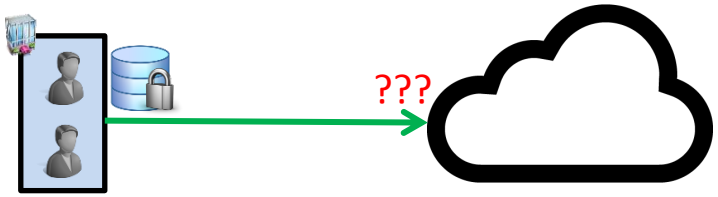
Point très important
MAIS
souvent pas documenté

Cryptographie

Crypto forte

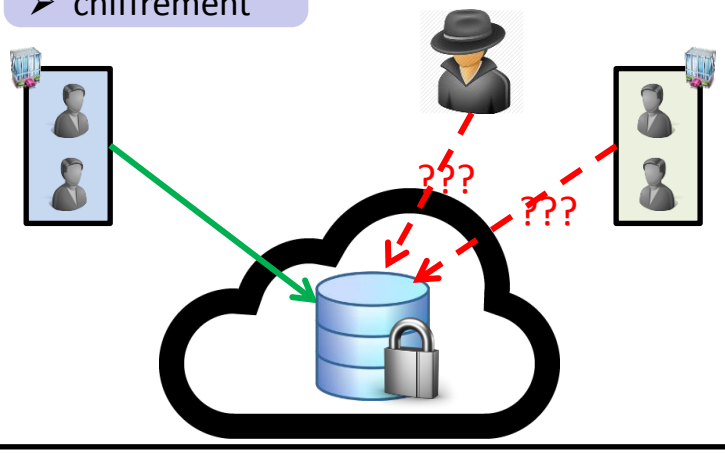
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Confidentialité vis-à-vis du CSP
- chiffrement

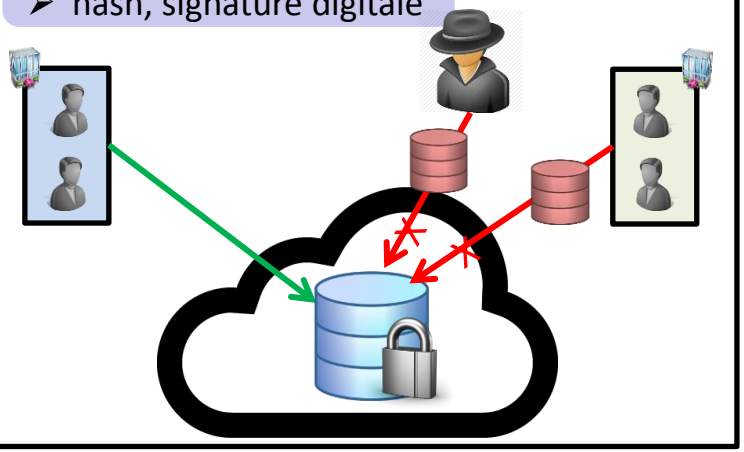


Outils: boxcryptor REF

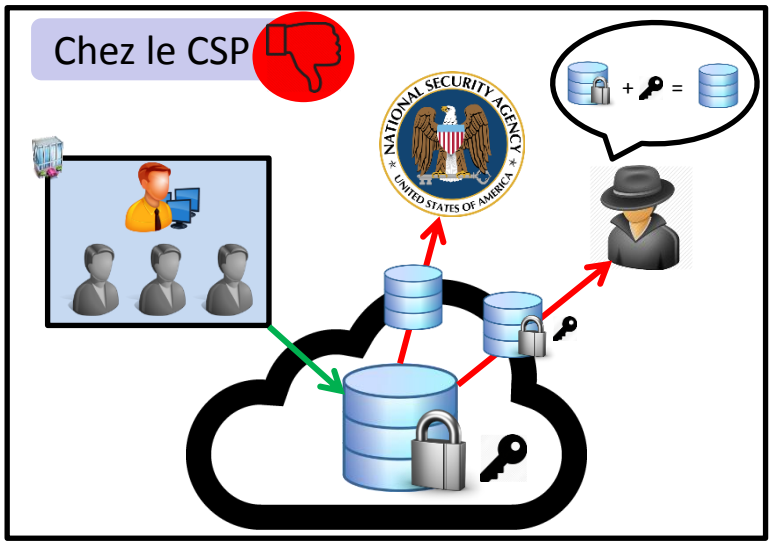
Confidentialité
- chiffrement

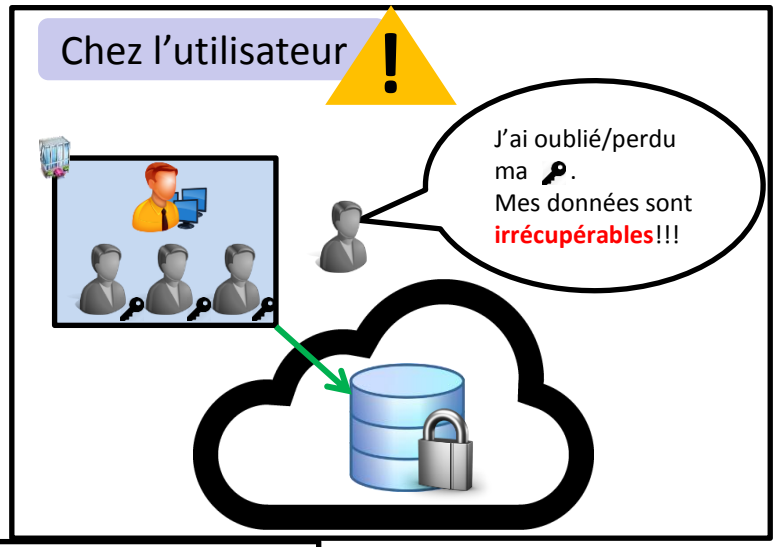


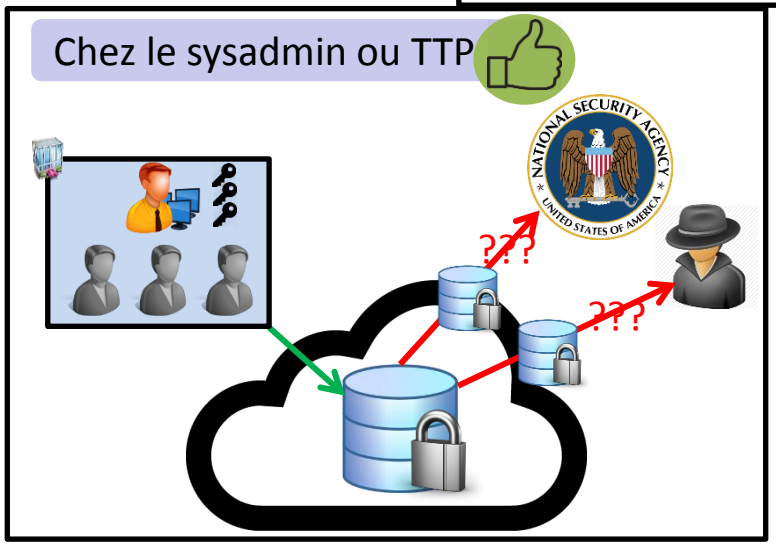
Intégrité
- hash, signature digitale



Gestion des clés







Exemple: Dropbox for Business

	Category Title	Score	Minimal weighted score	Maximal weighted score
3	**IT Security**		**37%**	**76%**
3.1	Segregation of data		0%	16%
3.1.1	Can the cloud service be provided as private or community?	No	0	0
3.1.2	In a multi-tenant system, are the data of the respective tenants segregated/isolated in such a way that it is technically impossible for any user of tenant A to receive entitlements to data of tenant B?	Unknown	0	62
3.2	Interface security		7%	12%
3.2.1	Are APIs developed in accordance with standards?	Unknown	0	40
3.2.2	Are data integrity and security ensured for input and output?	Yes	60	60
3.3	Infrastructure and virtualization security		14%	22%
3.3.1	Is the access to hypervisors management functions and administration consoles highly controlled?	Unknown	0	14
3.3.2	Is data securely deleted from all storage media when the user's or tenant's account is deleted?	Yes	17	17
3.3.3	Does the CSP take defense-in-depth approach to wired or wireless network security?	Yes	23	23
3.3.4	Are sufficient controls in place at the hardware and virtual (if applicable) levels?	Yes	23	23
3.3.5	Are security mechanisms to prevent and analyze data leakage at the hardware and virtual (if applicable) levels available?	Unknown	0	23
3.4	OS security (only for SaaS and PaaS cloud services)		10%	18%
3.4.1	Are tools to prevent, detect and mitigate viruses and malwares at server stations available?	Yes	40	40
3.4.2	Is hardening process performed on the server stations?	Unknown	0	30
3.5	Cryptography		6%	9%
3.5.1	Who is in charge of the key management?	CSP	2,7	2,7
3.5.2	Has the key management been defined through policies and procedures as required by the ISO/IEC27002:2013 standard?	No	0	0
3.5.3	Have the cryptographic mechanisms used for the cloud service been defined to guarantee adequate cryptographic strength?	Yes	13	13
3.5.4	Does the CSP use HSMs (Hardware Security Modules) for the protection of keys?	No	0	0
3.5.5	Is client-side encryption of data possible?	No	0	0
3.5.6	Is data-at-rest confidentiality ensured?	Yes	19	19
3.5.7	Is data-at-rest integrity ensured?	Unknown	0	19

Exemple: Dropbox for Business

	Score	Minimal weighted score	Maximal weighted score
		37%	76%
		0%	16%
	No	0	0
in such a way that it is technically	Unknown	0	62
		7%	12%
	Unknown	0	40
	Yes	60	60
		14%	22%
nly controlled?	Unknown	0	14
s deleted?	Yes	17	17
?	Yes	23	23
	Yes	23	23
irtual (if applicable) levels available?	Unknown	0	23

IT security: à retenir

Standards de sécurité en place?

Ségrégation des données?

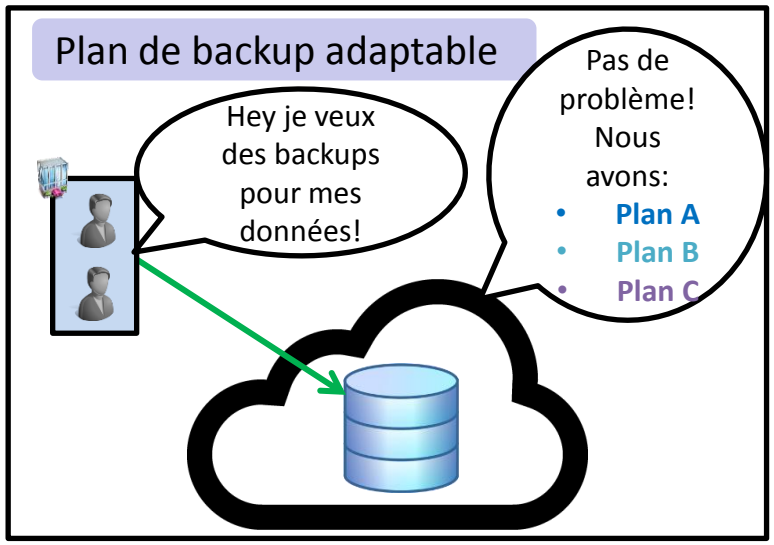
Standards de cryptographie utilisés?

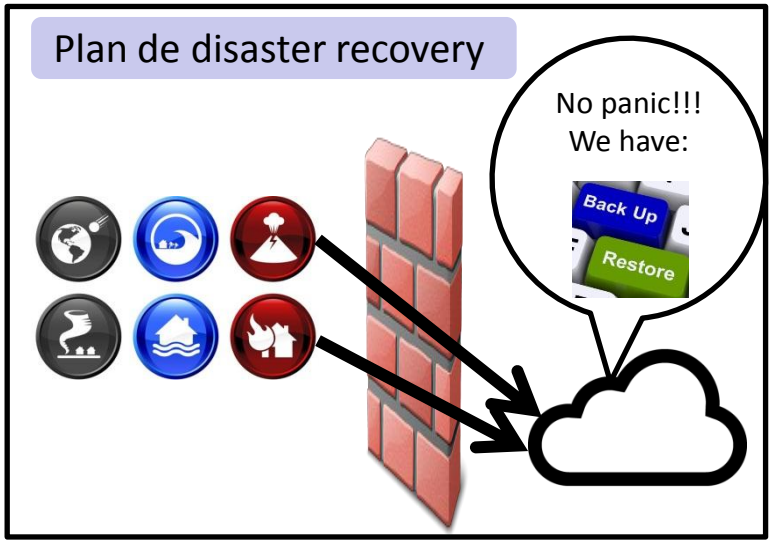
Confidentialité et intégrité des données?

Gestion des clés crypto chez le sysadmin?

Operational Security

Backup et disaster recovery





Quelques chiffres sur les RTO et RPO

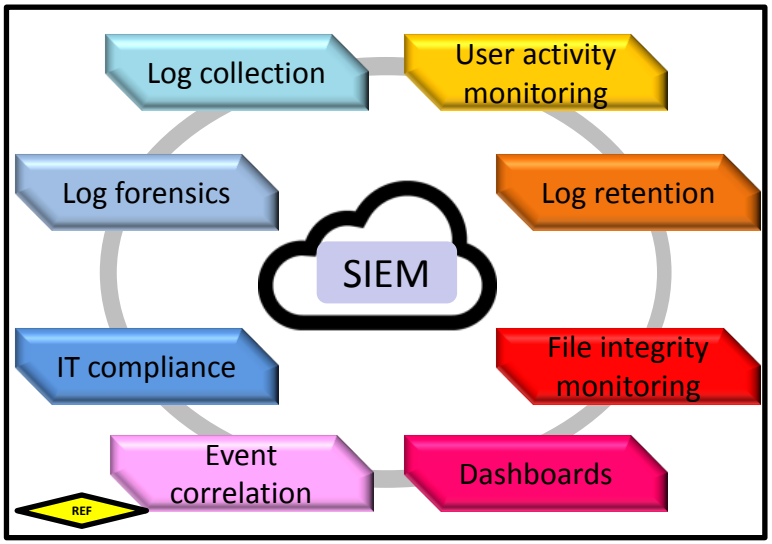
≈ 1 semaine

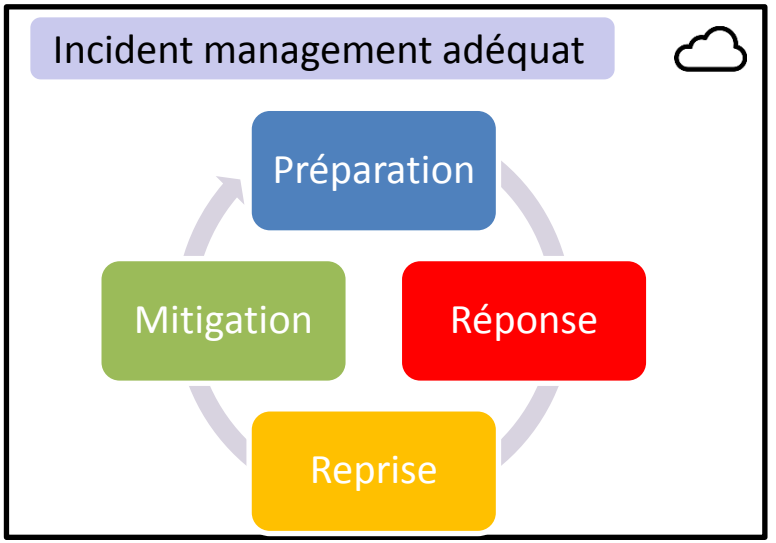
≈ 1 jour

≈ 1 heure

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

Incident management





Exemple: Dropbox for Business

	Category Title	Score	Minimal weighted score	Maximal weighted score
4	**Operational Security**		**20%**	**66%**
4.1	Backup and disaster recovery		0%	14%
4.1.1	Can the backup retention plan be defined by the tenant?	No	0	0
4.1.2	Are backup controls defined and adequate?	No	0	0
4.1.3	What it the RTO (Recovery Time objective) of the cloud service?	Unknown	0	15
4.1.4	What it the RPO (Recovery Point objective) of the cloud service?	Unknown	0	15
4.1.5	Are tenants able to perform recovery tests, including reporting?	Unknown	0	10
4.2	Incident management		20%	20%
4.2.1	Does the CSP have a SIEM (Security Information and Event Management) for analyzing the security alerts and data logs?	No	0	0
4.2.2	Does the CSP have an adequate incident management procedure for managing and minimizing the impact of security incidents on tenants' data?	Yes	40	40
4.2.3	Does the CSP have adequate security policies and procedures regarding CSP employee security?	Yes	20	20
4.3	Vulnerability management		0%	33%
4.3.1	Is there a documented patch management process implemented in the cloud service?	Unknown	0	50
4.3.2	Does the CSP test patches in acceptance environments prior to deployment?	Unknown	0	50

Exemple: Dropbox for Business

	Score	Minimal weighted score	Maximal weighted score
		20%	66%
		0%	14%
	No	0	0
	No	0	0
	Unknown	0	15
	Unknown	0	15
	Unknown	0	10
		20%	20%
alyzing the security alerts and	No	0	0
and minimizing the impact of	Yes	40	40
ployee security?	Yes	20	20

Operational security: à retenir

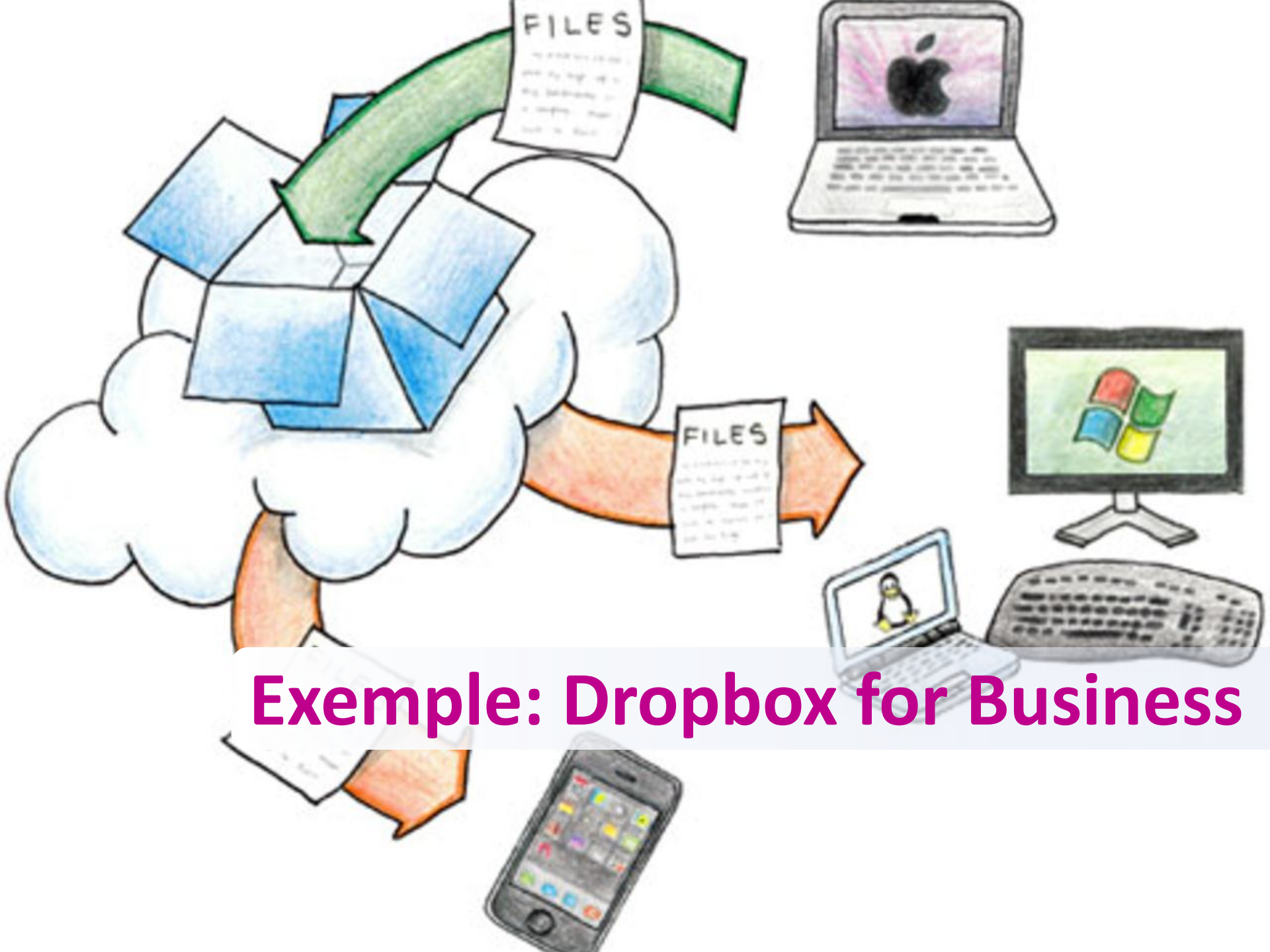
Plan de backup adaptable?

RTO et RPO < 1 jour?

SIEM?

Gestion d'incident adéquate?

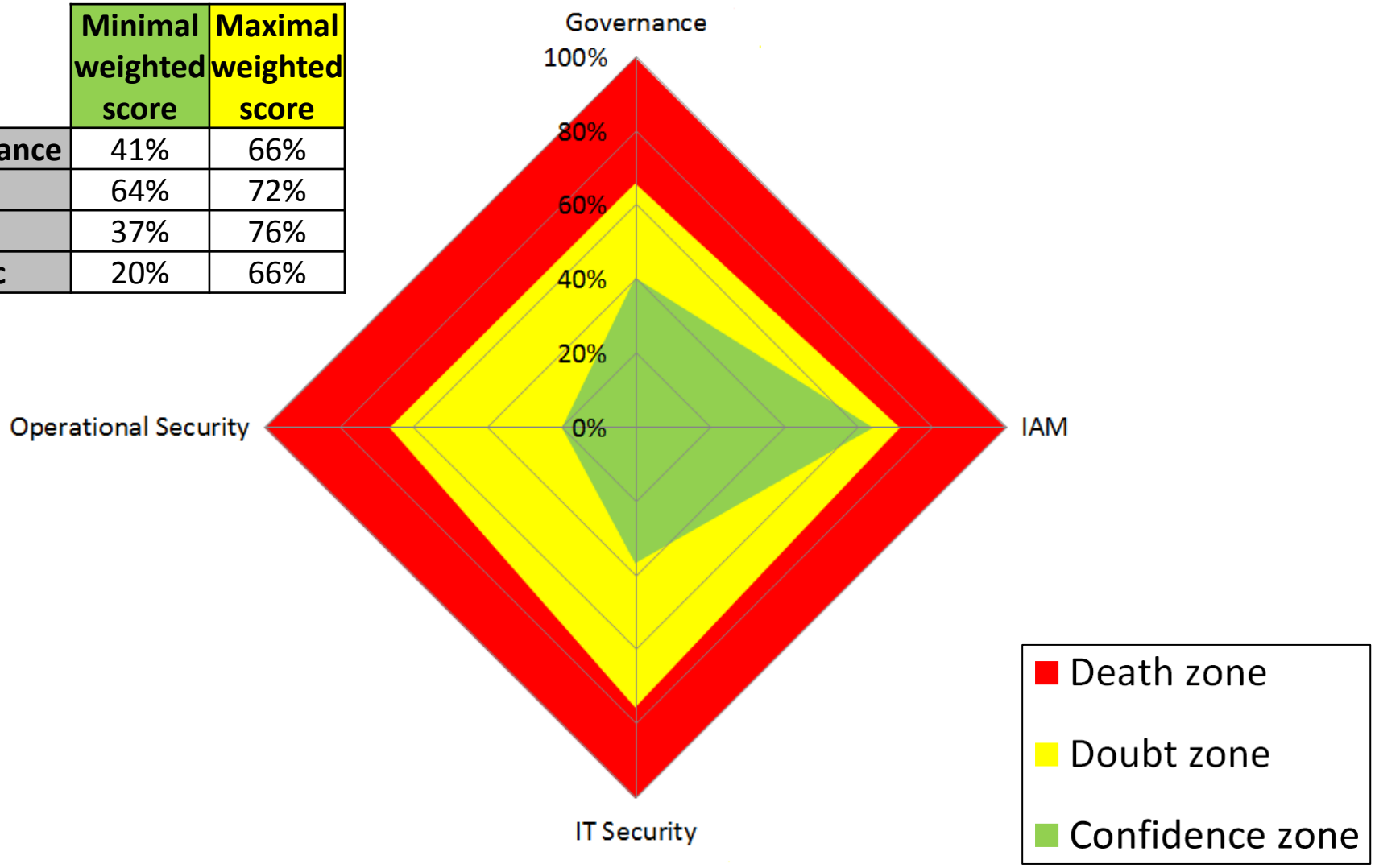
Formation sécurité des employés?



Exemple: Dropbox for Business

Résultat préliminaire de l'analyse

	Minimal weighted score	Maximal weighted score
Governance	41%	66%
IAM	64%	72%
IT Sec	37%	76%
Ope Sec	20%	66%



Cloud policy de la sécurité sociale

But?

- Etablit les **exigences de sécurité** quand une institution de la sécurité sociale envisage d'utiliser un service cloud

URL?

- QR code de l'URL

REF

Modèle?

- Chaque point est restitué dans le modèle
- Mais le modèle va un peu plus loin

Cloud policy dans le modèle

	Category Title	Score	Minimal weighted score	Maximal weighted score
1	**Governance**		**41%**	**66%**
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 dans le modèle

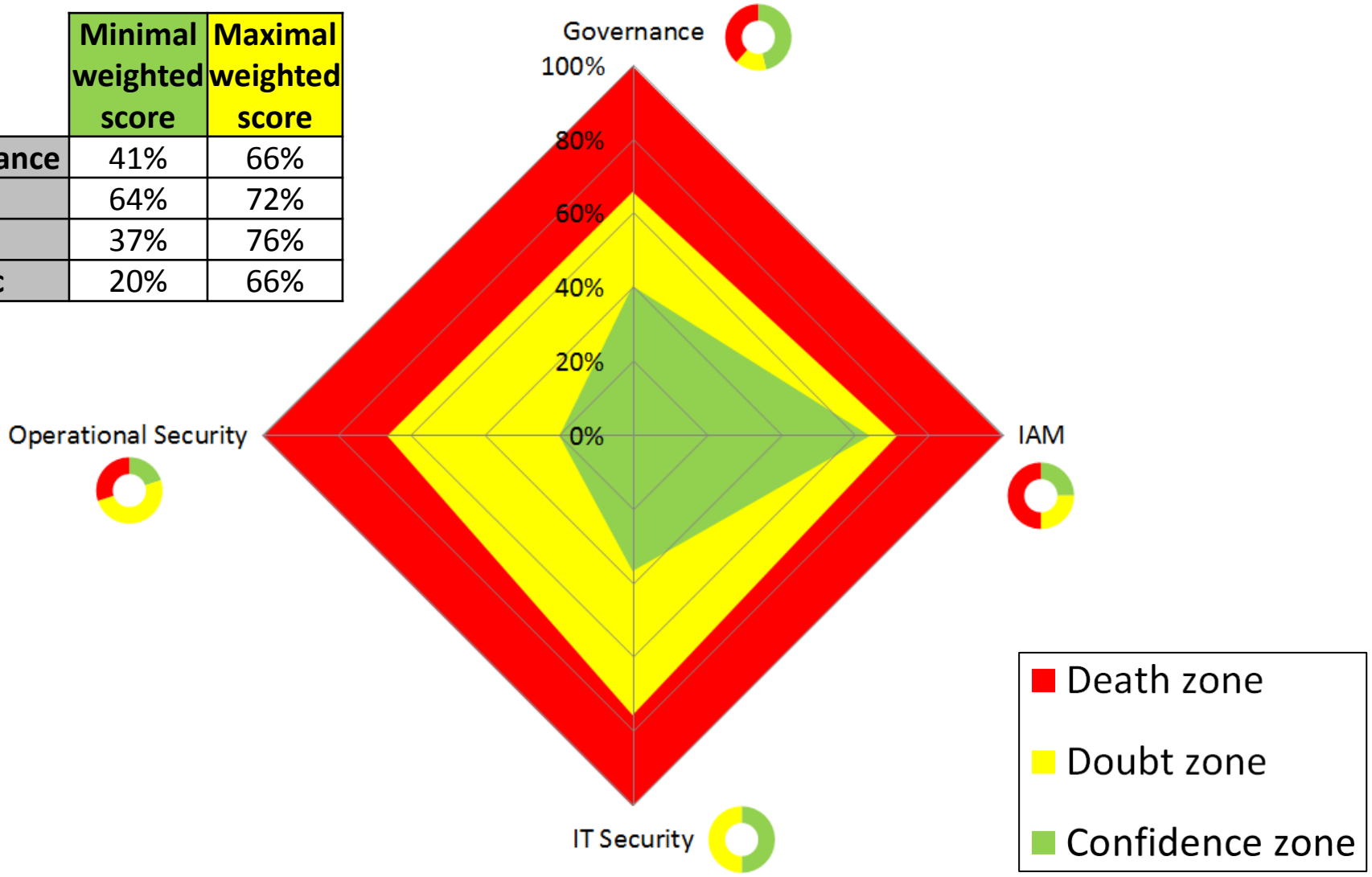
	Category Title	Score	Minimal weighted score	Maximal weighted score	Compliance with cloud policy
1	Governance		41%	66%	
1.1	Legal implication		6%	11%	
1.1.1	What is the physical location of data-at-rest?	Unknown	5,25	21	
1.1.2	Which jurisdiction is the CSP subject to?	US	10,5	10,5	
1.1.3	Can the CSP accomodate 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	X
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	X
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	V
1.2.3	If so, will the CSP inform the tenant of any change in the course of the contract?	Yes	20	20	V
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	V
1.3.2	If the cloud service is audited, are the scopes of the audits accurately defined?	Yes	32	32	V
1.3.3	At which time interval is the cloud service (including all its subcontractors) pen-tested?	1 year	5,95	5,95	V
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	V
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	X
1.4	Business continuity		0%	8%	
1.4.1	Is the cloud service delivery managed under SLAs (Service Level Agreements)?	No	0	0	X
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	X
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	

Visualisation de la conformité

	Minimal weighted score	Maximal weighted score	Compliance with cloud policy
Governance	41%	66%	
IAM	64%	72%	
IT Sec	37%	76%	
Ope Sec	20%	66%	

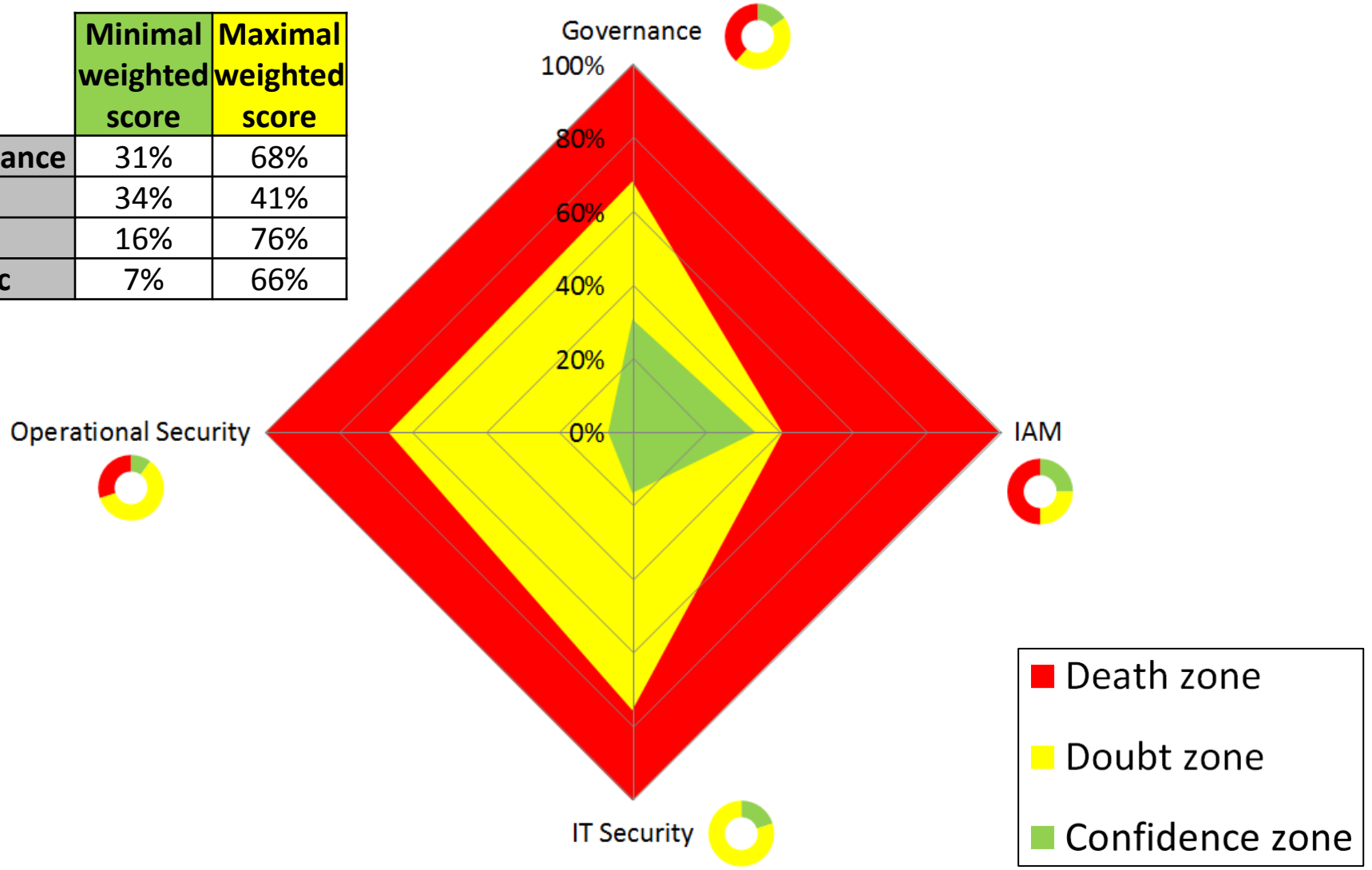
Résultat complet de l'analyse

	Minimal weighted score	Maximal weighted score
Governance	41%	66%
IAM	64%	72%
IT Sec	37%	76%
Ope Sec	20%	66%



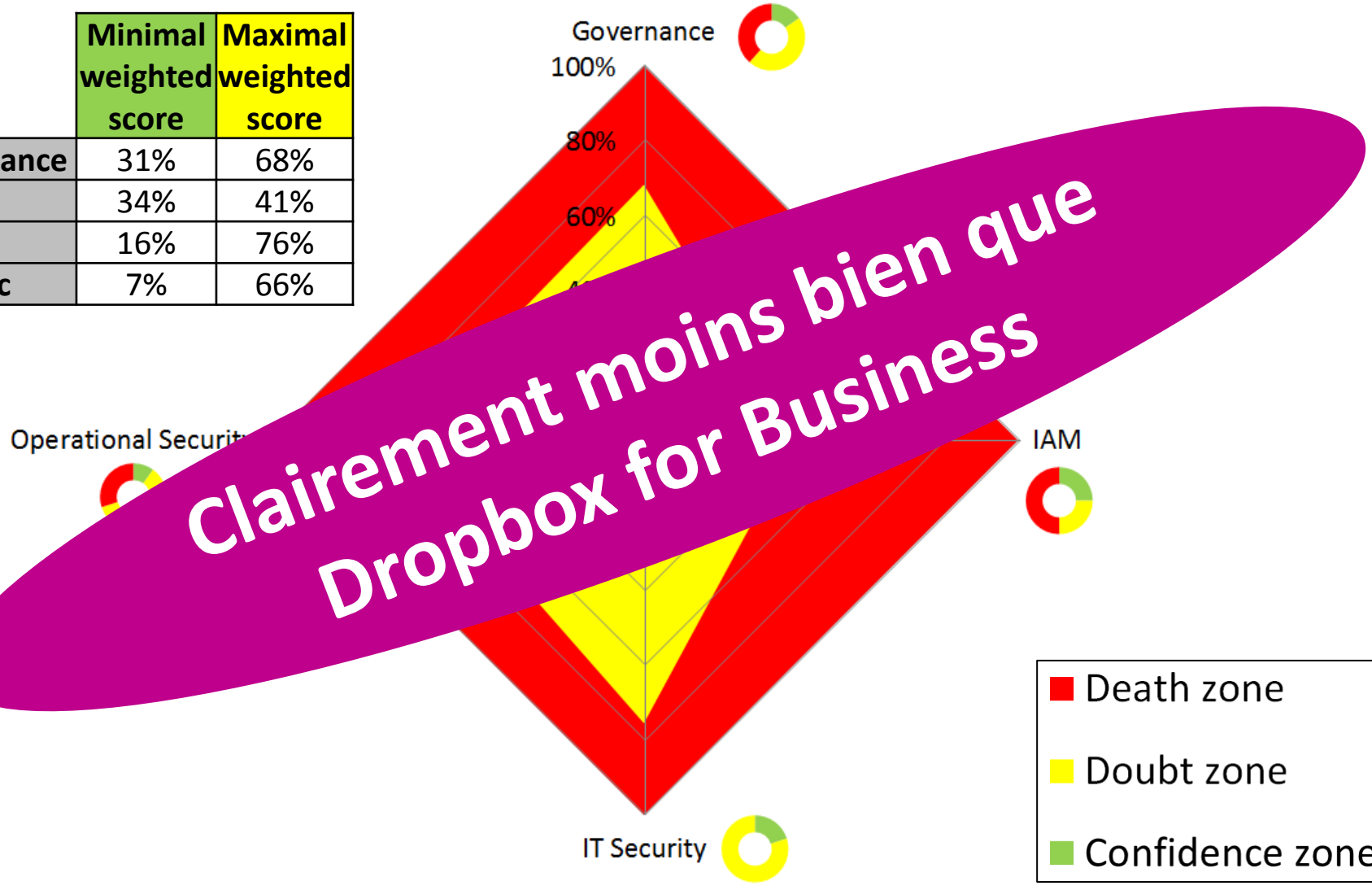
Et Dropbox Free alors?

	Minimal weighted score	Maximal weighted score
Governance	31%	68%
IAM	34%	41%
IT Sec	16%	76%
Ope Sec	7%	66%



Et Dropbox Free alors?

	Minimal weighted score	Maximal weighted score
Governance	31%	68%
IAM	34%	41%
IT Sec	16%	76%
Ope Sec	7%	66%



Clairement moins bien que Dropbox for Business


Choisir un service cloud

But du modèle

Aide pour les experts en sécurité

Modèle pratique

« Quel service cloud puis-je utiliser si je souhaite y mettre un type X de données ? »

Eliminer/filtrer les pistes non fructueuses

Sélectionner les candidats potentiels

Comment choisir un bon candidat?

1
- Experts analysent des services cloud
- Résultats sont diffusés

2
- Client fait une auto-évaluation de ses besoins/exigences

3
- Client compare:  /  = 

Auto-évaluation

Quel type de données?

Quel niveau de sécurité?

Auto-éval: quel type de données?

Publiques

Internes

Confidentielles

Personnelles

Sociales

Médicales

Ref: Data classification policy de la sécurité sociale REF

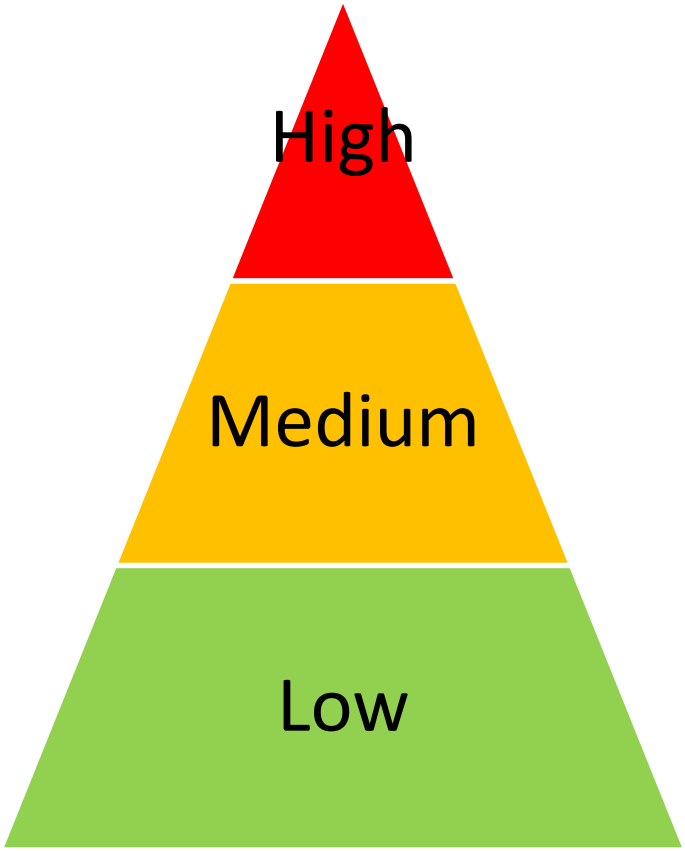
Auto-éval: quel niveau de sécurité?

- Question 1?
- Question 2?
- …

- Question 1?
- Question 2?
- …

- Question 1?
- Question 2?
- …

- Question 1?
- Question 2?
- …



Auto-éval: quel niveau de sécurité?

- Question 1?
- Question 2?
- …

Required score

- Question 1?
- Question 2?
- …

Required score

- Question 1?
- Question 2?
- …

Required score

- Question 1?
- Question 2?
- …

Required score

Ex: stockage des fiches de salaire

	Category Title		Score	Required score
0	**Data Type**			
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	**Governance**			**75%**
1.1	Which level of governance must be attained by the cloud service?		High	75
2	**Identity and Access Management (IAM)**			**78%**
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	**IT Security**			**68%**
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	**Operational Security**			**75%**
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

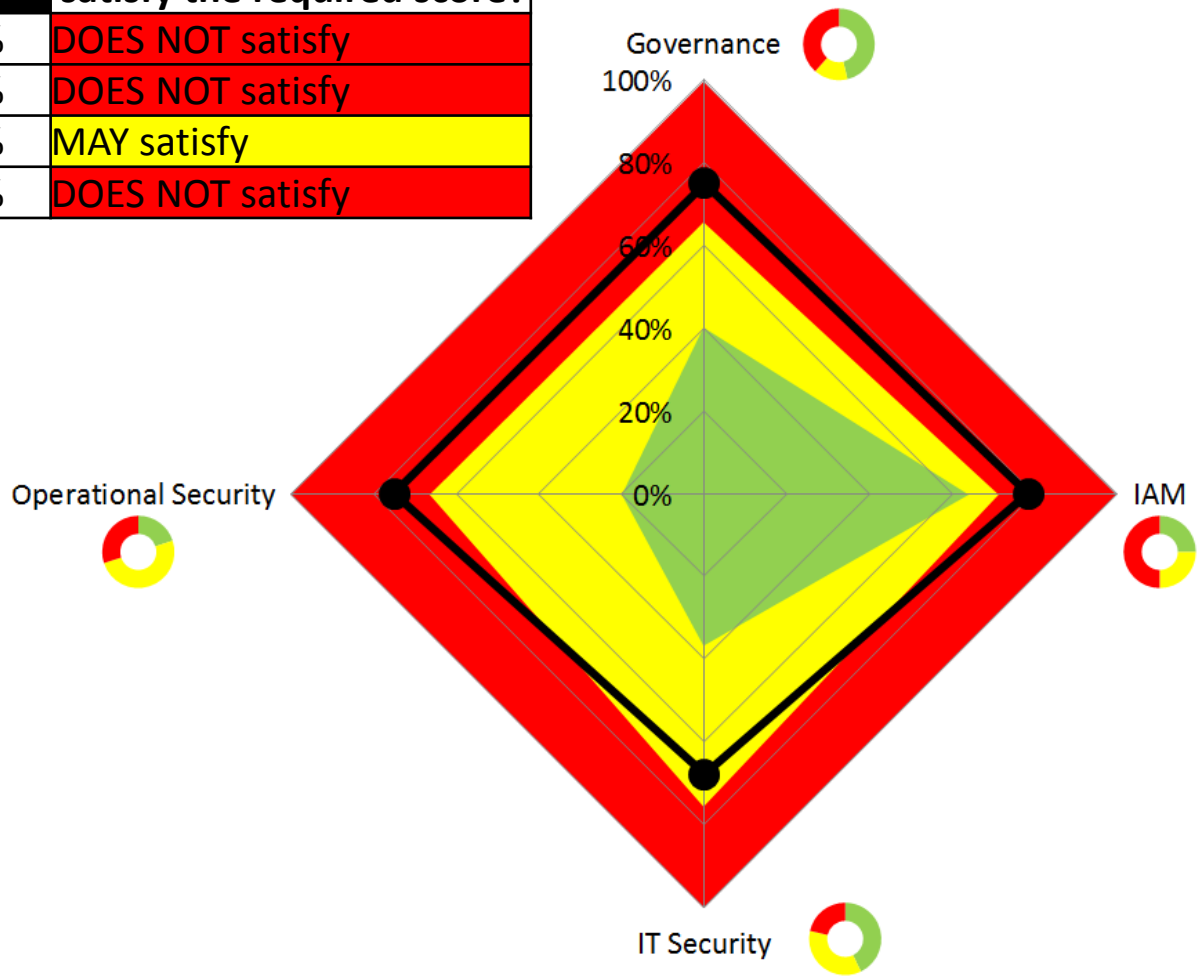
Ex: stockage des fiches de salaire

	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)	
1	Which level of authentication must be offered by the cloud service?	High
2	Which level of control on the user management must be proposed by the cloud service?	High
	Which level of access management must be provided by the cloud service?	High

Ex: stockage des fiches de salaire

	Minimal weighted score	Maximal weighted score	Required score	Does Dropbox for Business satisfy the required score?
Governance	41%	66%	75%	DOES NOT satisfy
IAM	64%	72%	78%	DOES NOT satisfy
IT Sec	37%	76%	68%	MAY satisfy
Ope Sec	20%	66%	75%	DOES NOT satisfy

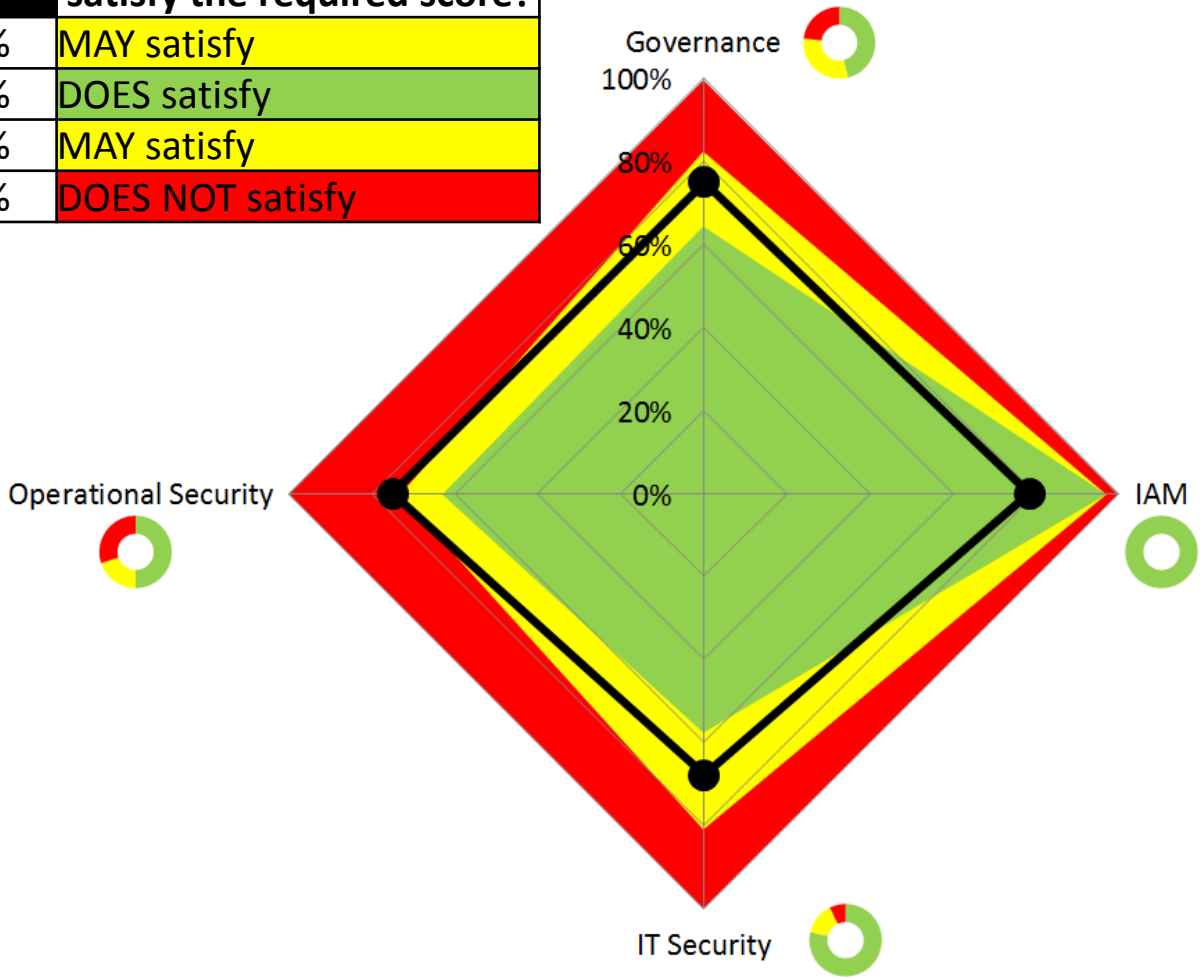
DOES NOT SATISFY



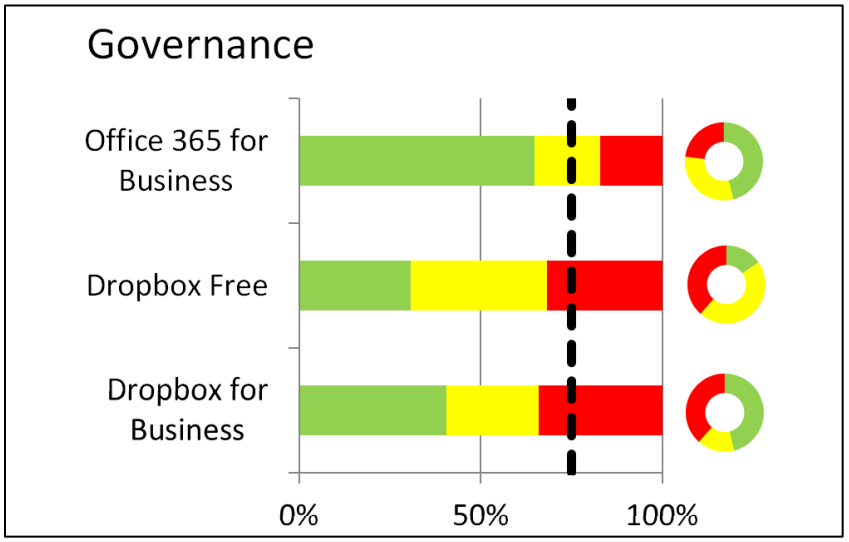
Ex: stockage des fiches de salaire

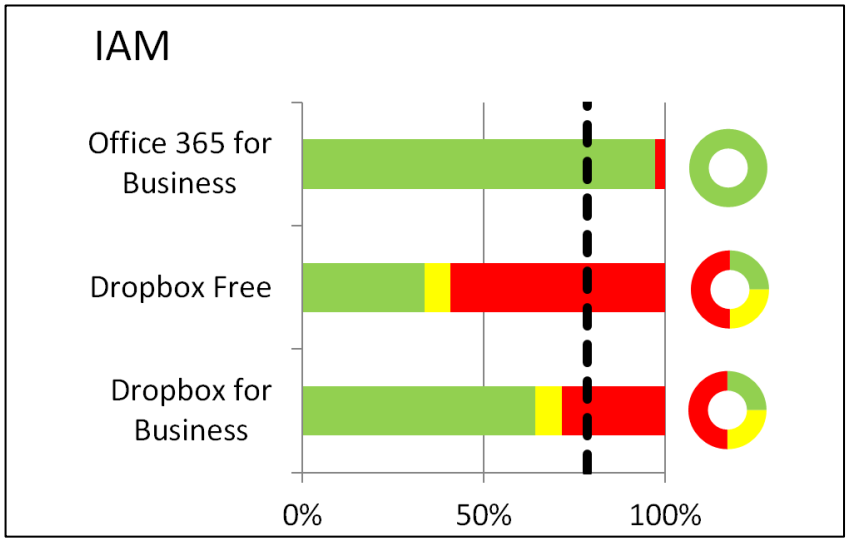
	Minimal weighted score	Maximal weighted score	Required score	Does Office 365 for Business satisfy the required score?
Governance	65%	83%	75%	MAY satisfy
IAM	97%	97%	78%	DOES satisfy
IT Sec	58%	81%	68%	MAY satisfy
Ope Sec	63%	73%	75%	DOES NOT satisfy

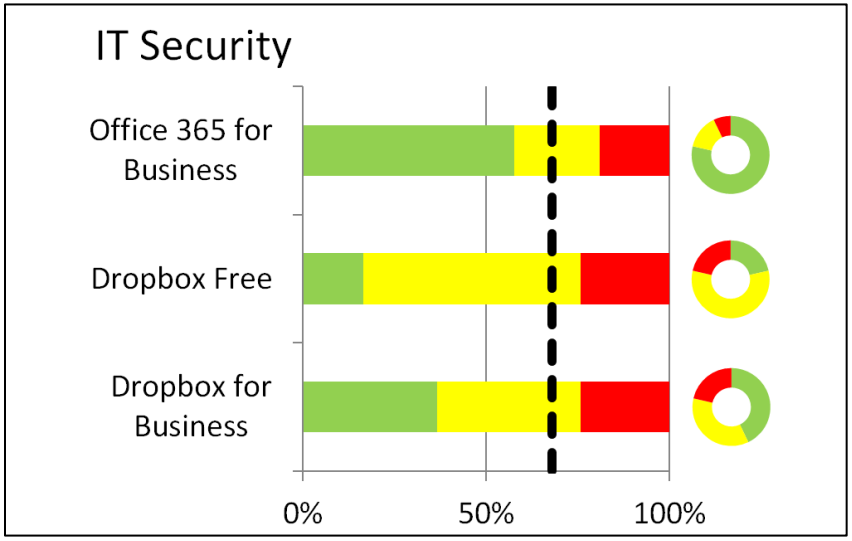
DOES NOT SATISFY

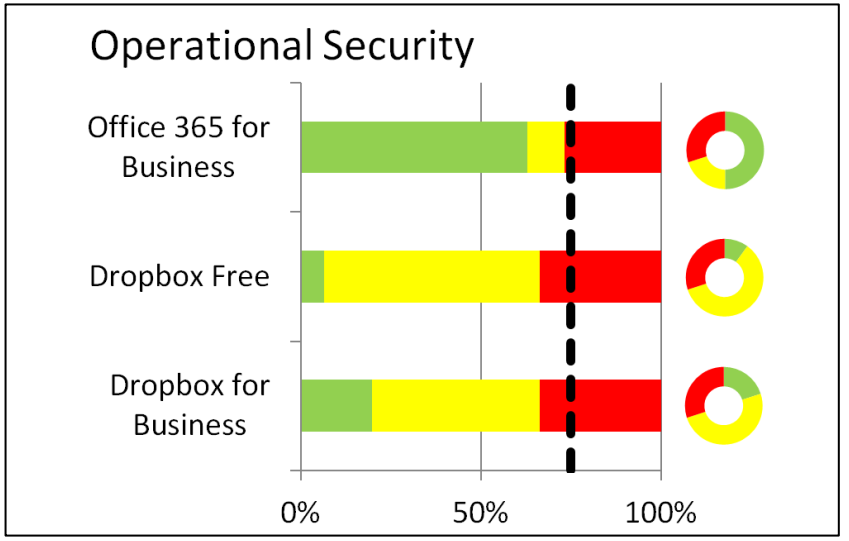


Ex: stockage des fiches de salaire

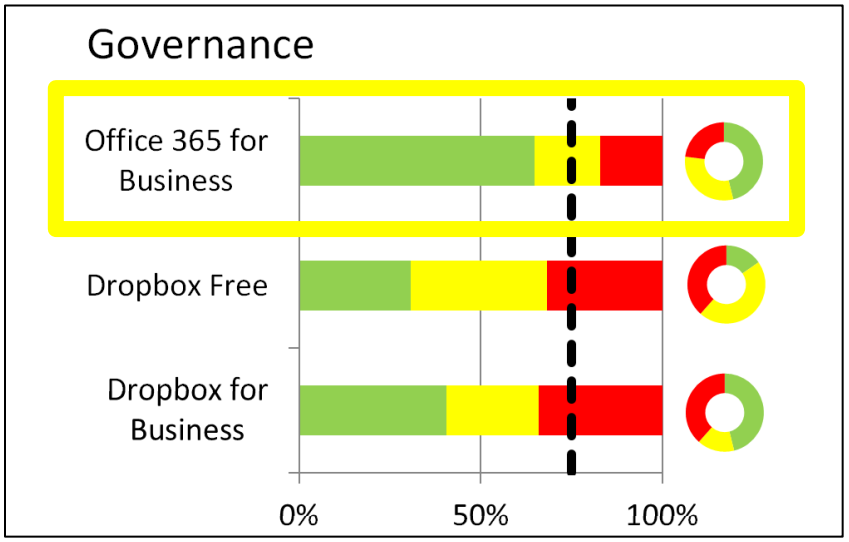


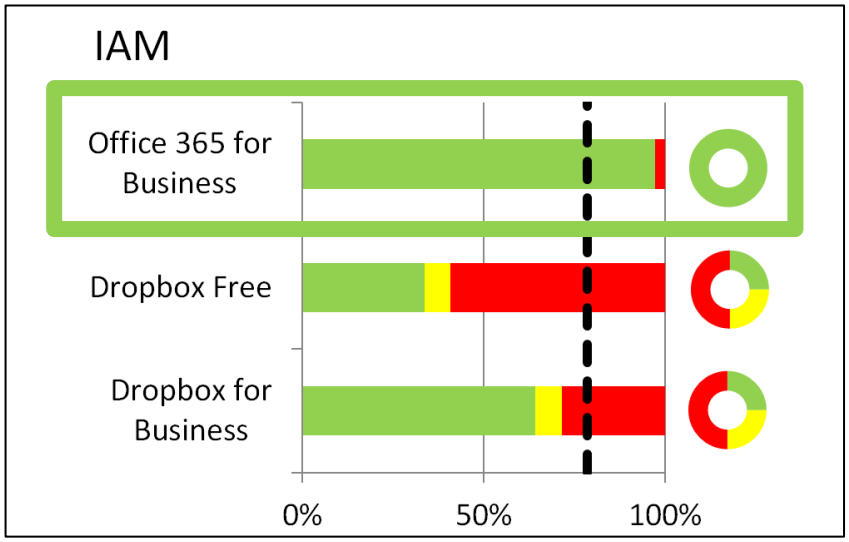


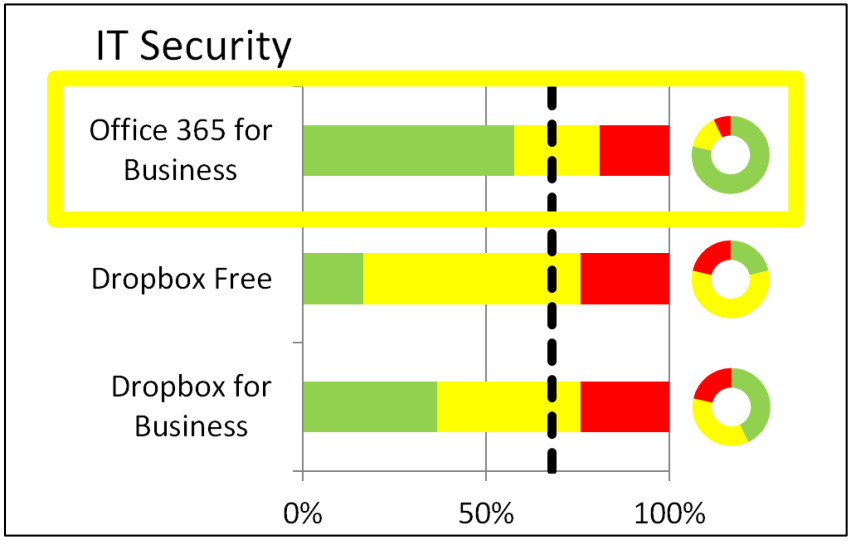


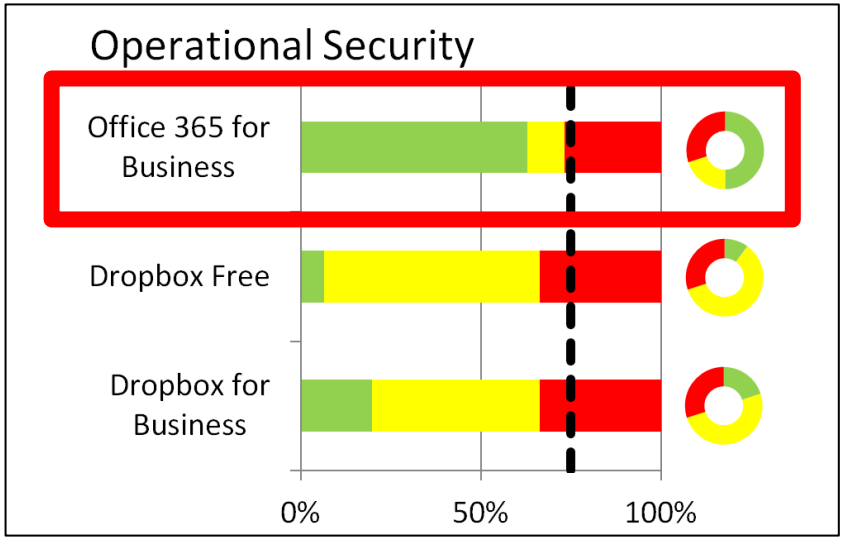


Ex: stockage des fiches de salaire

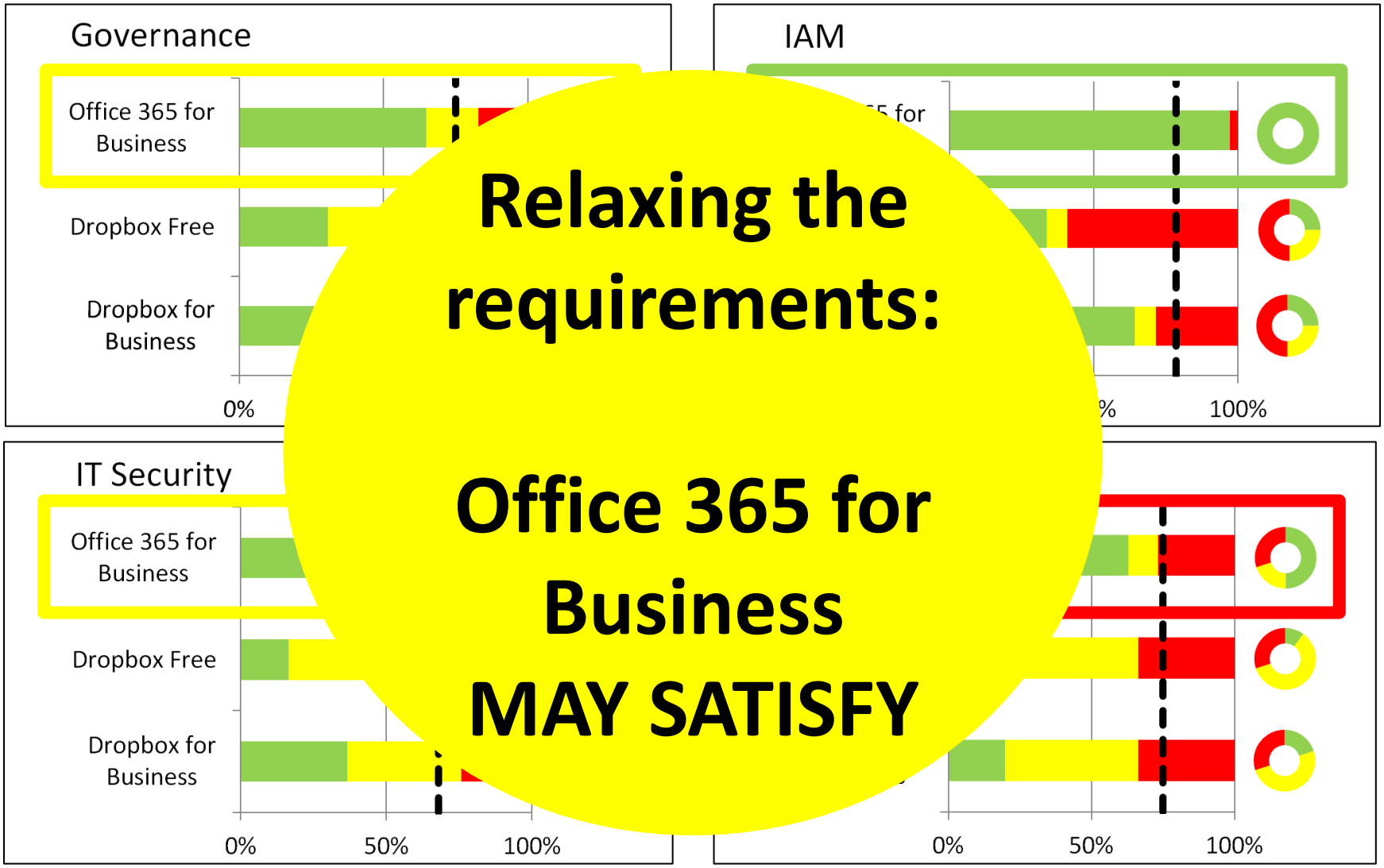








Ex: stockage des fiches de salaire




Conclusion

Conclusion

Sécurité du cloud **cruciale**

Surtout si on souhaite y mettre des données **sensibles**

Importance d'**évaluer** la sécurité d'un service cloud

Proposition d'un outil d'évaluation:

le modèle

Un expert humain est le seul vrai juge du résultat

Où trouver le modèle?

URL?

- Version FR
- Version NL

REF

Pour qui?

- Experts et conseillers en sécurité

Quelques REF intéressantes

- Koen Vanderkimpen and Bert Vanhalst, “Application Platform as a Service”
- NIST, “Special Publication 800-145 – The NIST Definition of Cloud Computing”
- 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”
- Sécurité sociale, “Politique de sécurité relative à des services de Cloud Computing”
- Sécurité sociale, “Policy dataclassification”
- Smals Research, “Modèle d’évaluation de sécurité cloud”
- Smals Research, “Cloud security evaluatiemodel”

Tania Martin

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

Smals

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