Avis n° 04/2015 du 25 février 2015

Objet : avis relatif à un projet de circulaire portant sur l'utilisation du "cloud" par les hôpitaux (CO-A-2014-053)

La Commission de la protection de la vie privée (ci-après "la Commission") ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après "la LVP"), en particulier l'article 29 ;

Vu la demande d'avis de Madame L. Onkelinx, Ministre des Affaires sociales et de la Santé publique, chargée de Beliris et des Institutions culturelles fédérales, reçue le 18/09/2014 ;

Vu un premier examen du dossier lors de la séance plénière de la Commission du 5 novembre 2014 ;

Vu que la Commission a alors jugé, après délibération, qu'il était recommandé de transmettre le dossier pour un avis complémentaire à la section Santé du Comité sectoriel de la Sécurité sociale et de la Santé, ce qui a été fait par courrier du 12 novembre 2014 ;

Vu la réception de la recommandation n° 15/01 du 20 janvier 2015 *relative à un projet de circulaire du SPF Santé publique portant sur l'utilisation de services "cloud" dans les hôpitaux* en date du 2 février 2015 ;

Vu le rapport de Monsieur F. De Smet ;

Émet, le 25 février 2015, l'avis suivant :

I. OBJET DE LA DEMANDE D'AVIS

1. La Ministre des Affaires sociales et de la Santé publique, chargée de Beliris et des Institutions culturelles fédérales, ci-après le demandeur, sollicite l'avis de la Commission concernant un projet de circulaire portant sur l'utilisation du "cloud" par les hôpitaux.

2. Le 10 avril 2014, l'article 20, § 1er de la loi *coordonnée sur les hôpitaux et autres établissements de soins* du 10 juillet 2008 a été modifié en ce sens que la conservation des dossiers de patients et l'enregistrement de l'activité médicale ne doivent plus se faire "à" l'hôpital mais "par" l'hôpital. Cette modification permet en principe aux hôpitaux et autres établissements de soins de recourir au cloud computing.

3. Avec le projet de circulaire faisant l'objet du présent avis, le demandeur souhaite mettre à la disposition des établissements hospitaliers susmentionnés un document de référence concernant le cloud computing.
   Le demandeur indique les finalités suivantes de la circulaire :
   - déterminer quelles informations et quels services peuvent être externalisés ;
   - vérifier quelle qualité et quelles garanties le fournisseur de service "cloud" doit offrir au niveau de la protection des données.

4. Compte tenu de sa compétence spécifique en matière de protection des données relatives à la santé, notamment dans le secteur hospitalier, la Commission a transmis le projet de circulaire pour avis préalable à la section Santé du Comité sectoriel de la Sécurité sociale et de la Santé.

5. Vu la recommandation n° 15/01 du 20 janvier 2015 *relative à un projet de circulaire du SPF Santé publique portant sur l'utilisation de services "cloud" dans les hôpitaux*, la Commission estime que les considérations et recommandations suivantes en matière de protection des données à caractère personnel sont importantes dans un contexte de cloud computing dans les hôpitaux.

II. EXAMEN DE LA DEMANDE D'AVIS

6. Le projet de circulaire fournit une description textuelle du contexte du cloud, des risques potentiels et d'une série de points d'attention. La Commission estime que le projet de circulaire constitue un instrument utile pouvant, dans une certaine mesure, répondre à un besoin d'encadrement au sein des hôpitaux. La Commission constate cependant que le projet ne contient pas d'outil d'évaluation efficace d'un point de vue opérationnel pouvant servir de

guide aux hôpitaux dans des situations concrètes lors de l'analyse de risques dont il est question ci-après.

7. L'utilisation de services "cloud" comporte certains risques inhérents. Ainsi, le traitement de données dans le cloud peut conduire à une fragmentation physique des données sur différents serveurs et dans différents centres de données qui peuvent se trouver dans plusieurs pays. Le client du service "cloud", en tant que responsable du traitement [1], perd ainsi potentiellement une partie du contrôle de ses données et la protection de ces données peut être compromise (protection insuffisante, perte, abus, consultation par des tiers ou des autorités étrangères, ...). Par ailleurs, il existe un risque que des autorités étrangères puissent consulter et réclamer des données selon leur propre législation[2].

8. Les hôpitaux ou autres établissements de soins qui envisagent d'adopter le cloud computing doivent vérifier au moyen d'une analyse de risques quelles seront les répercussions sur la sécurité et la confidentialité si des données à caractère personnel des personnes concernées sont placées dans le cloud.

   Cette analyse de risques doit notamment porter sur les points suivants :

   - une évaluation minutieuse des données à caractère personnel qui sont ou non enregistrées dans le cloud, en particulier pour les données dites "sensibles" telles que visées dans la LVP, dont les données à caractère personnel relatives à la santé ;
   - une analyse des conditions contractuelles ;
   - une évaluation de la conformité des conditions de sécurité proposées par le fournisseur de service "cloud", les mesures de sécurité exigées par la Commission devant servir de norme minimale[3] ;

---

[1] Dans son avis n° 05/2012 *sur l'informatique en nuage*, le Groupe 29 stipule qu'en principe, le client du cloud (en l'occurrence l'hôpital) doit être considéré comme le responsable du traitement et le fournisseur de service "cloud" comme un sous-traitant (voir http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_fr.pdf#h2-3).

[2] D'autres pays sont équipés pour entrer en possession de données informatiques mais également pour repérer des communications électroniques, les localiser ou en prendre connaissance et en identifier les utilisateurs. La finalité poursuivie est généralement de faire appliquer la loi ou de lutter contre le terrorisme. Toutefois, d'autres objectifs publics augmentant le risque de consultation abusive sont parfois poursuivis. Les affaires PRISM et XKeyscore (programmes de surveillance de masse américains) ont révélé l'ampleur insoupçonnée du nombre d'accès des autorités américaines aux données de grands fournisseurs de services de la société de l'information américaine.

[3] Dans ce cadre, on peut notamment faire référence :

- aux "*Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel*" dans lesquelles la Commission a concrétisé l'obligation de "sécurité de l'information" de l'article 16, § 4 de la LVP (voir http://www.privacycommission.be/sites/privacycommission/files/documents/mesures_de_reference_en_matiere_de_securite_applicables_a_tout_traitement_de_donnees_a_caractere_personnel_0.pdf.) ;
- à l'article 25 de l'arrêté royal du 13 février 2001 portant exécution de la LVP qui impose un certain nombre de mesures de sécurité supplémentaires à respecter au responsable du traitement de données à caractère personnel sensibles, dont celles relatives à la santé ;
- à l'article 7, § 4 de la LVP qui oblige le responsable du traitement à traiter les données à caractère personnel relatives à la santé sous la responsabilité d'un professionnel des soins de santé ;

- la garantie du fournisseur de service "cloud" quant à certains droits, de l'exécution à la fin du contrat, afin qu'il puisse se concentrer sur ses propres obligations en matière de protection des données à caractère personnel :
    - clause *intuitu personae*[4] ;
    - règles d'audit[5] ;
    - clause quant à l'intégrité, à la continuité, à la disponibilité et à la qualité du service ;
    - dispositions relatives à l'interopérabilité, à la réversibilité[6] et à la portabilité[7] des données, ... ;
- la prise en considération des conséquences d'un accès possible aux données par des personnes extérieures à l'établissement de soins, en particulier à des fins de "law enforcement"[8] et à d'autres fins ;
- la possibilité de tenir compte des droits des patients concernés, comme le droit à l'information[9], le droit de consultation[10], le droit de rectification et, le cas échéant, le droit d'opposition[11]. À cet égard, la Commission estime que les services de cloud computing doivent précisément pouvoir permettre, dans le chef du patient, un accès direct et immédiat à son propre dossier.

- à la recommandation n° 01/2013 du 21 janvier 2013 *relative aux mesures de sécurité à respecter afin de prévenir les fuites de données* (voir http://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_01_2013_0.pdf) ;
- à la surveillance de la sécurité de l'information par le conseiller en sécurité dont chaque hôpital doit disposer en vertu du point 9°*quater*, g) de l'Annexe A, III de l'arrêté royal du 23 octobre 1964 *portant fixation des normes auxquelles les hôpitaux et leurs services doivent répondre.*

[4] La Commission recommande d'interdire contractuellement que les points essentiels des contrats puissent être à leur tour confiés par le fournisseur de service "cloud" à un sous-traitant ; une éventuelle sous-traitance ne sera de toute façon possible qu'après un accord avec l'établissement hospitalier.

[5] Des systèmes de contrôle indépendants (la Commission, l'auditeur de l'établissement hospitalier) doivent pouvoir contrôler le système du fournisseur de service "cloud".

[6] Au terme du contrat, l'établissement doit pouvoir récupérer ses données et reprendre ses activités. Dans cette optique, le contrat devrait établir que le client peut obtenir une copie intégrale de ses données sous une forme structurée et couramment utilisée.

[7] Il doit être possible pour un établissement de transférer ses données vers un autre fournisseur.

[8] La Commission incite en tout cas à la prudence vis-à-vis de fournisseurs de service "cloud" étrangers ou de fournisseurs qui sont établis à l'étranger et qui doivent rendre des comptes à des autorités étrangères.

Pour les transferts internationaux de données à caractère personnel, il convient de toujours tenir compte des articles 21 et 22 de la LVP en vue de garantir un régime de protection adéquat. Le site Internet de la Commission reprend de plus amples informations à ce sujet : http://www.privacycommission.be/fr/flux-transfrontieres.

[9] Article 9 de la LVP.

[10] Article 10 de la LVP et article 9, § 2 de la loi du 22 août 2002 *relative aux droits du patient*. L'Exposé des motifs de l'article 9, § 2 de la loi *relative aux droits du patient* stipule explicitement que les auteurs ont par principe opté pour un droit de consultation directe (sans l'intervention d'un tiers) dans le chef du patient. La Commission renvoie également à cet effet au Plan d'action e-Santé 2013-2018 approuvé par la Conférence Interministérielle du 29 avril 2013 et plus particulièrement au point d'action essentiel n° 10 (Accès aux données par le patient – voir http://www.rtreh.be/EHEALTH/_images/20130419plandaction_esantefr.pdf).

[11] Article 12 de la LVP. On pourrait même envisager en plus d'autoriser le patient à effectuer lui-même des ajouts et à formuler des remarques dans une partie du dossier spécialement destinée à cet effet. Il ne pourra évidemment pas apporter de modifications aux données et informations introduites par les prestataires de soins. Voir également le Plan d'action e-Santé 2013-2018, point d'action essentiel n° 10.

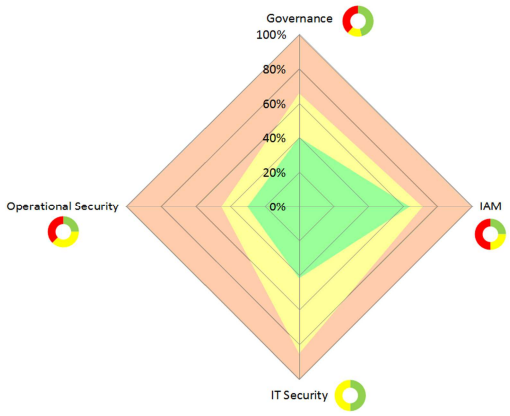
9. Pour permettre aux hôpitaux ou à d'autres établissements de soins de réaliser une telle analyse de risques, la Commission estime qu'outre l'encadrement théorique qu'offre le projet de circulaire, il convient de mettre à la disposition des hôpitaux et des autres acteurs du secteur des soins de santé une méthode pratique et quantitative visant à évaluer la sécurité des services "cloud". La Commission renvoie à cet effet, à titre d'exemple, au modèle d'évaluation[12] recommandé par la section Santé du Comité sectoriel de la Sécurité sociale et de la Santé qui est expliqué ci-après.

   La Commission fait toutefois d'abord remarquer qu'il est préférable que (le projet de) la circulaire relative aux services "cloud" s'abstienne de recommander un type déterminé de cloud, en l'occurrence le 'community of privé-cloud', car celui-ci n'offre, en soi, pas nécessairement plus de garanties sur le plan de la protection des données à caractère personnel. Indépendamment du type de cloud, il faut se concentrer sur les garanties réellement apportées en matière de protection des données.

10. Ci-après une description du modèle à deux volets permettant, sur la base d'une grille simple et évolutive, d'une part, d'évaluer le niveau de maturité en ce qui concerne la sécurité d'un service cloud spécifique et, d'autre part, d'évaluer l'utilisation d'un service cloud spécifique en fonction du type de données qu'on souhaite y transférer.

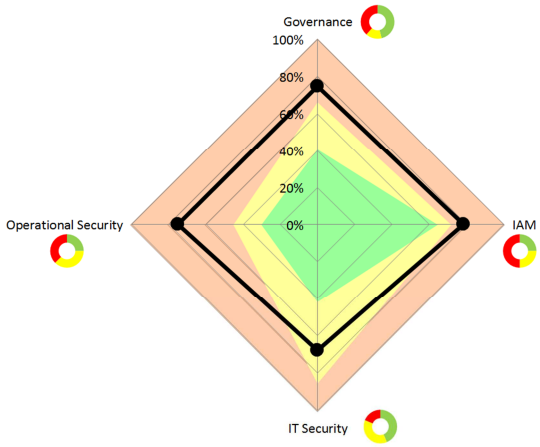
11. Concrètement, la méthode proposée est composée de deux volets:

- un volet A constitué du questionnaire "Security-assessment-cloud-service.xlsm" qui permet d'évaluer le niveau de maturité en ce qui concerne la sécurité d'un service cloud spécifique. Cette évaluation doit reposer uniquement sur les données publiques que l'évaluateur a pu récolter au préalable (p.ex. sur le site Internet officiel du service cloud). La figure ci-dessous est un exemple du résultat d'analyse obtenu pour un service cloud une fois le questionnaire du volet A rempli. Le résultat est présenté sous forme de radar.



[12] Voir la recommandation n° 15/01 du 20 janvier 2015 *relative à un projet de circulaire du SPF Santé publique portant sur l'utilisation de services "cloud" dans les hôpitaux.*

- un volet B constitué du questionnaire "Client-guide-cloud-assessment.xlsm" qui permet d'évaluer la possibilité d'utiliser un service cloud spécifique en fonction du type de données qu'on souhaite y transférer. La figure ci-dessous est un exemple du résultat de comparaison obtenu. La figure reprend le radar obtenu suite à l'application du volet A à un service cloud. La ligne noire correspond aux besoins et exigences de l'utilisateur ayant rempli le questionnaire du volet B. Le résultat final du volet B est donc basé sur un radar résultant du volet A, complété par l'évaluation de l'utilisateur.



12. Les points-clé de sécurité qui sont évalués par le modèle sont regroupés en 4 critères majeurs : gouvernance, gestion des identités et du contrôle d'accès, sécurité IT et enfin sécurité opérationnelle. Dans le contexte (de la sécurité sociale et) des soins de santé, le modèle évalue aussi la conformité du service cloud avec la "Politique de sécurité relative à des services de Cloud Computing" publiée par la Banque carrefour de la sécurité sociale[13]. Cette conformité est représentée dans les volets A et B par les bouées (une bouée par critère majeur).

13. Les codes couleur sont identiques pour les bouées ou les radars. La zone verte, dite "confidence zone", représente le pourcentage de conformité totale d'un service cloud à un critère majeur. La zone jaune, dite "doubt zone", représente le pourcentage de conformité potentielle d'un service cloud à un critère majeur. On parle de "conformité potentielle" pour ne pas pénaliser le service cloud évalué : la "doubt zone" représente donc les questions du questionnaire "Security-assessment-cloud-service.xlsm" où il est impossible de répondre avec certitude. Enfin, la zone rouge, dite "death zone", représente le pourcentage de non-conformité d'un service cloud à un critère majeur.

[13] https://www.ksz-bcss.fgov.be/binaries/documentation/fr/securite/policies/isms_050_cloud_computing_policy_fr.pdf.

14. Les figures ci-dessous présentent une comparaison entre 5 services "cloud" différents et les besoins/exigences d'un client ayant rempli le questionnaire du volet B. Le modèle compare ainsi les services "cloud" par critère pour faciliter l'analyse.

15. Les deux questionnaires du volet A et du volet B sont joints en annexe au présent avis et seront publiés avec l'avis sur le site Internet de la Commission.[14]

16. L'utilisation de ce modèle (ou d'un autre modèle similaire) devrait permettre à un hôpital ou à tout autre acteur des soins de santé d'évaluer lui-même dans quelle mesure le niveau de sécurité d'un service "cloud" déterminé répond aux besoins spécifiques. Les acteurs des soins de santé concernés sont ainsi en mesure d'évaluer d'une manière fondée les divers risques avant d'avoir recours, sous leur propre responsabilité, à un service "cloud" déterminé.

III. CONCLUSION

17. La Commission estime que le projet de circulaire portant sur l'utilisation du "cloud" par les hôpitaux peut offrir des garanties suffisantes en matière de protection des données à caractère personnel des personnes concernées[15], à condition que :
    - celle-ci soit complétée par un outil d'évaluation efficace d'un point de vue opérationnel permettant aux hôpitaux et autres établissements de soins d'évaluer, sous leur propre

[14] Pour le 'tool' opérationnel voir: http://www.privacycommission.be/fr/le-modele-devaluation-de-securite-des-services-cloud.

[15] La Commission a toutefois constaté que la version néerlandaise du document était perfectible en matière de terminologie utilisée (probablement suite à une traduction peu soignée) à certains endroits. Par exemple : partout dans le texte 'behandeling' et 'verantwoordelijke voor de 'behandeling' ' doivent être remplacés par 'verwerking' et 'verantwoordelijke voor de 'verwerking' ' (traitement en français) ; à la page 8, deuxième alinéa du point 6.3., 'niet zinvol' doit être remplacé par 'zinvol', …

responsabilité, la sécurité des services "cloud". La Commission renvoie à cet effet, à titre d'exemple, au modèle d'évaluation recommandé en la matière par le Comité sectoriel de la Sécurité sociale et de la Santé (voir les points 6, 9 et 16) ;

- la recommandation d'un type de cloud déterminé, en l'occurrence le 'community of privé-cloud' soit supprimée du texte du projet. En effet, le choix d'un 'community of privé-cloud' n'offre en soi pas nécessairement plus de garanties sur le plan d'une meilleure protection des données. Indépendamment du type de cloud, il faut se concentrer sur les garanties réellement apportées en matière de protection des données (voir le point 9).

PAR CES MOTIFS,

en référence à la recommandation n° 15/01 du Comité sectoriel de la Sécurité sociale et de la Santé, section Santé, **la Commission** émet un **avis favorable** sur le projet de circulaire portant sur l'utilisation du "cloud" par les hôpitaux, à la condition expresse et absolue d'intégrer dans le texte les remarques susmentionnées, vu le caractère sensible éventuel des données.

Pour l'Administrateur f.f., abs. Le Président,

(sé) An Machtens (sé) Willem Debeuckelaere
Chef de section ORM f.f.

Cloud Service Security Assessment Model

VERSION: 1.0

Change tracking	
1.0	First release
How to use this template:	
1.	The goal of this evaluation form is for a person (called assessor) to assess the security level of a cloud service offered by a Cloud Service Provider (CSP) according to 4 main criteria: - Governance - Identity and Access Management (IAM) - IT Security - Operational Security
2.	Before filling the evaluation form, the assessor should be in possession of a standard contract and all the available datasheets that can be found on the website of the cloud service. We assume that the information found about the cloud service on the official website are correct.
3.	The "Information" tab should be filled all the general info related to the assessment: cloud service name/provider/model, the name of the assessor, and the date of the assessment.
4.	The "Assessment" tab contains all the questions necessary for the evaluation of a cloud service.
4.1.	The column "answer's value" contains the relative score of each expected response for each question (over 100) as a reference. The cells containing the relative scores must not be changed.
4.2.	The column "score" has to be filled using the possible answers.
	Note: The questions must be filled according to the given order, as some questions depend on the answers given in previous questions.
	Note: If a score is not applicable, the option "N/A" must be chosen. This will redistribute the weights for the sub questions.
	Note: If the assessor does not know the answer to a question, the option "Unknown" must be chosen. This will give two different scores for one topic.

4.3.	Each question has been defined with a specific weight. From the scores of each question, the final weighted scores are automatically filled (in combination with the defined weights).
4.4.	There are 2 different results: the **minimal weighted score** and the **maximal weighted score**. - The **minimal weighted score** corresponds to the situation where all the "Unknown" responses have been replaced by the worst answer. This is the worst case of the security evaluation, considering the uncertainty of the "Unknown" responses. - The **maximal weighted score** corresponds to the situation where all the "Unknown" responses have been replaced by the best answer. This is the best case of the security evaluation, considering the uncertainty of the "Unknown" responses.
4.5.	The two last columns grouped under "compliance with cloud policy" refer to the guarantees required by the cloud policy of the Social Security.
	The column "ignoring the data type" refers to the cloud policy guarantees that do not depend on the type of data to be stored in the cloud service.
	The column "if personal, social or medical data" refers to the additional cloud policy guarantees expected when the data to be stored in the cloud service are personal, social or medical.
5.	The "Overview" tab is a visual aide for the assessor.
5.1.	The chart represents the minimal and maximal weighted scores of each criterion.
5.2.	The donuts represent the compliance to the cloud policy per criterion when the data type is ignored.
6.	Be careful with the interpretation of the scores.

Cloud service informations	
Cloud service name:	<name>
Cloud service provider (CSP):	<CSP>
Cloud service model:	<choose a model>
Evaluated by:	<assessor name>
Evaluated date:	<dd/mm/yyyy>

Assessment of <name>

	Category Title	Answer's value	Score	Minimal weighted score	Maximal weighted score	Compliance with cloud policy	
	For more information open the outline (+ / -) left from row number	*Possibility to put some description in the question's rows*	*Select appropriate range or value for every question (select N/A if not applicable)*	*Values computed automated*	*Values computed automated*	*Ignoring the data type*	*If personal, social or medical data*
1	**Governance**			**0%**	**0%**		
1.1	Legal implication			0%	0%		
1.1.1	What is the physical location of data-at-rest?			0	0		
1.1.2	Which jurisdiction is the CSP subject to?			0	0		
1.1.3	Can the CSP accomodate with the tenant's data retention requirements?			0	0		
1.1.4	Can the data be given to governments if requested for judicial requirements without informing the tenant or without constitutional guarantees?			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?			0	0	X	
1.1.6	If the US-EU Safe Harbor applies, is the CSP registered?			0	0		
1.2	Supply chain management			0%	0%		
1.2.1	Does the CSP use subcontrators?			0	0		
1.2.2	If so, will the CSP inform the tenant of the subcontractors hired to provide the cloud service?			0	0	X	
1.2.3	If so, will the CSP inform the tenant of any change in the course of the contract?			0	0	X	
1.2.4	If so, does the CSP guarantee contractually to remain fully responsible for his engagements, even with the hiring of subcontractors?			0	0	X	
1.3	Audit			0%	0%		
1.3.1	At which time interval is the cloud service (including all its subcontractors) audited by a third party?			0	0	X	
1.3.2	If the cloud service is audited, are the scopes of the audits accurately defined?			0	0	X	
1.3.3	At which time interval is the cloud service (including all its subcontractors) pen-tested?			0	0	X	
1.3.4	Did the cloud service define an ISP (Information Security Policy) and obtain a security-related certification?			0	0	X	
1.3.5	Is there a Tier certification of data centers (especially for physical availability and security) or equivalent certification?			0	0	X	

1.4	Business continuity			0%	0%		
1.4.1	Is the cloud service delivery managed under SLAs (Service Level Agreements)?			0	0	X	
1.4.2	Does the CSP define and implement a business continuity plan?			0	0	X	
1.4.3	Is the reversibility of the cloud service provided?			0	0	X	
1.5	Others			0%	0%		
1.5.1	Does the CSP apply a segregation of duties in the CSP organization to protect the tenants?			0	0		
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?			0	0		
2	**Identity and Access Management (IAM)**			**0%**	**0%**		
2.1	Authentication level			0%	0%		
2.1.1	Are the different authentication mechanisms to access the cloud service documented?			0	0		
2.1.2	What is the strongest authentication mechanism to access the cloud service as a tenant system administrator offered by the CSP?			0	0		
2.1.3	What is the strongest authentication mechanism to access the cloud service as a tenant user offered by the CSP?			0	0		
2.1.4	Are password policy enforcements well-defined and implemented?			0	0		
2.1.5	Are secure password reset procedures well-defined and implemented?			0	0		
2.2	User management			0%	0%		
2.2.1	Who performs the tenants' user management?			0	0		
2.2.2	Is the integration with the IAM of the tenant possible?			0	0		
2.2.3	Is the integration with an ID-provider possible?			0	0		
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?			0	0	X	
2.3	Access management			0%	0%		
2.3.1	Does the CSP document how the IAM of its employees related to the tenants' assets is performed?			0	0		
2.3.2	Is data access of {tenant user, tenant system administrator, CSP system administrator} clearly defined?			0	0	X	

2.3.2	Is data access of {tenant user, tenant system administrator, CSP system administrator} clearly defined?			0	0	X	
2.3.3	Is data access of {CSP employees, third party, other tenants} denied?			0	0	X	
2.3.4	Is IAM management and data access logging clearly defined and available?			0	0	X	
3	**IT Security**			**0%**	**0%**		
3.1	Segregation of data			0%	0%		
3.1.1	Can the cloud service be provided as private or community?			0	0		X
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?			0	0	X	
3.2	Interface security			0%	0%		
3.2.1	Are APIs developed in accordance with standards?			0	0		
3.2.2	Are data integrity and security ensured for input and output?			0	0	X	
3.3	Infrastructure and virtualization security			0%	0%		
3.3.1	Is the access to hypervisors management functions and administration consoles highly controlled?			0	0	X	
3.3.2	Is data securely deleted from all storage media when the user's or tenant's account is deleted?			0	0	X	
3.3.3	Does the CSP take defense-in-depth approach to wired or wireless network security?			0	0	X	
3.3.4	Are sufficient controls in place at the hardware and virtual (if applicable) levels?			0	0	X	
3.3.5	Are security mechanisms to prevent and analyze data leakage at the hardware and virtual (if applicable) levels available?			0	0	X	
3.4	OS security (only for SaaS and PaaS cloud services)			0%	0%		
3.4.1	Are tools to prevent, detect and mitigate viruses and malwares at server stations available?			0	0	X	
3.4.2	Is harding process performed on the server stations?			0	0	X	
3.5	Cryptography			0%	0%		
3.5.1	Who is in charge of the key management?			0	0		X

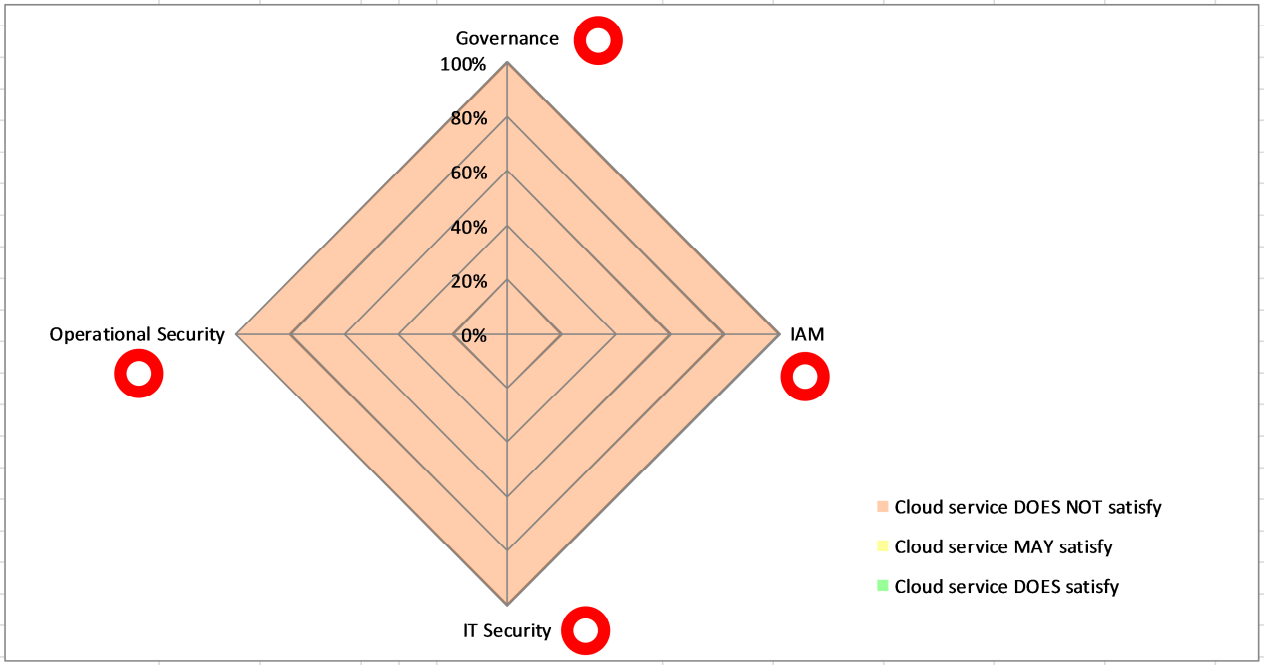
3.5.2	Has the key management been defined through policies and procedures as required by the ISO/IEC27002:2013 standard?			0	0		
3.5.3	Have the cryptographic mechanisms used for the cloud service been defined to guarantee adequate cryptographic strength?			0	0		
3.5.4	Does the CSP use HSMs (Hardware Security Modules) for the protection of keys?			0	0		
3.5.5	Is client-side encryption of data possible?			0	0		X
3.5.6	Is data-at-rest confidentiality ensured?			0	0		X
3.5.7	Is data-at-rest integrity ensured?			0	0	X	
4	**Operational Security**			**0%**	**0%**		
4.1	Backup and disaster recovery			0%	0%		
4.1.1	Can the backup retention plan be defined by the tenant?			0	0	X	
4.1.2	Are backup controls defined and adequate?			0	0	X	
4.1.3	Which RTO (Recovery Time objective) can be satisfied by the cloud service?			0	0	X	
4.1.4	Which RPO (Recovery Point objective) can be satisfied by the cloud service?			0	0	X	
4.1.5	Are tenants able to perform recovery tests, including reporting?			0	0	X	
4.2	Incident management			0%	0%		
4.2.1	Does the CSP have a SIEM (Security Information and Event Management) for analyzing the security alerts and data logs?			0	0	X	
4.2.2	Does the CSP have an adequate incident management procedure for managing and minimizing the impact of security incidents on tenants' data?			0	0	X	
4.2.3	Does the CSP have adequate security policies and procedures regarding CSP employee security?			0	0	X	
4.3	Vulnerability management (only for SaaS and PaaS cloud services)			0%	0%		
4.3.1	Is there a documented patch management process implemented in the cloud service?			0	0	X	
4.3.2	Does the CSP test patches in acceptance environments prior to deployment?			0	0	X	

Score overview of <name>

Copy **scores** for future use

	Minimal weighted score	Maximal weighted score
Governance	0%	0%
IAM	0%	0%
IT Security	0%	0%
Operational Security	0%	0%

	Compliance with cloud policy (ignoring the data type)			Compliance with cloud policy (if personal/social/medical data)		
	Does comply	May comply	Does not comply	Does comply	May comply	Does not comply
Governance	0	0	13	0	0	13
IAM	0	0	4	0	0	4
IT Security	0	0	10	0	0	14
Operational Security	0	0	8	0	0	8



Client Guide Cloud Assessment Model

VERSION: 1.0

Change tracking	
1.0	First release
How to use this template:	
1.	The goal of this evaluation form is for a person (called client) willing to use a cloud service offered by a Cloud Service Provider (CSP) to assess if his/her wish is possible, depending on the type of data that is intended to be moved to the cloud service and according to the 4 main characteristics expected of a cloud service: - Governance - Identity and Access Management (IAM) - IT Security - Operational Security
2.	The "Assessment" tab contains all the questions necessary for the client to assess what he/she expects from a cloud service.
2.1.	First fill all the client name at the beginning.
2.2.	The column "answer's value" contains the relative score of each expected response for each question (over 100) as a reference. The cells containing the relative scores must not be changed.
2.3.	The column "score" has to be filled using the possible answers.
2.4.	Each question has been defined with a specific weight. From the scores of each question, the final weighted scores (called "**required scores**") are automatically filled (in combination with the defined weights).
3.	The "Overview" tab is a visual aide.
3.1.	The chart represents the required scores.
3.2.	It is further possible to paste the scores of a cloud service that has been assessed, and to see if it satisfies the client's requirements.
3.3.	The donuts represent the compliance to the cloud policy per criterion depending on the type of data that is intended to be moved to a cloud service.
4.	The "Comparison" tab is another visual aide where it is possible to paste the scores of several cloud services that have been assessed.
4.1.	The charts allow the client to see which cloud service fits best his/her requirements.
4.2.	Here as well, the donuts represent the compliance to the cloud policy per criterion depending on the type of data that is intended to be moved to a cloud service.
5.	Be careful with the interpretation of the scores.

<Fill client name>

	Category Title	Answer's value	Score	Required score
	For more information open the outline (+ / -) left from row number	*Possibility to put some description in the question's rows*	*Select appropriate range or value for every question (even if not applicable N/A)*	
0	**Data Type**			
0.1	What type of data is intended to be moved to a cloud service?			
1	**Governance**			**0%**
1.1	Which level of governance must be attained by the cloud service?			0
2	**Identity and Access Management (IAM)**			**0%**
2.1	Which level of authentication must be offered by the cloud service?			0
2.2	Which level of control on the user management must be proposed by the cloud service?			0
2.3	Which level of access management must be provided by the cloud service?			0
3	**IT Security**			**0%**
3.1	Which deployment model must be provided by the cloud service?			0
3.2	Which level of interface security must be provided by the cloud service?			0
3.3	Which level of infrastructure and virtualization security must be achieved by the cloud service?			0
3.4	Which level of cryptography must be provided by the cloud service?			0
4	**Operational Security**			**0%**
4.1	Which level of backup and disaster recovery must be provided by the cloud service?			0
4.2	Which level of incident management must be provided by the cloud service?			0

Score overview of

Reset values

Paste scores

	Minimal weighted score	Maximal weighted score	Required score	Does the cloud service satisfy the required score?
Governance	0%	0%	0%	Cloud service DOES satisfy
IAM	0%	0%	0%	Cloud service DOES satisfy
IT Security	0%	0%	0%	Cloud service DOES satisfy
Operational Security	0%	0%	0%	Cloud service DOES satisfy
				Cloud service DOES satisfy

	Compliance with cloud policy when data type is:		
	Does comply	May comply	Does not comply
Governance	0	0	0
IAM	0	0	0
IT Security	0	0	0
Operational Security	0	0	0

Comparison when data type is:

		<Cloud Service 1>		<Cloud Service 2>		<Cloud Service 3>		<Cloud Service 4>		<Cloud Service 5>	
	Required score	Minimal weighted score	Maximal weighted score	Minimal weighted score	Maximal weighted score	Minimal weighted score	Maximal weighted score	Minimal weighted score	Maximal weighted score	Minimal weighted score	Maximal weighted score
Governance	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
IAM	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
IT Security	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Operational Security	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%

Reset values | Paste scores of cloud service 1 | Paste scores of cloud service 2 | Paste scores of cloud service 3 | Paste scores of cloud service 4 | Paste scores of cloud service 5