Annexe C : Aperçu des risques et des mesures[1]

La présente annexe vise à donner un aperçu général des risques et des mesures d'atténuation correspondantes. Pour les externalisations en nuage dans le cadre de l'appel d'offres OMC 20007, un standard minimal est garanti par les contrats-cadres (cf. ch. partie 1, ch. 5 du rapport)[2]. Les autres mesures nécessaires doivent être déterminées pour un projet concret sur la base d'une analyse des risques. Toutes les mesures ne doivent pas être mises en œuvre dans tous les cas, notamment lorsqu'il ne s'agit pas de données personnelles, ni de données classifiées ou de données nécessitant une protection particulière.
L'unité administrative décide si des services es services d'informatique en nuage doivent être achetés par elle et, le cas échéant, lesquels. Le TNI ChF met à disposition des instruments qui aident à la prise de décision et qui doivent être pris en compte avant celle-ci.

Catégories (cf.. partie 1, ch. 3.1, du rapport)

- C, risques de conformité (risques juridiques au sens strict) : violation des prescriptions légales concernant la protection des données, la protection du secret, la protection de l'information (par ex. accès non autorisés).
- BC, risques de continuité des activités : disponibilité de l'accès aux données propres, disponibilité des réseaux, intégrité des données.
- P, environnement juridique à l'étranger, par exemple restrictions à la libre circulation des données ; accès des autorités selon le droit étranger ; espionnage par des services de renseignement
- T, risque technique

N°	Risque	Catégorie	Description du risque	Mesures possibles
1	Les mandataires et les sous-traitants ne sont pas suffisamment instruits et contrôlés	C	Les organes fédéraux responsables doivent impérativement veiller à ce que les exigences en matière de protection des données (y compris la sécurité des données) soient respectées. L'organe fédéral responsable a des obligations de contrôle en cas d'externalisation dans le nuage.	Mesures contractuelles : • Réglementation des obligations des CSP et de leurs sous-traitants. • Réglementation des conditions auxquelles les CSP peuvent recourir à des sous-traitants, droit d'opposition au recours à des sous-traitants qui fournissent des parties essentielles de la prestation.

[1] Sources (en plus de celles citées dans le rapport) : David Rosenthal, Genügt eine Cloud-Lösung den Anforderungen einer Schweizer Bank; Dokumentation Microsoft Public Sector Cloud Design, version 1.4
[2] Il convient de rappeler que l'appel d'offres OMC 20007 Public Clouds Confédération a pour objectif d'aller chercher une offre existante sur le marché.

N°	Risque	Catégorie	Description du risque	Mesures possibles
			Les conditions contractuelles standard proposées par les fournisseurs de services nuagiques (CSP) ne sont pas suffisantes pour une externalisation conforme à la législation. Si les exigences légales ne sont pas respectées ou mises en œuvre, des risques de responsabilité et de réputation sont à craindre. Les personnes concernées peuvent porter plainte pour violation des droits fondamentaux.	• Prévoir des pouvoirs de contrôle du mandant, par exemple accès aux rapports d'audit, contrôles directs. • Les tâches de contrôle doivent être effectivement exécutées. • Prévoir une obligation d'information du CSP en cas d'incidents liés à la sécurité (cf. également risque n° 18) Mesures organisationnelles : • Clarification préalable de la mise en œuvre concrète des exigences juridiques générales et spécifiques à chaque domaine dans le cadre de projets d'informatique en nuage[3]. Cf.. partie 2, ch. 1.5.3, du rapport.
2	Communication de données à des États étrangers sans législation adéquate en matière de protection des données	C	Des données personnelles peuvent être communiquées à l'étranger si le Conseil fédéral a constaté que l'État concerné dispose d'une législation assurant un niveau de protection adéquat (art. 16, al. 1, nDSG) Si des données doivent être transmises à des États qui ne disposent pas d'une protection des données adéquate, des mécanismes de protection particuliers sont nécessaires. Ceux-ci peuvent être de nature contractuelle ou technique (art. 16, al. 2, nLPD).	Mesures contractuelles : • Lors de l'utilisation de solutions nuagiques, il faut garantir que les données ne sont traitées et stockées que dans un État étranger particulier ou des États étrangers particuliers et qu'un niveau de protection des données adéquat est garanti. • Obligation du CSP de conclure des clauses contractuelles types avec ses sous-traitants qui accèdent aux données personnelles depuis des États ne disposant pas d'une législation adéquate en matière de protection des données. Mesures techniques : • Cryptage des données qui exclut dans une large mesure l'accès au contenu personnel des données par le sous-traitant (étranger) (en particulier pour les *données au repos*).

[3] Utiliser les outils disponibles, en particulier l'analyse des besoins de protection (https://www.ncsc.admin.ch/ncsc/fr/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren/beurteilung-schutzbedarf.html) ; Concept de sécurité de l'information et de protection des données (SIPD) (https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren/erhoehter-schutz.html).

N°	Risque	Catégorie	Description du risque	Mesures possibles
				• Vérifier si des prescriptions concernant les *données en transit* sont possibles, par exemple concernant le routage. Cf. partie 2, ch. 1.2, du rapport.
3	Violation du droit en raison de l'applicabilité d'un droit étranger	C	Le cas échéant, la question se pose de savoir si le système juridique d'un pays de destination présente des risques particuliers, par exemple parce que les autorités de ce pays peuvent exiger l'accès aux données à l'insu de l'utilisateur du nuage (ou du moins sans qu'il ait la possibilité de s'y opposer) ou accéder au matériel (saisie).	Mesures contractuelles : • Obligation du CSP de se conformer au droit suisse applicable (en particulier à la loi sur la protection des données et, le cas échéant, aux lois spéciales) ; le for doit en principe être la Suisse. • Accords sur la manière dont le CSP répond aux questions des autorités ou aux procédures liées à la remise ou au transfert d'informations protégées. • Dans la mesure où la loi le permet (cf. partie 2, ch. 1.6, du rapport), les informations protégées ne devraient être transmises à des autorités étrangères : • qu'avec le consentement écrit de l'utilisateur du nuage, • que sur la base d'un jugement d'un tribunal suisse compétent, ou • qu'avec l'autorisation d'une autorité suisse. • Lorsque la loi l'autorise, ou qu'une injonction gouvernementale l'autorise, le CSP doit : • informer le client en temps utile s'il est confronté à une injonction d'une autorité étrangère concernant la transmission ou la divulgation de ses données stockées dans le nuage • donner à l'utilisateur du nuage le droit de mener la procédure et de participer au traitement des demandes des autorités étrangères • Si, en raison du droit impératif, le fournisseur n'est pas en mesure d'informer à l'avance l'utilisateur du nuage de la transmission ou de la divulgation d'informations protégées à des autorités étrangères ou à d'autres parties à l'étranger, il doit prendre les mesures juridiques ou de sécurité appropriées dans le cadre de l'accord conclu, dans l'intérêt de l'utilisateur du nuage. Définir les obligations de rapport du CSP et l'accès aux résultats des audits.

N°	Risque	Catégorie	Description du risque	Mesures possibles
				Mesures organisationnelles : • Le CSP informe suffisamment l'utilisateur de ses processus et des politiques d'accès aux données par les autorités pour permettre à l'utilisateur de prendre une décision éclairée à ce sujet. Mesures techniques : • Cryptage, en particulier des *données au repos* et *des données en transit*. • Gestion de la clef par le mandant (organe fédéral) ou, le cas échéant, par un fournisseur tiers. Le mandant autorise les utilisateurs et les processus et peut surveiller les autorisations. • Les conflits de lois (par ex. en cas de saisie de matériel informatique dans le cadre d'une procédure pénale à l'étranger, touchant également des données d'un organe fédéral) ne peuvent pas être totalement exclus. Cf. partie 2, ch. 1.2 et 1.6, du rapport.
4	Modification du cadre juridique en raison de la délocalisation des centres de calcul.	C	Cf. ch. 2 et 3. Traitement de données illicite sur des sites inconnus du mandant.	Mesures contractuelles : • Transparence permanente concernant les sites ; si possible, engagement du CSP concernant des sites spécifiques Cf.. partie 2, ch. 1.6, du rapport..
5	Les incidents de sécurité ne sont pas communiqués au mandant Confédération, les	C	En cas d'incident de sécurité grave, le mandant doit pouvoir analyser ce qui s'est passé, comment les pirates ont procédé, quels domaines ont été touchés et, le cas échéant, isoler ces derniers le plus rapidement possible.	Mesures contractuelles : • Réglementation de la défense en cas d'attaques contre des applications de la Confédération exploitées dans le nuage. • Définir les obligations de rapport du CSP et l'accès aux résultats des audits.

N°	Risque	Catégorie	Description du risque	Mesures possibles
	CSP ne prennent pas de mesures suffisantes.		Le mandant doit pouvoir définir des mesures pour éviter des incidents similaires. Le mandant doit pouvoir garder le contrôle de la gestion de la sécurité.	• Réglementation du soutien des services compétents de la Confédération (en particulier CSIRT/OFIT ; NCSC) par CSP (le cas échéant, prévoir une obligation de coopérer). Mesures organisationnelles : • Définir les responsabilités en matière de gestion des incidents de sécurité
6	Mesures de sécurité insuffisantes	T	Le CSP doit garantir au moins le même niveau de sécurité que le mandant. Les mesures de sécurité à prendre dépendent en particulier du type de données traitées et de la nécessité de compenser un niveau de protection des données inadéquat (résultat de l'analyse des besoins de protection). Des mesures spécifiques sont parfois prescrites à l'organe fédéral (par ex. concernant la journalisation, la conservation des données). L'utilisation d'appareils mobiles (privés) peut soulever des questions de sécurité (accès via des apps).	Mesures contractuelles : • Convenir des obligations supplémentaires avec le CSP (en particulier en cas de recours à des sous-traitants). • Le CSP doit présenter des rapports de contrôle qui documentent la sécurité des données (la preuve d'une certification ou d'une attestation de contrôle ne suffit pas). • Obligation du CSP de signaler les cyberattaques graves ayant un impact sur les données de la Confédération et les services achetés par la Confédération. Mesures organisationnelles : • Vérifier les conditions standard du CSP. • Établir un concept d'accès. • Accord concernant les contrôles sur place Mesures techniques : • Dispositions prises pour protéger l'intégrité et la disponibilité des données • L'accès à partir d'appareils mobiles se fait uniquement via une application sandbox Cf.. partie 2, ch. 1.2.2, du rapport.

N°	Risque	Catégorie	Description du risque	Mesures possibles
7	Saisie de matériel informatique contenant des données de la Confédération par des autorités à l'étranger	C	Si des supports de données sont saisis à l'étranger, l'utilisation commune de l'infrastructure matérielle peut entraîner la divulgation de données qui ne faisaient pas l'objet de l'injonction.	Mesures contractuelles : • Cf. no 3. Mesures organisationnelles : • éviter l'utilisation du nuage sur une infrastructure partagée pour certaines données (utilisation du nuage privé) Mesures techniques : • cryptage ; gestion de la clef par le mandant (organe fédéral) • séparation logique des données (propres mandants) Cf.. partie 2, ch. 1.2, du rapport.
8	Non-respect des dispositions légales en matière de protection des données ou de sauvegarde du secret	C	Le mandant doit s'assurer qu'au moins les prescriptions de la LPD (ou du RGPD) ainsi que les éventuelles prescriptions de lois spéciales sont respectées dans le domaine d'activité concerné. Dans la mesure où des données sont traitées dans des États qui ne disposent pas d'un niveau de protection des données adéquat, il convient d'examiner la nécessité d'accords supplémentaires avec le CSP. L'étendue de la responsabilité du CSP dépend également du modèle de nuage. Des règles d'accès peu claires peuvent entraîner des violations de la protection des données ou de la sauvegarde du secret.	Mesures contractuelles : • Formuler clairement les obligations du CSP. • Le CSP n'est pas autorisé à accéder aux données à des fins personnelles. Mesures organisationnelles : • Vérifier les spécifications de service du CSP. • Établir le concept d'accès. Mesures techniques : • Cryptage et gestion des clefs • Accès uniquement avec une authentification multifactorielle Cf.. partie 2, ch. 1.2, du rapport. Voir aussi risque n° 6

N°	Risque	Catégorie	Description du risque	Mesures possibles
9	Pression politique sur les CSP pour qu'ils coopèrent avec des autorités étrangères au détriment de la Confédération (divulgation de données, blocage de données)	P	Le cadre juridique et politique des pays dans lesquels les données sont hébergées ou traitées est dynamique et peut évoluer.	Mesures contractuelles : • Convenir de sites de traitement qui soient juridiquement et politiquement stables. • Convenir de clauses de sortie Mesures organisationnelles : • Examen régulier de lla situation juridique et politique • Contrôle régulier de la liste des États Mesures techniques : • Cryptage, gestion de la clef par le mandant (organe fédéral) Cf.. partie 2, ch. 1.2, du rapport.
10	Manque de personnel disposant d'une expertise adéquate	BC	Pas de risque spécifique au nuage. L'utilisateur du nuage doit avoir accès à des ressources adéquates pour l'exploitation d'environnements système hybrides. Il faut pouvoir garantir que les risques liés à l'externalisation dans le nuage sont évalués de manière exhaustive et que seuls des risques raisonnables sont pris. L'introduction de solutions nuagiques nécessite un processus d'adaptation globale des applications concernées et de préparation des collaborateurs.	Mesures organisationnelles : • Garantir l'accès aux ressources techniques nécessaires • Planification et préparation adéquates du projet • Soutien lors de la mise en service par le CSP • Échange de « bonnes pratiques » au sein de l'administration fédérale • Formation des collaborateurs qui travaillent avec l'application nuagique.

N°	Risque	Catégorie	Description du risque	Mesures possibles
13	Lacunes dans la collaboration entre la Confédération et le CSP, enraînant : arrêt ou modification imprévus du service, interruptions du service	BC	Les services peuvent ne plus être accessibles ou ne l'être qu'à des conditions différentes pour plusieurs raisons : Le CSP modifie les conditions standard événements dommageables Attaques La mesure dans laquelle de tels risques sont acceptables dépend des exigences en matière de continuité des activités des applications concernées.	Mesures contractuelles : • Le CSP doit communiquer suffisamment tôt les modifications importantes du service. • Option de sortie en cas de modification des conditions. • Réglementation de la collaboration avec le CSP pour les procédures de récupération, les analyses forensiques, l'utilisation illégale ou abusive des ressources. • Compensation financière ou peines conventionnelles pour les interruptions du service imprévues particulièrement critiques. Mesures organisationnelles : • surveillance des activités des CSP et des sous-traitants • planification alternative pour les pannes (BC). Mesures techniques : • Garantir que les données (éventuellement en Suisse) sont disponibles indépendamment de l'application nuagique (sauvegardes ou miroirs) • Mettre en œuvre des procédures de récupération Cf.. partie 2, ch. 1.2, du rapport. Voir aussi risque n° 16
14	Attaques par des collaborateurs malveillants	BC	Pas de risque spécifique au nuage, mais il est possible qu'un risque s'aggrave dans l'environnement nuagique. Les architectures nuagiques nécessitent des accès et des autorisations hautement privilégiés. Les auteurs d'attaques internes peuvent avoir la possibilité de	Mesures contractuelles : • Réglementation claire des compétences des administrateurs (des deux parties) • Réglementation contractuelle des procédures de sécurité à appliquer (le cas échéant, sur la base de conditions générales). • Le cas échéant, régler contractuellement les procédures et les contrôles de sécurité pour les collaborateurs du CSP ou convenir d'options correspondantes (par ex. *Advanced Secure Support*)

N°	Risque	Catégorie	Description du risque	Mesures possibles
			manipuler des données, de les transmettre à des personnes non autorisées ou de perturber la disponibilité d'un service. Le risque est plus élevé dans un scénario d'externalisation que dans un traitement sur site, notamment parce que l'utilisateur ne peut pas effectuer lui-même les contrôles de sécurité. Le risque dépend du modèle de nuage utilisé.	Mesures organisationnelles : • Aligner les modèles de rôles sur l'application nuagique, • Établir des concepts d'accès. Mesures techniques : • Journalisation • Application stricte du principe du besoin d'en connaître
15	Risques liés à l'utilisation commune de l'infrastructure (*multi-tenancy*, technologies partagées) ; défaillance de l'isolation, en particulier en cas d'attaque.	T	Dans le modèle de nuage public, le CSP partage généralement les ressources entre plusieurs clients. L'isolation des données peut alors être défectueuse ; une séparation logique est, du point de vue actuel, moins sûre qu'une séparation physique des données. Le risque peut être réduit par des mesures techniques, mais il ne peut pas être complètement éliminé.	Mesures techniques : • Cryptage • Traitement sécurisé • Architectures VM spécifiques et sécurisées Cf.. partie 2, ch. 1.2, du rapport.
16	Dépendance vis-à-vis du fournisseur (*vendor lock-in*), portabilité limitée des données	BC	Changer de fournisseur peut s'avérer difficile d'un point de vue technologique et économique. Le changement peut toutefois être nécessaire, ne serait-ce que	Mesures contractuelles : • Convenir d'un scénario de sortie (*opt-out*). • Régler l'exportation et la migration des données (par ex. APIs). Tenir compte du fait que les données peuvent être peu utiles sans la logique correspondante (par ex. modèle SaaS). Mesures organisationnelles :

N°	Risque	Caté-gorie	Description du risque	Mesures possibles
			pour des raisons de droit des marchés publics[4]. Il se peut que les CSP n'offrent qu'un soutien très limité lorsque les données sont migrées du nuage vers un autre fournisseur ou qu'elles reviennent dans leur propre environnement « sur site ». Le cas échéant, un CSP peut rendre de telles migrations plus difficiles, de manière active ou passive. Une migration peut nécessiter des adaptations organisationnelles ou techniques importantes.	• Planification BC pour changement de fournisseur ou rapatriement Définir une stratégie de sortie au démarrage du projet Mesures techniques : • Choisir une architecture (couche d'abstraction) qui permette l'exploitation indépendamment du modèle de nuage ou du fournisseur sous-jacent. • Mise à disposition d'APIs pour la migration • Clarifier si les structures de données propriétaires du CSP sont documentées et accessibles au mandant. • Documentation des formats d'exportation. • Définir les routines d'importation (*mapping*). • Garantir que les données (éventuellement en Suisse) sont disponibles indépendamment de l'application nuagique (sauvegardes ou miroirs)
17	Gestion des clefs insuffisante	BC, T	Les risques peuvent provenir du fait que le CSP ou des sous-traitants peuvent avoir accès aux clefs lorsque celles-ci doivent être stockées dans le nuage et sont donc logiquement et physiquement sous le contrôle du CSP. D'autre part, si la gestion des clefs est mal organisée, il y a un risque de perte de données.	Mesures organisationnelles : • Clarifier (éventuellement par contrat) où (chez le CSP ou chez des tiers impliqués) le cryptage a lieu, qui génère quelles clefs de décryptage et où ces clefs sont physiquement stockées pour chaque étape de traitement). • Définir le système de rôles, clarifier les responsabilités (règlement de traitement) • Utiliser les bonnes pratiques Mesures techniques : • Détection de l'utilisation non autorisée d'une clef

[4] Pour les externalisations en nuage dans le cadre des services achetés au moyen de l'appel d'offres OMC 20007, la durée des contrats-cadres est de 5 ans à compter du 14 juin 2021 (date de l'adjudication) (une prolongation est à l'étude).

N°	Risque	Catégorie	Description du risque	Mesures possibles
			Enfin, il faut garantir que les clefs sont effacées si nécessaire, en particulier lorsque des fournisseurs d'hébergement sont impliqués.	Cf.. partie 2, ch. 1.2, du rapport.
18	Logiciels compromis, composants matériels compromis (*backdoors*)	T	Ce risque se présente sous différentes formes : - Cryptage (clef générale/clef supplémentaire) - Failles de sécurité (*zero days*) non divulguées et utilisées, par exemple par les services de renseignement - *Backdoors* matérielles, puces espions Le risque peut être réduit, mais pas totalement éliminé.	Ce risque existe aussi en grande partie pour les solutions sur site. Mesures contractuelles : • Garantie que les demandes d'accès aux données émanant d'autorités étrangères ne sont traitées que dans le cadre des procédures juridiques prévues dans chaque cas et que les CSP prennent les mesures juridiques applicables. • Engagement du CSP à respecter les normes ISO. • Obligation d'informer en cas d'incidents de sécurité et d'attaques (réussies ou non) contre des données de la Confédération. • Accès de l'organe fédéral responsable aux résultats des audits. Mesures techniques : • Utilisation de *Trusted Platform Modules* • Cryptage, gestion de la clef par le mandant (organe fédéral)
19	Intégrité du système et interfaces de gestion compromises lors de l'accès via Internet	T	Lors de l'utilisation de services en nuage via Internet, des personnes non autorisées peuvent accéder aux applications et aux données en attaquant les interfaces de gestion.	Mesures contractuelles : • Définir l'information de l'organe fédéral responsable en cas d'attaques. • Garanties contractuelles concernant la détection des vulnérabilités par le fournisseur. • Directives relatives à la sécurité des personnes au sein du CSP et des sous-traitants Mesures organisationnelles :

N°	Risque	Catégorie	Description du risque	Mesures possibles
				• Clarifier la collaboration des administrateurs du côté des CSP et de la Confédération. Définir clairement la gestion des autorisations et des accès. Mesures techniques : • Test d'intrusion par l'administration fédérale, pour les systèmes très sensibles. • Restrictions d'accès aux adresses IP des clients autorisés
20	Effacement des données non sécurisé ou incomplet	C, T	L'effacement sûr et complet des données est nécessaire, en particulier dans les scénarios suivants : - Changement de fournisseur - Délais légaux maximaux, en particulier pour la conservation des données personnelles (en particulier aussi pour les données secondaires) - Mise en œuvre des demandes d'effacement des données personnelles.	Les processus du CSP concernant la suppression des données doivent être clarifiés au préalable. Mesures contractuelles : • Garantir l'accès aux résultats des audits qui certifient le respect des processus. • Prévoir une information/confirmation des effacements. • Convenir d'une obligation de confidentialité de durée indéterminée de la part du CSP (et des sous-traitants). Mesures organisationnelles : • Documenter les responsabilités en matière d'effacement des données. Mesures techniques : • Cryptage, gestion de la clef par le mandant (organe fédéral)
21	Capacités réseau insuffisantes	T	Pas de risque spécifique au nuage. La disponibilité des services nuagiques dépend en particulier de la disponibilité des réseaux utilisés pour l'échange de données.	Mesures contractuelles : • Exiger des engagements (du CSP ou, le cas échéant, d'un exploitant de réseau tiers) en matière de disponibilité (respect des normes/bonnes pratiques). • Convenir de peines conventionnelles qui seront dues si certains objectifs de disponibilité ne sont pas respectés.

N°	Risque	Caté-gorie	Description du risque	Mesures possibles
			Une bande passante insuffisante peut avoir pour conséquence que la disponibilité des services nuagiques ne soit pas suffisante. L'ampleur du risque dépend également du niveau de disponibilité du service ou de l'application concernés.	Mesures organisationnelles : • Clarifier l'alerte par le CSP • Définir les mesures BC en cas de défaillance du service Mesures techniques : • Prévoir des redondances • Connexion de l'administration fédérale aux fournisseurs de nuage public via le Cloud Exchange Provider (CXP). • Utilisation du futur service standard Transmission de données
22	Non-respect des obligations contractuelles par le CSP	C	Le CSP doit garantir la mise en œuvre de ses obligations conformément au contrat.	Mesures contractuelles : Exclusion des modifications contractuelles unilatérales. Alternative : possibilité d'informer suffisamment tôt des modifications du contrat. Droits de résiliation en cas de modification du contrat Responsabilité appropriée en cas de non-respect du contrat par le CSP et les sous-traitants, pas d'exclusion en cas de négligence grave ou de faute intentionnelle (là où le droit étranger le permet).