Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF

Administration fédérale des finances AFF
Service juridique et gestion des risques
Gestion des risques et politique en matière d'assurance

Manuel de gestion des risques de la Confédération

Version du 15 septembre 2022

Contrôle des modifications

Quand	Qui	Description
21.11.2011	rch	Première version (vérifiée par Kessler et par AON)
24.05.2013	rch	Ajout de l'agrégation des risques transversaux (y c. annexe «Feuille d'information sur les risques transversaux de la Confédération»)
24.05.2013	rch	Ajout du processus d'actualisation des risques
10.09.2015	mlu	Remaniement des interfaces, des risques liés à l'informatique, des définitions et corrections de nature rédactionnelle
28.09.2017	elm/Gre	Remaniement de l'identification des risques (nouveaux: alinéas ressources, niveau) et des interfaces (nouveau: 6.5 Engagements conditionnels, annexe 6; complètement remaniés: 6.2 Gestion des cas d'urgence et des crises, 6.3 Gestion de la continuité; 6.4 Analyse de la situation et de l'environnement).
23.11.2018	elm/Gre	Remaniements et compléments concernant la stratégie en matière de risques des unités administratives et des départements (1.2.1), l'intégration de la gestion des risques dans les processus de conduite (2.3), la surveillance des risques (3.6.1), les risques transversaux (4.3 et annexe 10), la classification (5.3.1), la gestion des assurances (6.7), les annexes 1, 2, 7 et 11 (nouveau)
29.05.2020	Gre	Correction de l'introduction de l'annexe 10
14.09.2020	Gre	Remaniement classification des informations et principe de la transparence (nouveau ch. 5.3.1)
24.09.2021	afl	Remaniement du ch. 6.8 Unité de pilotage informatique de la Confédération (nouveaux: 6.8 Centre national pour la cybersécurité [NCSC] et 6.9 Secteur Transformation numérique et gouvernance de l'informatique [TNI])
22.03.2022	ade	Correction des illustrations 3&7
du 07.07 au 02.09.2022	elm / afl	Présentation des principales fonctions de la gestion des risques de la Confédération (ch. 2.2), complément concernant l'actualisation des risques (ch. 3.1.2) et le choix du propriétaire d'un risque transversal (ch. 4.3.3), mise à jour et ajout concernant le gouvernement d'entreprise (ch. 6.6), complément concernant le NCSC (ch. 6.8), mise à jour de la définition du propriétaire du risque dans le glossaire (annexe 1), remplacement des modèles de rapport (annexe 2), nouvelle version des parties «Protection des infrastructures critiques» et «Analyse nationale des risques» (annexe 8)

Table des matières

Annexes

Liste des illustrations

Les désignations de fonction prennent la forme masculine dans le présent manuel pour faciliter la lecture. Elles s'appliquent toutefois aux deux sexes.

Liste des abréviations

AFF	Administration fédérale des finances
ACF	Arrêté du Conseil fédéral
BCM	*Business Continuity Management* (gestion de la continuité de l'activité)
CaSUS	Catastrophes et situations d'urgence en Suisse
CdG	Commissions de gestion
CENAL	Centrale nationale d'alarme
CF	Conseil fédéral
CGR	Conseiller en gestion des risques
ChF	Chancellerie fédérale
CSG	Conférence des secrétaires généraux
CTE	Coordination des transports dans l'éventualité d'événements (voir RS *520.16*)
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DEFR	Département fédéral de l'économie, de la formation et de la recherche
DélSéc	Délégation pour la sécurité
DETEC	Département fédéral de l'environnement, des transports, de l'énergie et de la communication
DFAE	Département fédéral des affaires étrangères
DFF	Département fédéral des finances
DFI	Département fédéral de l'intérieur
DFJP	Département fédéral de justice et police
EMPOC	État-major «Prise d'otage et chantage» (voir RS *172.213.80*)
ISO	Organisation internationale de normalisation
IT	*Information Technology* (technologie de l'information)
LAr	Loi fédérale sur l'archivage (RS *152.1*)
LFC	Loi sur les finances de la Confédération (RS *611.0*)
LMP	Loi fédérale sur les marchés publics (RS *172.056.1*)
LOGA	Loi sur l'organisation du gouvernement et de l'administration (RS *172.010*)
LRCF	Loi sur la responsabilité (RS *170.32*)
LTrans	Loi fédérale sur le principe de la transparence dans l'administration (RS *152.3*)
NCSC	Centre national pour la cybersécurité (National Cyber Security Centre)
OEMFP	Ordonnance sur l'État-major fédéral Protection de la population (RS *520.17*)
OFAE	Office fédéral pour l'approvisionnement économique du pays
OFC	Ordonnance sur les finances de la Confédération (RS *611.01*)
OFPP	Office fédéral de la protection de la population
OFSP	Office fédéral de la santé publique
ÖNORM	Réglementation de l'organisme autrichien de normalisation
OPrI	Ordonnance concernant la protection des informations (RS *510.411*)
OSANC	Organe sanitaire de coordination (voir RS *501.31*)
PC	*Personal Computer* (ordinateur personnel)
PIC	Protection des infrastructures critiques
R2C_GRC	Risk to Chance Gouvernance, gestion des risques et conformité (logiciel de gestion des risques de la Confédération)
RNS	Réseau national de sécurité
SCI	Système de contrôle interne
SIPD	Sûreté de l'information et protection des données
SOPA	Cellule spéciale pandémie (voir RS *818.101.23*)
SRC	Service de renseignement de la Confédération
TED	Traitement électronique des données
TNI	Transformation numérique et gouvernance de l'informatique
UA	Unité administrative
UO	Unité d'organisation

0 But du présent document

Le présent manuel de gestion des risques de la Confédération complète et commente les directives sur la gestion des risques menée par la Confédération[1]. Il est édicté par l'Administration fédérale des finances (AFF), après consultation des responsables de la gestion des risques des départements et de la Chancellerie fédérale (ChF).

Le manuel s'appuie sur les systèmes normatifs usuels[2]. Les termes utilisés pour la gestion des risques au sein de la Confédération sont expliqués plus avant ou définis à l'annexe 1. Le manuel aide les personnes participant à la gestion des risques (principalement les responsables de la gestion des risques des départements et des unités administratives [UA] et les propriétaires des risques) à accomplir leurs tâches; il sert également d'ouvrage de référence aux cadres et aux collaborateurs de l'administration fédérale pour les questions relatives à la gestion des risques de la Confédération.

Les encadrés sur fond gris comportent, d'une part, des prescriptions obligatoires et, d'autre part, des recommandations destinées aux responsables de la gestion des risques des départements et des UA. Ces prescriptions sont nécessaires pour permettre une mise en œuvre uniforme de la gestion des risques et un rapport consolidé au niveau du Conseil fédéral.

Le présent manuel régit les principaux éléments du système de gestion des risques de la Confédération, notamment:

- la politique de gestion des risques (voir le ch. 1);
- l'organisation de la gestion des risques au sein de la Confédération (voir le ch. 2);
- les descriptifs des fonctions dans la gestion des risques de la Confédération (voir le ch. 2.2);
- le processus de gestion des risques (voir le ch. 3);
- le rapport sur les risques (voir le ch. 4);
- la communication au sein de la gestion des risques (voir le ch. 5);
- les interfaces entre la gestion des risques et les autres processus et organisations (voir le ch. 6).

Le manuel sera adapté régulièrement aux besoins actuels et enrichi. Les départements et la ChF peuvent soumettre des propositions en ce sens.

1 Bases de la gestion des risques de la Confédération

1.2 Politique de gestion des risques

La politique de gestion des risques menée par la Confédération définit les objectifs dans ce domaine et présente les avantages qu'apporte une telle gestion.

1.1.1 Objectifs

La gestion des risques constitue un instrument de pilotage au niveau du Conseil fédéral (CF), des départements / de la ChF et des UA. Elle assure la transparence sur la situation actuelle de la Confédération et des différentes unités d'organisation (UO) en matière de risques et permet de prendre à temps les mesures requises pour prévenir ou atténuer ces derniers. La gestion des risques de la Confédération:

[1] Les directives ont été édictées par l'AFF sur la base du ch. 6, al. 1, des directives du 24 septembre 2010 sur la politique de gestion des risques menée par la Confédération (voir FF **2010** 5965; ci-après directives du CF sur la politique de gestion des risques).

[2] Concrètement: ISO 31000, ÖNORM 4900 ss

- soutient l'exécution des tâches légales et constitutionnelles de l'administration fédérale ainsi que l'atteinte des objectifs de la Confédération;
- permet au Conseil fédéral et à l'administration fédérale de prendre leurs décisions en tenant compte des événements et des évolutions qui sont susceptibles de se produire à l'avenir et dont les principaux effets négatifs sur la réalisation des tâches et des objectifs sont identifiés précocement et analysés;
- vérifie régulièrement sa propre efficacité et garantit une amélioration et un développement constants.

Il faut, par ailleurs, garantir la sécurité des représentants de la Confédération, protéger le patrimoine et la réputation de la Confédération et employer de manière efficace et économique les moyens à disposition[3].

1.1.2 Avantages

Exécutée selon des critères uniformes, la gestion des risques présente de nombreux avantages pour la Confédération[4]:

- elle contribue à assurer une exécution prévoyante des tâches de la Confédération et encourage une conduite proactive;
- elle contribue au bon fonctionnement du gouvernement et de l'administration;
- elle accroît la transparence et la vue d'ensemble de la situation en matière de risques et facilite dès lors la prise de décision à tous les échelons hiérarchiques;
- elle permet une répartition efficace et économique des ressources nécessaires pour atténuer les risques;
- elle contribue à renforcer la confiance des parties prenantes (Assemblée fédérale, population, etc.) dans l'administration fédérale et le Conseil fédéral;
- elle sensibilise les collaborateurs de l'administration fédérale aux risques inhérents à leur domaine d'activité.

Pour bénéficier des avantages et atteindre les objectifs mentionnés, il faut que la gestion des risques soit considérée, implémentée et mise en œuvre dans la pratique comme une partie des processus de conduite et de pilotage. Le ch. 2.3 fournit des précisions à ce sujet.

1.3 Stratégie et culture en matière de risques

1.2.1 Stratégie en matière de risques

En établissant une stratégie en matière de risques, une organisation détermine comment elle entend gérer les risques. Au sens strict, une telle stratégie consiste à définir le rapport entre les chances et les risques et à fixer la limite que les risques encourus ne doivent pas dépasser (tolérance au risque, actions possibles pour maîtriser les risques, voir également le ch. 3.4).

De manière plus générale, la stratégie en matière de risques montre comment la gestion des risques doit être conçue et mise en œuvre. Elle comprend l'engagement de la haute direction concernant la gestion des risques. Dans les grandes organisations, il s'avère en outre judicieux de définir une stratégie concernant l'ensemble de l'organisation (souvent appelée «politique de gestion des risques»), qui est ensuite précisée par des stratégies distinctes au niveau des unités d'organisation inférieures.

[3] Ch. 3, al. 1, des directives du CF sur la politique de gestion des risques

[4] Ch. 3 des directives du CF sur la politique de gestion des risques

Stratégie en matière de risques au niveau de la Confédération

Le Conseil fédéral a établi la stratégie (globale) de la Confédération en matière de risques dans ses directives sur la politique de gestion des risques. Ces directives comportent principalement la définition du risque, le champ d'application des directives, les buts, les principes et les fonctions de la gestion des risques.

S'agissant de la tolérance au risque et de la maîtrise des risques, il est généralement admis que les risques liés à l'exécution des tâches légales ne peuvent pas être complètement évités. La Confédération est prête à prendre sciemment des risques contrôlés si cela est indispensable à l'atteinte des objectifs ou à l'exécution des tâches. Conformément au principe d'une utilisation économe des ressources de la Confédération, les risques pris lors de l'accomplissement des tâches fédérales doivent demeurer aussi faibles que possible. L'application de mesures de réduction du risque est décidée en fonction d'une analyse coûts / avantages (y c. pesée des intérêts[5]).

En principe, la Confédération assume le risque pour les dommages causés à son patrimoine et supporte les conséquences de son activité sur le plan de la responsabilité civile[6] (principe de l'auto-assurance). L'AFF n'autorise un transfert du risque financier (par ex. par l'intermédiaire d'un contrat d'assurance, de dérivés, etc.) que dans des cas particuliers[7].

Stratégie en matière de risques au niveau des départements et des UA

Au niveau des départements / de la ChF et des UA, la stratégie en matière de risques doit montrer comment chaque direction entend mettre en œuvre dans son propre domaine la politique de gestion des risques du Conseil fédéral et quels objectifs spécifiques elle a l'intention d'atteindre. Une telle stratégie devrait notamment inclure les aspects suivants[8]:

- engagement et intention de la haute direction;
- objectifs et avantages visés par l'unité d'organisation (UO) en matière de gestion des risques;
- paramètres en vue de la mise en œuvre d'une gestion intégrée des risques dans l'UO, c'est-à-dire l'interaction visée entre les processus de conduite et la gestion des risques (voir le ch. 2.3);
- fonctions, tâches et attentes en matière de gestion des risques;
- maîtrise des risques (stratégie en matière de risques au sens strict): procédure d'appréciation de la tolérance au risque (voir le ch. 3.4), actions possibles pour maîtriser les risques, pilotage des mesures visant à réduire le risque, définition de l'objectif de réduction.

Tous les cadres et les collaborateurs de l'UO doivent connaître la stratégie en matière de risques. Cette dernière doit servir de base pour les décisions relatives à la conduite et fait partie intégrante de la culture du risque visée.

1.2.2 Culture du risque

Une culture du risque adéquate constitue l'une des conditions principales pour une gestion des risques efficace et prévoyante: tous les collaborateurs et les cadres ont parfaitement conscience des risques et entretiennent une culture positive de l'erreur.

- ***Gestion des erreurs:*** une culture positive de l'erreur permet de discuter ouvertement des déficiences et encourage la couverture des risques inhérents aux processus et aux systèmes. Des solutions peuvent être élaborées pour réduire ces risques. De plus, une communication ouverte permet d'apprendre des erreurs des autres.

---

[5] Par ex.: dignité humaine, indisponibilité du corps humain (vie et intégrité corporelle), propriété, etc.

[6] Art. 50, al. 2, OFC (RS **611.01**)

[7] Voir les directives de l'AFF du 11 septembre 2015 applicables à la prise en charge des risques et au règlement des sinistres à la Confédération

[8] Voir le projet de modèle «Stratégie en matière de risques» (annexe 11)

- ***Échange d'informations transparent et culture d'apprentissage:*** la volonté d'apprendre des autres et une communication ouverte qui tient compte des prescriptions de sécurité relatives aux informations classifiées (voir le ch. 1.4) favorisent auprès des collaborateurs et des cadres une meilleure compréhension de leurs propres tâches et processus. Cela facilite notamment l'identification et la maîtrise des risques liés à une interface entre deux ou plusieurs UO. Chaque domaine bénéficie des expériences des autres.
- ***Respect du savoir et des possibilités techniques:*** l'analyse des risques et l'élaboration des différentes solutions pour les surmonter doivent reposer sur l'avis de personnes dotées d'un vaste savoir-faire, même si elles n'ont aucun pouvoir décisionnel. Les avis de ces personnes et les décisions éventuellement divergentes de la hiérarchie (*management overruling*) seront documentées.
- ***Obligation d'informer:*** l'obligation pour chaque collaborateur d'informer ses supérieurs hiérarchiques des dangers pertinents dans son domaine d'activité renforce la vigilance et se traduit par un comportement responsable en matière de risques.

En vue d'améliorer la culture du risque, il est important de promouvoir des principes généraux, mais aussi de discuter régulièrement des sujets liés à la gestion des risques. Il s'agit d'encourager la prise de conscience des risques et la sensibilisation à la gestion des risques (voir également le ch. 5.1).

Il va de soi que le développement ou l'amélioration de la culture du risque ne peut se réaliser du jour au lendemain. Cela prend du temps, car les habitudes de travail et les mentalités changent en général très lentement. L'AFF portera une attention particulière à ce thème dans le cadre de l'amélioration régulière de la gestion des risques de la Confédération et, le cas échéant, elle prendra des mesures en vue d'autres améliorations.

1.4 Champ d'application et définition du risque

En matière de gestion des risques, la définition du risque est délimitée matériellement par les tâches et les objectifs de l'administration fédérale. La définition précise du risque est la suivante:

Texte de la définition	Élément défini
Par risques, on entend des événements et développements	*Type de survenance (immédiate ou progressive)*
qui ont une certaine probabilité de se produire	*Incertitude*
et qui ont des conséquences négatives majeures d'ordre financier et non financier	*Importance, type de conséquences*
sur l'atteinte des objectifs et l'exécution des tâches	*Périmètre matériel*
dans l'administration fédérale.	*Périmètre institutionnel*

La gestion des risques de la Confédération est assurée dans l'administration fédérale centrale et dans les unités décentralisées qui n'ont pas de comptabilité propre[9].

1.5 Traitement des informations classées «SECRÈTES»

La gestion des risques porte sur *tous* les domaines de tâches de la Confédération, donc également sur des domaines très sensibles tels que la sécurité intérieure et extérieure. Les risques correspondants figurent, eux aussi, dans le rapport sur les risques destiné au Conseil fédéral. Les informations classées SECRÈTES doivent être répertoriées de manière adéquate dans la gestion des risques. La protection des informations de la Confédération et de l'armée dans l'intérêt du pays, et notamment leur classification et leur traitement, est réglementée dans l'ordonnance concernant la protection des informations (OPrI)[10]. Le ch. 0 ci-après expose la classification des informations relatives à la gestion des risques.

[9] La définition du risque et le champ d'application figurent au ch. 2 des directives de l'AFF sur la gestion des risques de la Confédération.
[10] RS **510.411**

2 Organisation de la gestion des risques à la Confédération

2.1 Mise en place

La gestion des risques s'appuie sur une organisation décentralisée au sein de l'administration fédérale. Les départements et la ChF sont responsables de la mise en œuvre dans leur domaine. Une fonction de gestion des risques est prévue au niveau des départements / de la ChF et dans chaque UA[11]. La personne exerçant cette fonction assure la coordination des différentes activités liées à la gestion des risques et pilote le processus correspondant. De son côté, le service de coordination Gestion des risques de l'AFF (service de coordination de l'AFF) assume une fonction interdépartementale et veille à une mise en œuvre uniforme de la gestion des risques dans l'administration fédérale.

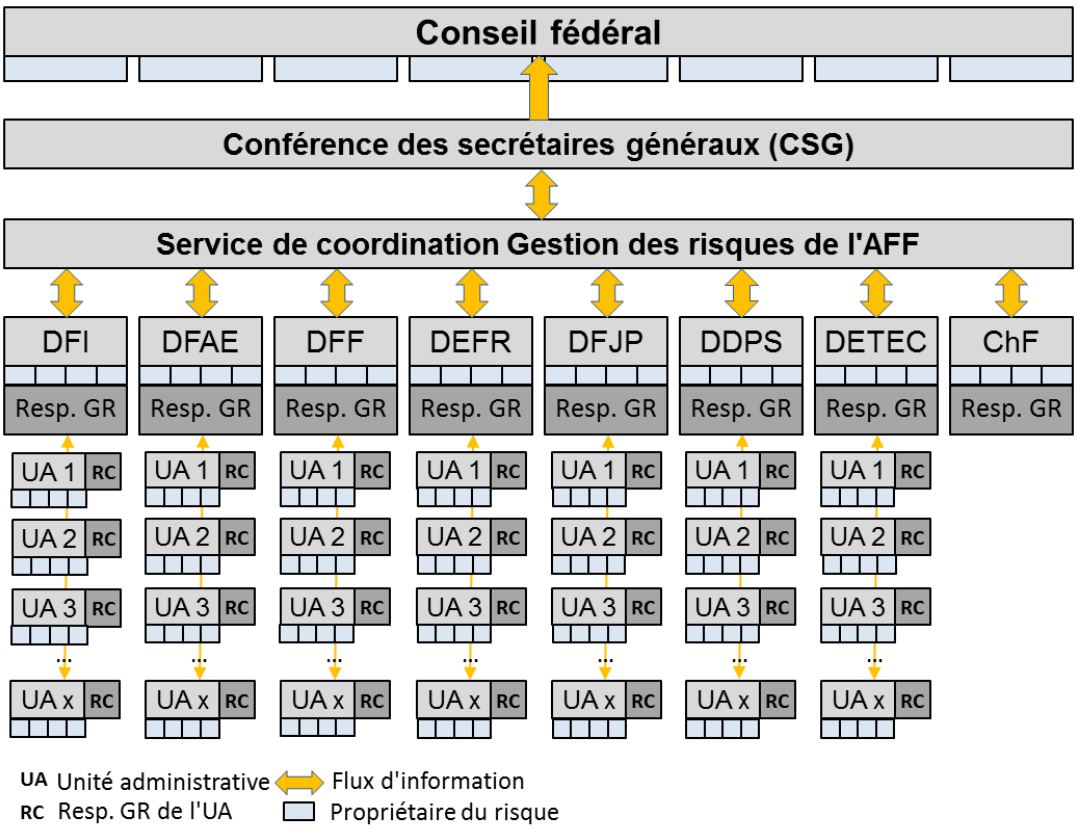


Illustration 1: Organisation de la gestion des risques à la Confédération

2.2 Fonctions et responsabilités

Les tâches et les responsabilités des différentes fonctions dans la gestion des risques au sein de la Confédération sont décrites au ch. 3 des directives de l'AFF. Voici les principales fonctions:

- **Responsable de la gestion des risques de l'UA:** personne chargée de l'application adéquate de la méthodologie de la gestion des risques de la Confédération au sein de l'UA, de la ***mise*** en œuvre du processus de gestion des risques ainsi que des conseils à la direction, aux propriétaires des risques et aux responsables des mesures (voir également l'annexe 4 Cahier des charges).

[11] Cela vaut également pour les secrétariats généraux. La fonction de responsable de la gestion des risques au sein du Secrétariat général peut être exercée par le responsable de la gestion des risques du département, mais ce n'est pas une obligation.

- **Responsable de la gestion des risques du département:** fonction analogue à celle décrite ci-dessus, mais au niveau du département. De plus, cette personne veille dans son département à l'application uniforme de la méthodologie et à son développement en collaboration avec le service de coordination, à la mise en œuvre et à la qualité des rapports ainsi qu'à des échanges spécialisés réguliers entre les responsables de la gestion des risques des UA et les fonctions apparentées telles que le système de contrôle interne (SCI) ou la gestion de la continuité de l'activité (*Business Continuity Management*, BCM; voir également l'annexe 4 Cahier des charges).
- **Propriétaire du risque:** personne qui gère un risque de manière dynamique grâce à ses mesures de réduction du risque et qui est chargée du rapport sur les risques. Elle dispose des compétences décisionnelles nécessaires. Lorsque les risques ont une portée particulière (risques transversaux, par ex.), il est également possible de confier en plus la responsabilité du risque à un organe stratégique, qui est informé des principales questions liées à la gestion, y participe ou prend des décisions en la matière.
- **Responsable des mesures:** personne mandatée par le propriétaire du risque pour gérer une mesure spécifique visant à réduire le risque.

Les fonctions de l'administration fédérale nécessitant un contrôle de sécurité relatif aux personnes (par ex. responsables de la gestion des risques du département) sont répertoriées à l'annexe 1 de l'ordonnance sur les contrôles de sécurité relatifs aux personnes (OCSP; RS *120.4*).

2.3 Gestion des risques dans les processus de conduite de l'administration fédérale

«La gestion des risques est un instrument de pilotage. Elle fait partie intégrante des processus de travail et de conduite et contribue à une exécution soigneuse et économe des tâches.»[12] Avec ce premier principe des directives sur la politique de gestion des risques menée par la Confédération, le Conseil fédéral engage les directions de tous les échelons hiérarchiques à s'assurer que la gestion des risques:

1. est étroitement liée aux processus de conduite et que la notion de risque est systématiquement prise en considération dans le travail de conduite (intégration fonctionnelle);
2. est mise en œuvre à tous les échelons de la conduite et que le flux d'informations entre ces échelons est garanti, de haut en bas et de bas en haut (intégration verticale);
3. est mise en réseau avec les autres processus d'aide à la conduite – par exemple, la gestion financière, le pilotage informatique ou le système de contrôle interne – et exploitée de manière coordonnée (intégration horizontale).

La mise en œuvre pratique de ces trois points d'une *gestion intégrée des risques* est exposée dans les chapitres qui suivent.

2.3.1 Intégration fonctionnelle: prise en compte dans les processus de planification et de stratégie

Les tâches de conduite comprennent une gestion consciente et rationnelle de l'incertitude: les risques possibles dans le domaine de l'exécution des tâches et de l'atteinte des objectifs doivent être identifiés en temps utile et traités de manière systématique. La gestion des risques de la Confédération prévoit à cet effet les instruments, méthodes et rôles qui conviennent[13]. L'intégration fonctionnelle de la gestion des risques requiert une collaboration optimale entre les responsables de la conduite et leurs spécialistes de la gestion des risques (responsable de la gestion des risques du département, responsables de la gestion des risques des UA) telle qu'elle est exposée au ch. 2.1. Cette collaboration se caractérise par les critères suivants:

[12] Ch. 4, al. 1, des directives du CF sur la politique de gestion des risques

[13] Description détaillée au ch. 3.1.3 du présent document (Flux d'informations concernant la gestion des risques de la Confédération) ainsi qu'au ch. 3 des directives de l'AFF sur la gestion des risques de la Confédération (Fonctions et responsabilités)

- **Les cadres** utilisent la gestion des risques dans leurs tâches de conduite et la prennent en compte systématiquement dans leurs processus de conduite. Ils l'intègrent notamment dans les processus ordinaires de planification et de stratégie ainsi qu'en cas de changement important interne ou externe à l'organisation. Ils analysent généralement deux fois par année la situation en matière de risques dans leur UO et examinent au sein de la direction la mise en œuvre et l'efficacité des mesures.
- **Les spécialistes de la gestion des risques (responsables de la gestion des risques des UA et les responsables des départements)** conseillent les cadres avec compétence et soutiennent les processus décisionnels au sein de la direction en apportant des informations pertinentes et des propositions convaincantes. Ils tiennent à jour le portefeuille des risques et des mesures, ils coordonnent les processus d'établissement des rapports et les soumettent à la direction[14].

Un *échange régulier et ciblé* entre la direction et les spécialistes de la gestion des risques est indispensable pour la réussite de l'intégration fonctionnelle. Tout d'abord, cet échange doit avoir lieu lors de la préparation des plans et des stratégies, notamment lors de la *planification stratégique ordinaire* des UA, des départements et de la ChF, dont découlent (tous les quatre ans) les objectifs de la législature, et qui est actualisée annuellement. Formellement, cette planification figure dans les objectifs annuels du Conseil fédéral et des départements. Au cours du processus budgétaire (budget assorti d'un plan intégré des tâches et des finances [PITF]), les objectifs et les projets sont dotés de ressources, puis ils sont mis à jour, précisés et détaillés dans les *conventions* annuelles *de prestations entre le département et l'UA*. En dehors de ces processus standardisés de planification, *des modifications importantes concernant les tâches, les stratégies et les objectifs* peuvent être apportées en tout temps dans le cadre de la procédure politique et nécessiter un recours aux spécialistes de la gestion des risques. Une prise en compte immédiate des risques dans les processus de planification et de stratégie permet de prendre des décisions viables et contribue ainsi à une utilisation efficiente des ressources (voir le ch. 1.1.2 Avantages).

Ensuite, un dialogue sur les risques s'instaure entre la direction et les spécialistes de la gestion des risques pendant l'établissement du *rapport sur les risques* et l'*actualisation des risques*. Contrairement à l'approche suivie pour les processus de planification, les risques sont ici au centre de l'attention. Alors que l'établissement du *rapport* permet d'évaluer de manière globale l'exposition des UA aux risques (actualisation des risques existants, examen des nouveaux risques possibles et suppression des risques devenus obsolètes), l'*actualisation des risques* se concentre sur les principaux risques à transmettre au Conseil fédéral[15]. Les rapports qui découlent de ces deux processus sont soumis pour approbation à la direction, puis remis à l'échelon hiérarchique supérieur.

Enfin, il est essentiel que la direction examine en profondeur, au moins une fois par législature, l'exposition aux risques et la gestion des risques de ses UA. Le but de cet examen est d'identifier et d'évaluer au moyen d'une approche descendante les champs de risques importants à moyen terme et de vérifier le fonctionnement de sa propre gestion des risques.

[14] Les rapports sur les risques sont les principales contributions visibles de la gestion des risques et ils constituent un critère central de qualité (voir l'annexe 2 «Formulaire commenté de recensement des risques»).

[15] Des informations complémentaires sur le rapport figurent aux ch. 3.1 et 4.

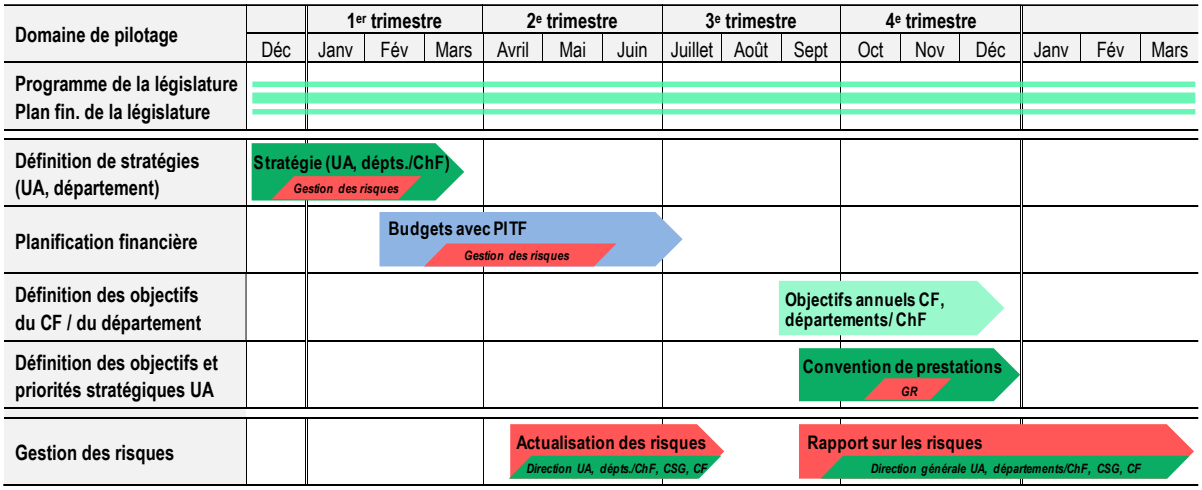


Illustration 2: Intégration fonctionnelle de la gestion des risques en tant que processus de conduite

Deux approches principales permettent donc d'intégrer la gestion des risques en tant qu'instrument de conduite. La première consiste à prendre en compte la gestion des risques ponctuellement dans le cadre des processus de préparation de la planification et de la stratégie gérés par la direction. La deuxième prévoit que la gestion des risques forme à la fois le contexte et le principe directeur du rapport sur les risques et de l'actualisation des risques. Dans les deux cas, la direction des UA, des départements / de la ChF et, en fin de compte, le Conseil fédéral sont toujours responsables des risques dans leur domaine[16].

2.3.2 Intégration verticale: perméabilité entre les échelons hiérarchiques

La direction doit s'assurer que les informations pourront circuler librement entre les différents échelons hiérarchiques – de la conduite stratégique à la gestion opérationnelle jusqu'aux différents processus: les mandats doivent être transmis depuis le haut vers l'échelon hiérarchique auquel ils doivent être mis en œuvre. À l'inverse, les cadres doivent pouvoir être informés, depuis le bas, sur la mise en œuvre de leurs mandats.

Cette exigence s'applique aussi à la gestion des risques de la Confédération, qui accompagne les processus de conduite à tous les échelons (illustration 3): alors que les directives applicables à l'ensemble de l'administration – c'est-à-dire la politique, la méthodologie et l'organisation en matière de gestion des risques – sont édictées par le Conseil fédéral et suivent un parcours descendant, leur mise en œuvre – identification, évaluation et maîtrise des risques – adopte un parcours ascendant, ce qui implique une application systématique des normes communes en ce qui concerne les méthodes et les instruments. C'est la seule manière de comparer les risques des différentes UA et de les classer et les transmettre selon leur priorité dans la pyramide de conduite[17].

La combinaison de l'approche descendante et de l'approche ascendante n'est pas seulement utilisée à l'échelon de l'administration fédérale dans son ensemble, mais aussi par les différentes UA, à leur propre échelon. Ainsi, le processus de gestion des risques (identification, analyse, évaluation, maîtrise, voir le ch. 3) va d'abord de bas en haut. Grâce à l'expertise et à l'expérience pratique de l'échelon de base, on s'assure que les risques importants sont reconnus. La direction est quant à elle chargée d'évaluer ces risques et de les classer selon leur niveau de priorité en suivant l'approche descendante. Elle limite ainsi son portefeuille à un nombre raisonnable de risques. Elle doit également examiner périodiquement les champs de risques et l'exposition aux risques de ses UA en partant d'une vision globale (voir le ch. 2.3.1). Le même principe est suivi au niveau du département.

[16] Voir le ch. 5, al. 4, let. a et al. 5, let. a, des directives du CF sur la politique de gestion des risques

[17] Voir le ch. 4.4 sur la sélection des risques dans la gestion des risques de la Confédération

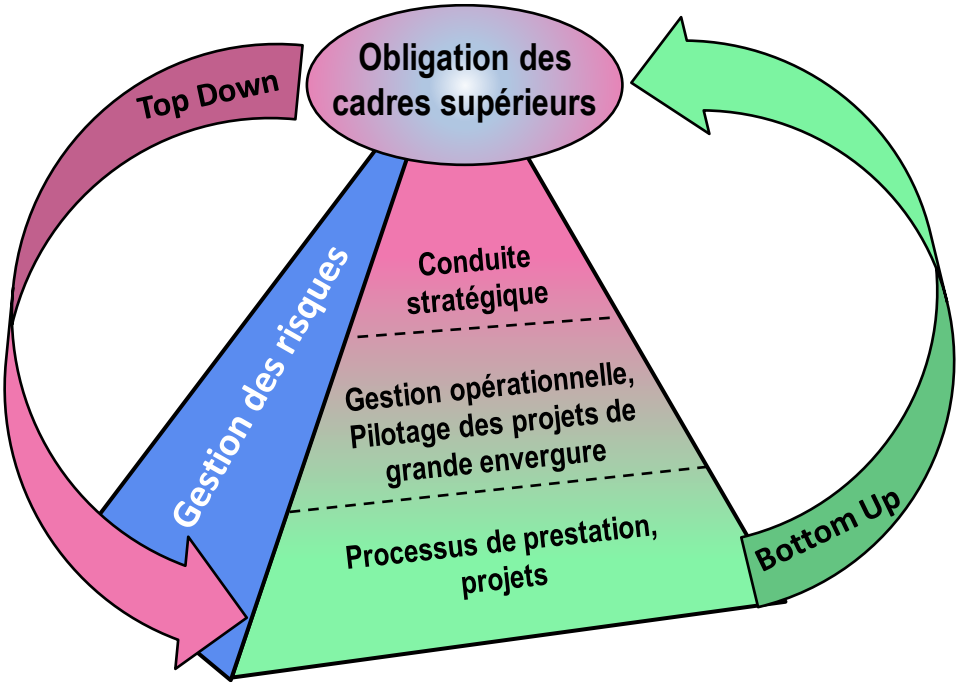


Illustration 3: Intégration verticale des différents échelons hiérarchiques dans la gestion des risques

2.3.3 Intégration horizontale: mise en réseau avec d'autres domaines d'aide à la conduite

À part la gestion des risques, la direction d'une UA assume d'autres tâches liées à la conduite, dont la BCM, le SCI ou la gestion de la sécurité informatique. En fonction de leur mission principale, certaines UA assurent en outre une gestion de la qualité, de la conformité ou de la sécurité au travail. En tant que fonctions d'état-major, ces *domaines* doivent soutenir la direction tout en allégeant sa charge.

Des liens parfois étroits unissent la gestion des risques et ces domaines d'état-major. Une bonne mise en réseau contribue à trouver les synergies et évite que chacun ne se limite à son propre domaine (travail en silo). Ainsi, les connaissances de domaines voisins peuvent fournir des renseignements essentiels sur des risques latents. La gestion des risques peut quant à elle révéler d'éventuelles lacunes dans les processus des domaines voisins et montrer quelles mesures peuvent être prises pour réduire les risques. Les liens entre la gestion des risques et les autres domaines ont pour but de permettre une utilisation réciproque des spécificités des uns et des autres, afin d'augmenter l'efficacité globale de l'aide à la conduite. Les échanges entre la gestion des risques et les autres domaines d'état-major porteront notamment sur les questions suivantes:

- **SCI:** les processus SCI ont-ils été mis en place de manière pertinente et systématique ou des lacunes subsistent-elles? Y a-t-il des indices concernant des déficiences systémiques qui pourraient entraîner des risques accrus pour l'UA ou le département? (voir le ch. 6.1)
- **BCM:** les processus indispensables au bon fonctionnement des opérations ont-ils été identifiés et actualisés lorsque cela était nécessaire? Les mesures prévues sont-elles suffisantes pour la réduction visée des risques et sont-elles efficaces en cas de survenance du risque ou, autrement dit, ont-elles fait l'objet de tests pertinents? (voir les ch. 6.2 et 6.3)
- **Informatique:** les risques liés aux projets sont-ils systématiquement analysés et gérés? Le contrôle de gestion informatique a-t-il trouvé des risques liés à des projets qui pourraient s'accentuer en cas de changements dans leur contexte? L'analyse en matière de sûreté de l'information et de protection des données (SIPD) a-t-elle révélé d'importantes failles de sécurité? (voir le ch. 6.8)

- **Analyse de la situation et du contexte:** y a-t-il des signaux annonçant des changements à moyen terme au niveau politique, social ou économique ou de grandes évolutions qui pourraient engendrer de nouveaux risques ou accentuer les risques existants? (voir le ch. 6.4)

Un échange régulier d'informations assure l'intégration horizontale de la gestion des risques et des autres processus d'aide à la conduite et permet d'améliorer la vue d'ensemble de l'exposition aux risques des UA.

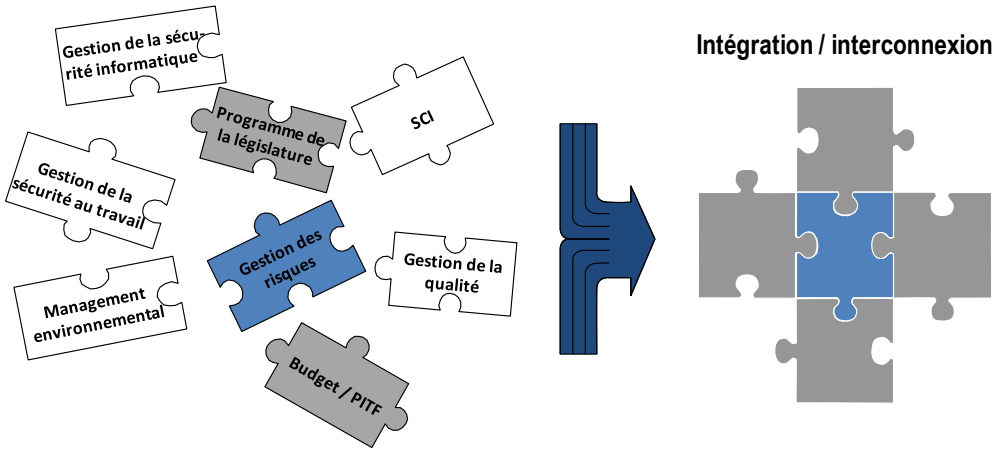


Illustration 4: Mise en réseau des domaines d'aide à la conduite au sein de l'administration fédérale

Définition des conditions-cadres: gestion intégrée des risques
Une gestion intégrée des risques est étroitement liée aux processus de conduite et à leurs domaines d'état-major à tous les échelons.

Recommandation de l'AFF:

- L'échange entre la direction et la gestion des risques a lieu, d'une part, dans le cadre des processus de planification, de stratégie et de définition des objectifs et, d'autre part, dans le cadre du rapport sur les risques et de l'actualisation des risques. En outre, la direction doit examiner au moins une fois par législature l'exposition aux risques et la qualité de la gestion des risques à moyen terme en partant d'une vision globale (intégration fonctionnelle).
- La gestion des risques doit pouvoir être exploitée à tous les échelons hiérarchiques et sans rupture entre l'un et l'autre. Elle suit donc à la fois une approche descendante et une approche ascendante, au moyen de normes appliquées dans l'ensemble de l'administration fédérale concernant les méthodes et les instruments (intégration verticale).
- La gestion des risques est liée aux autres domaines d'aide à la conduite et permet ainsi de trouver les synergies. Un échange structuré avec les domaines SCI, BCM, contrôle de gestion informatique et sécurité informatique a lieu au moins une fois par année. En fonction des tâches et des fonctions d'une UA, un échange est également nécessaire avec d'autres domaines d'état-major (intégration horizontale).

3 Processus de gestion des risques

La consolidation des risques au niveau des départements / de la ChF et du Conseil fédéral implique que les évaluations des différents risques soient comparables. L'identification, l'analyse et l'évaluation, l'appréciation, la maîtrise et la surveillance des risques doivent donc suivre des règles homogènes, qui sont prédéfinies de manière contraignante dans les directives de l'AFF sur la gestion des risques de la Confédération. Une application informatique commune (R2C_GRC) est utilisée pour la gestion des risques et le rapport sur les risques[18]. Mise à disposition et administrée par l'AFF, elle soutient la mise en œuvre uniforme du processus de gestion des risques dans l'administration fédérale et permet de remettre des rapports au Conseil fédéral et aux départements / à la ChF.

L'exécution des tâches liées au processus de gestion des risques (voir l'ill. 4) au sein de l'administration fédérale est exposée dans le présent chiffre et dans les suivants.

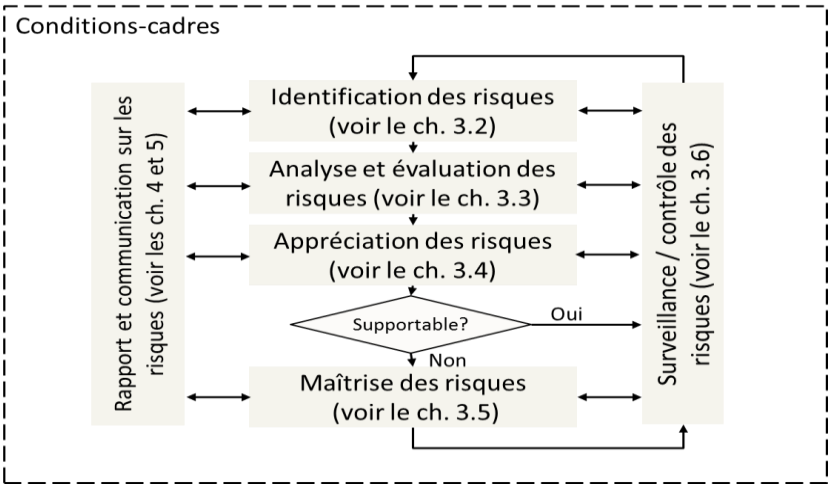


Illustration 5: Processus de gestion des risques selon les normes en vigueur

3.1 Procédures et flux d'information au sein de l'administration fédérale

Le graphique suivant présente brièvement les procédures:

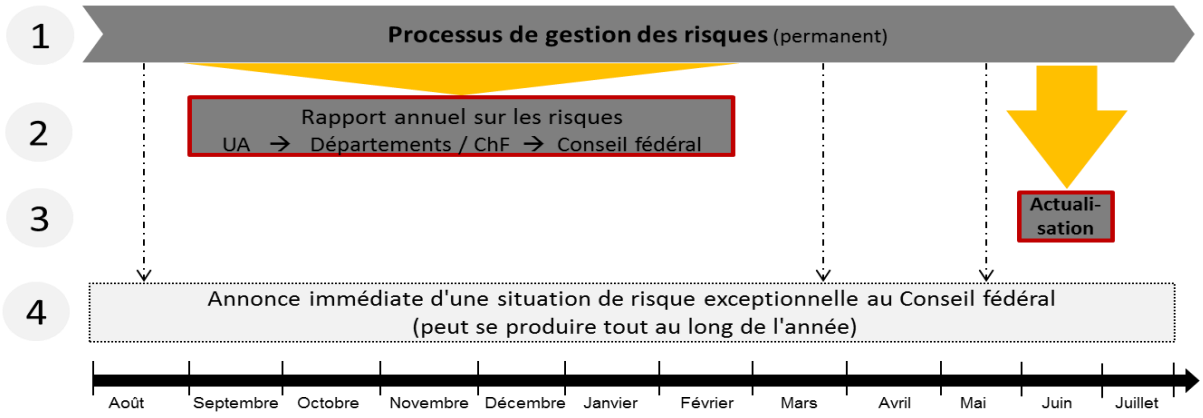


Illustration 6: Procédures de gestion des risques de la Confédération

[18] Ch. 3, al. 1, des directives du CF sur la politique de gestion des risques

Les collaborateurs et les cadres surveillent en permanence la situation de la Confédération en matière de risques (1). En plus du rapport annuel sur les risques au niveau de la Confédération (2), les principaux risques de cette dernière font l'objet d'une actualisation (3). Le Conseil fédéral est informé sans délai de toute situation de risque exceptionnelle (4)[19].

3.1.1 Rapport annuel sur les risques

L'administration fédérale établit une fois par an un rapport *détaillé* sur les risques (voir l'ill. 5). Il incombe aux responsables de la gestion des risques des départements et des UA de définir précisément les procédures internes et le calendrier pour leur UO. Le service de coordination de l'AFF n'indique que la date de remise obligatoire des rapports des départements.

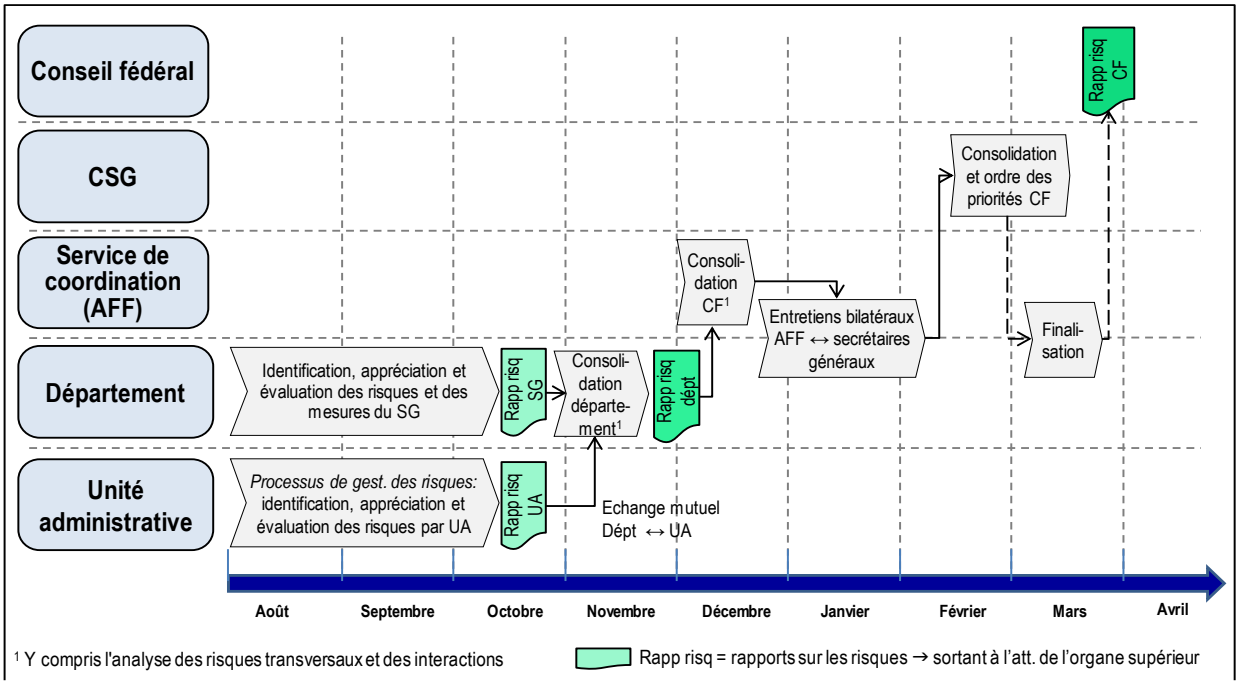


Illustration 7: Procédure pour le rapport annuel sur les risques de l'administration fédérale

Ce rapport à l'attention du Conseil fédéral est examiné par un groupe de travail des Commissions de gestion (CdG) lors d'une séance au mois d'avril.

3.1.2 Actualisation des risques

En outre, une actualisation des risques a lieu au mois de juin afin de dynamiser et de renforcer la gestion des risques de la Confédération. Il s'agit d'un processus descendant (*top-down*), qui se concentre sur les principaux risques de cette dernière. Les risques suivants sont vérifiés et mis à jour:

- risques du Conseil fédéral;
- risques transversaux de la Confédération et risques initiaux au niveau des départements et de la ChF (y c. d'éventuels nouveaux risques initiaux);
- nouveaux risques présentant un potentiel de crise et nouveaux risques initiaux.

L'actualisation des risques est annoncée au service de coordination en exportant le rapport détaillé ou le rapport succinct depuis R2C_GRC. Le Secrétaire général appose sa signature numérique sur la page de titre du rapport à titre de confirmation. Les résultats de l'actualisation des risques sont transmis au Conseil fédéral par l'intermédiaire d'une note d'information ou d'une proposition. L'actualisation des risques est également remise au groupe de travail «Gestion des risques de la Confédération» des deux CdG.

[19] c.f. ch. 5, al. 4, des directives du CF sur la politique de gestion des risques; le service de coordination de l'AFF est informé en parallèle.

3.1.3 Flux d'information concernant la gestion des risques de la Confédération

L'illustration suivante présente brièvement les principaux flux d'information concernant la gestion des risques, jusqu'au niveau des UA.

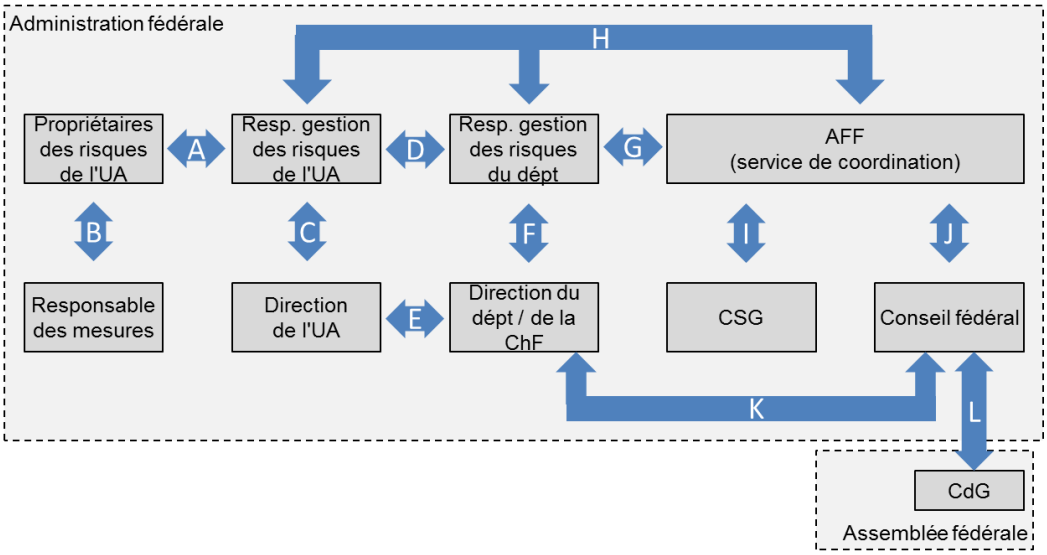


Illustration 8: Flux d'information

Les différentes relations en matière d'information sont décrites ci-après:

A Lors du processus annuel de gestion des risques, le responsable de la gestion des risques de l'UA collabore avec les différents propriétaires des risques de l'UA pour identifier, analyser, évaluer et maîtriser les nouveaux risques ainsi que pour mettre à jour ceux qui avaient déjà été identifiés.

B Le propriétaire du risque[20] charge le responsable des mesures d'appliquer ces dernières et surveille leur mise en œuvre. Le responsable des mesures l'informe régulièrement de l'avancement de la mise en œuvre ainsi que des éventuels problèmes ou retards.

C Le responsable de la gestion des risques de l'UA prépare un projet de rapport sur les risques à l'intention de la direction de l'UA. Celle-ci analyse et complète les risques et statue sur la mise en œuvre de mesures dans son domaine de compétences.

D Échanges réguliers. Le responsable de la gestion des risques du département définit le calendrier et la méthodologie. Les responsables de la gestion des risques des UA lui transmettent des informations sur les risques de leur UA.

E Informations et discussion sur les principaux risques des UA qui sont déclarés au département. Examen et décision sur les mesures du département concernant les risques.

F Le responsable de la gestion des risques du département consolide les risques de toutes les UA et prépare un projet de rapport sur les risques à l'intention de la direction du département / de la ChF. Celle-ci analyse et complète les risques et approuve le rapport du département à l'attention du Conseil fédéral, qui est remis par l'intermédiaire du service de coordination de l'AFF.

G Échanges d'expériences réguliers. Le service de coordination de l'AFF définit le calendrier et la méthodologie. Les responsables de la gestion des risques des départements lui transmettent des informations sur les principaux risques de leur département / de la ChF.

[20] La direction de l'UA ou du département / de la ChF peut également être le propriétaire du risque.

H Formation technique des responsables de la gestion des risques des départements et des UA ainsi que formation et soutien pour l'utilisation de R2C_GRC (Risk to Chance Gouvernance, gestion des risques et conformité), l'application commune sur les risques.

I Le service de coordination de l'AFF remet à la Conférence des secrétaires généraux (CSG) un projet de rapport sur les risques à l'intention du Conseil fédéral. La CSG consolide les risques des départements et de la ChF et les classe par ordre de priorité; elle analyse les interactions et approuve le rapport sur les risques à l'attention du Conseil fédéral.

J Le service de coordination de l'AFF finalise le rapport sur les risques et le soumet au Conseil fédéral par l'intermédiaire du DFF.

K Informations du Conseil fédéral à la direction du département / de la ChF à l'issue de ses séances; le cas échéant, mandat pour la mise en œuvre de mesures en matière de risques au niveau du Conseil fédéral.

L Examen annuel du rapport du Conseil fédéral sur les risques par un comité des CdG.

Définition des conditions-cadres
Prescriptions de l'AFF :

- Dans le cadre du processus de gestion des risques, les procédures et les délais des UA doivent être coordonnés avec le processus parent du département et de la Confédération.
- Un rapport sur les risques est établi au moins une fois par an dans l'administration fédérale, au niveau du Conseil fédéral, des départements / de la ChF et des UA.
- En outre, les risques du Conseil fédéral et ceux qui pourraient déclencher une crise sont mis à jour.
- Le Conseil fédéral est informé sans délai de toute situation de risque exceptionnelle.

3.2 Identification

Le processus de gestion des risques au sens strict commence par l'identification des risques. Il s'agit d'identifier le plus précisément possible les risques importants d'une UO, de les délimiter judicieusement et d'en faire une description claire. Cette étape requiert beaucoup de soin: elle permet de déterminer ce qui relève des responsables hiérarchiques; elle garantit également la qualité et la pertinence des phases suivantes du processus de gestion des risques, notamment celles de l'analyse et de l'évaluation des risques ainsi que celles du développement de mesures. L'identification des risques requiert donc non seulement une bonne connaissance des tâches, objectifs, processus et projets de l'UO, mais aussi un bon équilibre entre rigueur méthodique et pragmatisme. Les points traités dans les paragraphes suivants ne doivent pas être considérés comme une liste de contrôle à traiter mécaniquement, mais comme un guide permettant de mieux comprendre quels sont les éléments constitutifs de l'identification des risques.

3.2.1 Point de départ et limite

Objet

L'identification des risques consiste à déterminer précocement les événements et les évolutions susceptibles d'affecter les tâches et l'atteinte des objectifs de la Confédération. Elle doit non seulement prendre en considération les événements pouvant se produire à court terme, mais aussi les évolutions à long terme. Un processus *systématique* et régulier est indispensable pour garantir une identification des risques fiable et non aléatoire. Il complète l'attention constante que portent les collaborateurs de la Confédération aux nouveaux développements qui peuvent avoir des effets négatifs sur l'administration fédérale.

L'identification systématique des risques s'appuie sur les éléments suivants:

- les objectifs et les tâches découlant des lois et de leurs dispositions d'exécution (ordonnances);
- les objectifs et les fonctions répertoriés dans les ordonnances sur l'organisation des départements et de la ChF, et
- les objectifs annuels du Conseil fédéral, des départements / de la ChF et des UA.

En plus des tâches et des objectifs de la Confédération, il est possible d'utiliser une *schématisation des processus* si une UA souhaite déterminer les points faibles d'un processus donné et les points d'impact des risques correspondants. Les projets en cours sont également soumis au processus de gestion des risques.

Cadre de référence: risques pour la Confédération

Lors de la recherche et de l'identification des risques pouvant menacer ou affecter négativement l'exécution des tâches ou l'atteinte des objectifs de la Confédération, il faut chaque fois analyser en détail dans quelle mesure la *Confédération* est exposée à un risque. Les deux exemples suivants illustrent la difficulté de définir les limites d'un risque:

Pandémie

- La Confédération n'est en principe pas responsable des dommages économiques découlant d'une pandémie (pertes de productivité, frais médicaux supplémentaires).
- L'Office fédéral de la santé publique (OFSP) doit assumer toute une série de tâches en relation avec la détection précoce de nouvelles menaces pour la santé[21]. Par exemple, le fait que l'OFSP ne parvienne pas à identifier à temps une pandémie et à fournir les informations nécessaires à la population constitue un risque pour l'OFSP (et donc pour la Confédération).
- Les collaborateurs de l'administration fédérale peuvent être touchés par une pandémie. Si un nombre important d'entre eux est absent pour cause de maladie, l'exécution des tâches de plusieurs UA pourrait être remise en question, ce qui constitue un risque supplémentaire pour la Confédération.

Faillite d'une grande banque

- La faillite d'une grande banque en Suisse et ses conséquences directes (par ex. pertes des créanciers et des investisseurs) ne constituent pas en soi un risque de la Confédération.
- Veiller à la stabilité du secteur financier suisse est l'une des tâches du Secrétariat d'État aux questions financières internationales. Si un établissement est systémique (too big to fail), de sorte que sa défaillance pourrait menacer ou paralyser le système financier suisse, le risque concerne alors également la Confédération, qui serait contrainte, le cas échéant, de prendre des mesures de sauvetage.

La restriction des ressources ne constitue (presque) jamais un risque

Les ressources financières et humaines dont une UA dispose pour accomplir ses tâches et atteindre ses objectifs sont calculées très exactement et doivent être utilisées de manière économe et efficace[22]. Elles sont déterminées par les organes supérieurs (direction de l'UA, du département ou de la ChF, Conseil fédéral) dans le cadre des processus d'établissement du budget et du plan financier; le Parlement dispose de la souveraineté budgétaire[23]. Dans ce contexte, les compétences et les processus décisionnels sont réglés dans le détail sur la base des lois fédérales pertinentes. Techniquement parlant, la répartition des ressources est donc

[21] Art. 9 de l'ordonnance sur l'organisation du DFI (RS **172.212.1**)

[22] Art. 12, al. 4 et 57, al. 1, LFC (RS **611.0**)

[23] Art. 167 de la Constitution (RS **101**), art. 25 de la loi sur le Parlement (RS **171.10**)

endogène[24]: elle résulte de décisions liées à la politique et à la gestion, qui sont prises par les organes compétents de la Confédération dans le cadre du pilotage des tâches et du budget. Les décisions concernant les ressources prises par l'Assemblée fédérale, le Conseil fédéral ou la direction du département *ne sont donc en principe jamais à l'origine d'un risque*[25]. C'est également le cas lorsque les tâches ne peuvent être accomplies et les objectifs atteints qu'au prix de grands efforts en raison de règles budgétaires strictes (par ex. réformes structurelles) ou lorsque les tâches ou les objectifs doivent être redéfinis (révision de loi), ce qui est souvent le cas dans le cadre des programmes d'économie.

La décision budgétaire influence tant la compréhension des tâches ou des objectifs que l'exécution des premières ou l'atteinte des seconds. Plus il y a de ressources pour une tâche, plus son accomplissement doit être complet. Au contraire, lorsqu'il y a moins de ressources à disposition, il faut éventuellement réduire la prestation ou supprimer des tâches. La gestion des risques ne doit pas être utilisée (1) comme instrument pour obtenir des ressources supplémentaires, ou (2) comme échappatoire, au cas où l'UA estime que la qualité et la quantité requises pour les tâches ou les objectifs ne peuvent être atteintes avec les ressources à disposition. Une telle utilisation ne serait pas conforme aux buts de la gestion des risques et cette dernière s'en trouverait affaiblie. L'examen des décisions budgétaires s'appuie sur des instruments et des processus qui lui sont propres.

Il peut cependant arriver que des ressources financières ou humaines insuffisantes représentent un risque lorsque des événements ou des développements externes viennent déséquilibrer les ressources disponibles et les tâches légales, remettant en question l'accomplissement de ces dernières:

- **Exemple 1 (migration):** le nombre attendu de demandes d'asile constitue un paramètre important pour la fixation du budget concernant le domaine de l'asile. L'arrivée imprévue d'un nombre fortement accru de réfugiés est source de défis logistiques, qui ne peuvent plus être affrontés avec les ressources à disposition. Il incombe à la Confédération de prendre toutes les mesures nécessaires en collaboration avec les autres acteurs du domaine afin que tous les réfugiés soient enregistrés, soumis aux contrôles de sécurité et aux mesures sanitaires à la frontière, hébergés et encadrés.
- **Exemple 2 (prévoyance vieillesse):** des changements structurels concernant les prestations (augmentation de l'espérance de vie, évolution démographique) ou les finances (faiblesse persistante des taux d'intérêts) peuvent conduire à un appauvrissement des assurances sociales et mettre en péril le respect des engagements légaux, voire entamer la confiance dans le système de prévoyance en général.
- **Exemple 3 (recrutement de spécialistes):** le budget d'une UA prévoit suffisamment de ressources et de postes pour répondre aux besoins en matière de personnel. Il peut toutefois arriver que les spécialistes recherchés ne puissent pas être trouvés pour repourvoir certaines fonctions clés, car le marché du travail est asséché dans le secteur concerné. Les postes restent vacants plus longtemps, risquant de compromettre un accomplissement des tâches conforme à la loi.

L'identification d'un risque s'avère judicieuse lorsqu'il est possible d'envisager des mesures appropriées. La mise en place de systèmes d'alerte (précédant une aggravation de la situation) ou la planification d'un dispositif de crise permettant de maîtriser plus rapidement la situation (en cas d'apparition d'un risque), par exemple, apportent une amélioration dans le pilotage des tâches.

[24] C'est-à-dire décidée par des organes de la Confédération; contraire: exogène = qui provient de l'extérieur.

[25] Voir les directives de l'AFF sur la gestion des risques de la Confédération, état au 31 mars 2016, chiffre 2.2.1, p. 4. La Conférence des secrétaires généraux s'est également prononcée en ce sens lors de sa séance du 24 février 2017.

3.2.2 Procédure et structure

Recensement des risques

Diverses méthodes existent pour identifier les risques. Elles vont de la recherche d'idées spontanées (insuffisante) aux analyses des systèmes et processus (coûteuses), en passant par les enquêtes auprès d'experts et de collaborateurs. Au sein de la Confédération, une *réflexion structurée (brainstorming)* basée sur les objectifs, les tâches et les processus pour rechercher les risques concrets de l'UO examinée a fait ses preuves dans la pratique[26]. Elle peut être réalisée à l'aide d'entretiens individuels ou d'entretiens de groupe.

Choix du cadrage approprié: situer et délimiter les risques avec justesse

Une fois que les champs de risques ou les risques individuels ont été identifiés (par ex. par un brainstorming), il s'agit de les délimiter judicieusement, c'est-à-dire de les rendre «tangibles» (on parle d'objectiver les risques). Une délimitation judicieuse apporte notamment les précisions suivantes concernant le risque considéré:

- sa portée (sans se perdre dans les généralités);
- sa spécificité (sans entrer trop dans le détail);
- sa cohérence (sans cacher des conditions ou des aspects importants).

Une objectivation judicieuse des risques est indispensable pour la qualité des étapes suivantes du processus de gestion des risques (voir les ch. 3.3 à 3.6). Elle constitue la base pour une description pertinente (scénario) et une évaluation plausible des risques ainsi que pour le développement de mesures cohérentes visant à maîtriser les risques. Ces trois éléments sont étroitement liés; ils doivent être coordonnés entre eux pour pouvoir être effectués même par des personnes qui ne sont pas spécialisées dans ce domaine (direction des départements, Conseil fédéral, organes de surveillance parlementaires).

Le **choix du cadrage approprié** est déterminant, c'est-à-dire le cadre ou le degré d'abstraction du risque identifié. Si le **cadre** est **trop large,** le risque devient trop général. Les informations le concernant s'apparentent à des lieux communs, car elles portent sur un trop grand nombre d'événements ou de développements. Par conséquent, une telle approche entraîne souvent les problèmes suivants:

1. La description du risque est trop générale ou elle présente une liste d'événements ou de développements indépendants les uns des autres. Un seul événement est choisi arbitrairement pour le pire cas crédible (*credible worst case*). Le risque manque alors de cohésion, et s'apparente parfois à un amas de risques.
2. L'évaluation du risque (probabilité, conséquences) est empreinte de subjectivité et manque de justifications objectives, car ses références sont trop hétérogènes. Le risque étant très global, il est généralement surestimé, ce qui fausse la comparaison avec d'autres risques de la Confédération.
3. Les mesures sont souvent définies de manière floue, elles sont souvent trop nombreuses et donc confuses. On ne peut guère comprendre si les mesures choisies sont appropriées et si l'ordre des priorités est adéquat. Elles sont pratiquement inutiles pour le pilotage des tâches.

Dans la Constitution, dans l'article énonçant le but d'une loi et dans les ordonnances sur l'organisation des départements et de la ChF, les tâches et les buts de la Confédération sont très généraux. Ils sont précisés ailleurs. Dès lors, ces dispositions ne sont pas très utiles pour l'identification des risques. Il est recommandé de subdiviser les thèmes en composantes connexes, et d'en tirer deux ou plusieurs risques individuels.

[26] Des listes de dangers comprenant des observations, des remarques ou des prévisions et provenant du système de gestion de la qualité, de la sécurité au travail, de la gestion de la sécurité informatique, etc. devraient être utilisées dans la mesure du possible.

Exemple: selon l'art. 1 de l'ordonnance sur son organisation[27], le DFAE «défend les intérêts de politique extérieure de la Suisse dans le cadre du mandat constitutionnel.» Si l'identification des risques se fondait uniquement sur cette disposition, elle comprendrait un programme entier de législature, y compris les défis et les incertitudes que ce dernier implique. Il en résulterait une structure des risques incluant de tout et vide de sens: les responsables hiérarchiques verraient le nombre de buts et de mesures redoubler, sans aucune valeur ajoutée.

Il faut également éviter d'opter pour un **cadre trop serré**, c'est-à-dire de descendre dans le détail, et de se concentrer sur un contexte trop restreint. Dans ce cas, c'est le trop grand nombre de petits risques figurant dans la matrice des risques qui pose problème. Le portefeuille des risques manque alors de clarté, il comporte trop de détails et ne peut plus être géré efficacement. L'erreur provient généralement du fait que seuls des processus partiels ou des phases d'un projet découlant d'une approche ascendante (*bottom-up*) sont pris en compte[28]. Si de tels risques peuvent être traités sous un seul thème commun, ils doivent être réunis dans un scénario *credible worst case* selon une perspective descendante (voir les ch. 3.3.2 ss).

Il n'est pas facile de choisir le cadrage adéquat. Il faut faire preuve de discernement. Il arrive parfois qu'on découvre au cours de l'analyse des risques qu'un risque a été mal délimité. Dans ce cas, une démarche itérative entre les différentes phases du processus de gestion des risques contribue à une meilleure compréhension et finalement à une représentation plus judicieuse du risque.

Notamment au sein de grandes organisations telles que l'administration fédérale, il convient de tenir compte des *interactions* possibles entre les risques (voir le ch. 4.5). Des risques peuvent être liés entre eux et se renforcer mutuellement, ou alors un risque identifié peut avoir des effets simultanés dans plusieurs UO. Toutes ces interactions doivent être évaluées ensemble afin d'en garantir une gestion optimale. Dans certaines conditions, il peut être judicieux de les *agréger à un risque transversal* (voir le ch. 4.3). L'agrégation implique que les risques aient été cadrés adéquatement.

Classification des risques (catégories de risques)

Les risques sont très variés dans l'administration fédérale. Pour permettre leur classement et leur identification systématique, ils sont répartis dans les six catégories suivantes *en fonction de leur cause*[29]:

- ***risques économiques et financiers:*** risques concernant la gestion financière, la dépendance (économique) de la Confédération vis-à-vis de tiers ou ses prestations subsidiaires (prêts, cautionnements, garanties, etc.);
- ***risques juridiques / compliance:*** risques concernant les dommages liés à l'exécution de tâches fédérales, le respect de dispositions juridiques ou contractuelles, la violation des obligations de surveillance, la responsabilité subsidiaire de la Confédération en vertu de l'art. 19 de la loi sur la responsabilité (LRCF)[30];
- ***risques matériels, techniques et risques liés aux éléments naturels:*** risque de destruction ou d'endommagement (y c. interruption de l'exploitation) de bâtiments, d'équipements, d'installations techniques, de données ou de biens culturels appartenant à la Confédération;
- ***risques liés aux personnes et à l'organisation:*** risques liés à l'organisation, à la conduite, aux collaborateurs, à la protection des personnes, au recrutement de spécialistes, à la défaillance de personnes-clés, à l'abus de confiance;

[27] Ordonnance sur l'organisation du Département fédéral des affaires étrangères (RS **172.211.1**)

[28] Par exemple dans le cadre d'analyses fonctionnelles comme les AMDEC (ch. 3.3.2)

[29] L'annexe 3 présente d'autres manières de structurer ou de regrouper plusieurs risques.

[30] L'annexe 7 expose plus précisément et d'un point de vue juridique certains risques de la Confédération qui sont liés aux organisations extérieures à l'administration fédérale.

- ***risques technologiques et biologiques:*** risques découlant de la recherche et du développement de nouvelles applications technologiques ou scientifiques (y c. leurs effets ultérieurs), telles que les nanotechnologies ou la génétique;
- ***risques sociaux et politiques:*** changements de la société (par ex. démographie), conflits d'intérêts avec l'étranger, etc. Cette catégorie comprend des risques complexes, tels que la sortie du nucléaire, les nanotechnologies ou les accords bilatéraux avec l'UE.

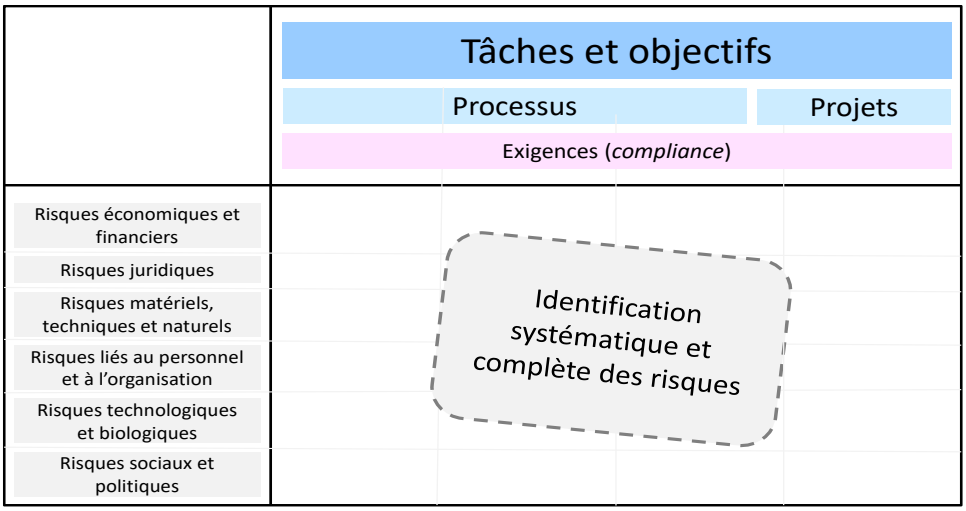


Illustration 9: Identification des risques

Aussi sérieuse que soit l'identification des risques, des *risques résiduels* non identifiables et non gérables demeureront toujours[31].

Étape du processus: identification des risques
Prescriptions de l'AFF:

- L'identification des risques doit être effectuée *sur la base des objectifs et des tâches de l'UO* (voir les lois, les ordonnances, l'ordonnance sur l'organisation du département / de la ChF, les objectifs annuels, le règlement de l'UA).
- Un manque de ressources financières ou humaines ne constitue généralement pas un risque, car il dépend de décisions du Conseil fédéral et du Parlement et est donc d'ordre systémique.
- Les risques doivent être délimités et formulés de manière pertinente (portée, spécificité et cohérence; choix du cadrage approprié).
- Les risques sont répartis dans les six catégories susmentionnées. L'affectation à une catégorie dépend de la cause du risque.

Recommandation de l'AFF:

- Réalisation d'ateliers ou d'entretiens avec les membres de la direction et les collaborateurs chargés de domaines spécifiques (détenteurs du savoir).

Retombées de l'identification: liste aussi exhaustive que possible des risques pouvant influer négativement sur l'exécution des tâches et la réalisation des objectifs de la Confédération.

Moyens auxiliaires: modèle d'identification des risques (voir l'annexe 2), descriptions des processus.

[31] La non-identification de risques peut en particulier résulter d'un manque de clairvoyance de l'entreprise, d'une surestimation des capacités d'une organisation ou de ses cadres dirigeants (hybris), de la sous-estimation d'une évolution ou d'un événement, ou encore de l'apparition de phénomènes entièrement nouveaux et inattendus («cygnes noirs»).

3.3 Analyse et évaluation des risques

3.3.1 Généralités sur le recensement des risques

Les risques de la Confédération sont recensés et documentés par voie électronique à l'aide de l'application informatique Risk to Chance (R2C_GRC). Sur cette base les rapports sur les risques avec ses deux formats standard – rapport détaillé et rapport succinct – sont établis [cf. ch. 4.1 et annexe 2]. Les risques actualisés sont consignés dans un historique après chaque arrêté du Conseil fédéral concernant les rapports sur les risques, en général à la mi-mars et à la mi-septembre.

Étape du processus: analyse et évaluation des risques
Prescriptions de l'AFF: Les informations suivantes doivent être recensées pour chaque risque:

- désignation claire du risque: brève et compréhensible par des tiers (voir le ch. 3.2);
- propriétaire du risque;
- unité administrative / département;
- tâche / objectifs concernés par le risque;
- catégorie du risque (voir le ch. 3.2);
- analyse qui expliquant le risque (voir le ch. 3.3.2);
- interactions éventuelles avec d'autres risques (voir les ch. 3.3.7 et 4.5);
- causes du risque;
- Pire cas credible (voir le ch. 3.3.2);
- évaluation du risque (conséquences et probabilité, voir le ch. 3.3.2 ss);
- explications et motifs de l'évaluation du risque;
- mesures nouvelles/planifiées pour réduire le risque y inclus appréciation et commentaire concernant la mise en œuvre et l'efficacité attendue/observée (voir le ch. 3.5);
- mesures existantes pour réduire le risque.

3.3.2 Méthodes d'analyse et d'évaluation des risques

L'analyse des risques vise principalement à décrire de manière compréhensible le risque identifié (y c. pour des personnes extérieures), à en déterminer les causes et les conséquences et à comprendre les interactions (y c. avec d'autres risques; voir les ch. 3.3.7 et 4.5). De plus, la probabilité et les conséquences du risque sont évaluées sur le plan qualitatif ou quantitatif. Cette analyse repose sur le meilleur savoir-faire disponible. Au besoin et si la charge est proportionnelle, on fait appel à des experts externes à l'administration fédérale.

Les risques pouvant être très différents, plusieurs méthodes ont été développées pour leur analyse et leur évaluation. Certaines sont présentées brièvement ci-après[32]:

- ***Analyses de scénarios:*** les analyses de scénarios permettent de déterminer les causes des risques identifiés ainsi que d'évaluer et de présenter les effets de plusieurs scénarios. Elles visent à comprendre le rapport de cause à effet avant et après l'apparition d'un risque. On recourt généralement au scénario du pire cas crédible (*credible worst case*) pour exposer le risque (voir le ch. 3.3.3). Le diagramme des causes et de leurs effets (utilisé pour analyser les dommages survenus) et l'analyse par arbre de panne et arbre d'événements (utilisée pour les systèmes techniques complexes) sont des formes spécifiques de l'analyse de scénarios.

[32] Voir à ce sujet, par ex., ÖNORM 4902-2

- ***Analyses d'indicateurs:*** comme son nom l'indique, cette analyse tente d'identifier des indicateurs ou des incidents qui auraient pu occasionner un dommage. Ceux-ci peuvent fournir des informations sur la survenance éventuelle du scénario le plus grave (*worst case*) en matière de risques. L'analyse de ces incidents ou indicateurs permet d'élaborer et de mettre en œuvre des mesures de réduction du risque. Le *change based risk management*, qui identifie et évalue systématiquement les *modifications* et analyse leur influence sur l'organisation est une forme spécifique de l'analyse d'indicateurs.
- ***Analyses fonctionnelles:*** l'analyse fonctionnelle consiste à diviser l'objet examiné (en général, un système technique ou un processus) en sous-systèmes ou sous-processus dont on détermine les fonctions et les tâches. On recherche ensuite les défaillances éventuelles (et leurs causes) qui pourraient affecter le bon fonctionnement des sous-systèmes et de l'ensemble du système. L'analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC; également appelée *failure mode and effects analysis*, FMEA) est souvent utilisée en la matière.
- ***Analyses statistiques:*** dans ce type d'analyses, le risque est considéré comme la valeur statistique de l'insécurité. Une base de données fiable et suffisamment volumineuse est nécessaire à ces analyses. L'écart type et la valeur de confiance (*value at risk*) sont des indicateurs de risque usuels. La simulation Monte-Carlo permet de reproduire des risques en utilisant un procédé aléatoire récurrent et de déterminer la répartition des dommages inhérents à un risque ou à un groupe agrégé de risques.

L'analyse de scénarios est une méthode universelle qui convient parfaitement à une approche descendante (*top-down*), alors que certaines des autres méthodes présentées ici ne s'appliquent qu'à des cas très spécifiques.

Étape du processus: analyse et évaluation des risques
Prescription de l'AFF:

- Dans l'administration fédérale, les risques sont présentés à l'aide d'une analyse de scénarios. Les autres méthodes d'analyse sont facultatives.

Recommandation de l'AFF:

- L'analyse des risques doit reposer sur le meilleur savoir-faire disponible. Au besoin et si la charge est proportionnelle, on fera appel à des experts externes à l'administration fédérale.

3.3.3 Répartition des dommages inhérents à un risque

La plupart des risques peuvent apparaître avec une ampleur différente. Ainsi, une inondation peut constituer un événement local fréquent qui occasionne des dommages modérés ou devenir la «crue du siècle», c'est-à-dire un événement très rare aux effets dévastateurs. En général, les manifestations d'un risque sont prises en compte de trois façons:

- ***Répartition des dommages:*** un risque peut être décrit à l'aide d'une répartition précise des dommages s'il est suffisamment compris ou si des données statistiques existent.
- ***Scénarios:*** ils constituent une bonne approche. On utilise souvent trois scénarios pour illustrer toute l'ampleur possible d'un risque.
- ***Pire cas crédible (credible worst case):*** le risque est présenté sous sa forme la plus grave, mais néanmoins réaliste. L'organisation rencontrerait alors des difficultés majeures.

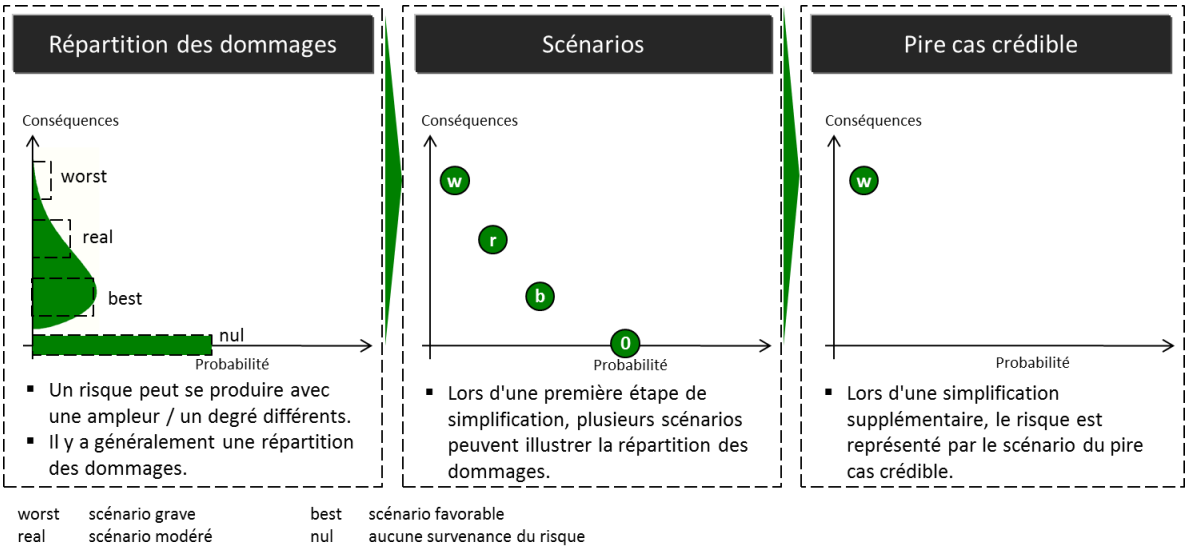


Illustration 10: Répartition des dommages inhérents à un risque

Étape du processus: analyse et évaluation des risques
Prescription de l'AFF:

- Dans l'administration fédérale, le risque est exposé en tant que *credible worst case* (pire cas crédible). Le cas échéant, plusieurs scénarios ou une répartition des dommages sont établis en vue d'une meilleure compréhension du risque.

3.3.4 Évaluation des conséquences

Un risque peut avoir des conséquences multiples. D'après la gestion des risques de la Confédération, différentes conséquences jouent souvent un rôle important en même temps. En accord avec les responsables de la gestion des risques des départements et de la ChF, il a été décidé de décrire les conséquences des risques à l'aide des cinq dimensions suivantes:

- **Conséquences financières**
- **Dommages corporels**
- **Atteinte à la réputation**
- **Entrave aux processus opérationnels**
- **Conséquences environnementales**

Lorsque l'une de ces cinq dimensions est pertinente pour un risque, les conséquences correspondantes doivent être évaluées sur une échelle de six niveaux (de «très faibles» à «très importantes»; voir la matrice d'évaluation de la gestion des risques de la Confédération). Chaque dimension a la même pondération et la même importance que les autres. Chaque risque doit être apprécié en fonction de chacune des cinq dimensions (conséquences) et **classé globalement**, selon la dimension la plus élevée mesurée. Si plusieurs dimensions sont pertinentes, le classement repose sur la conséquence la plus élevée. L'exemple ci-après (évaluation globale élevée) illustre ce principe:

Conséquences	Très faibles	Faibles	Modérées	Notables	Importantes	Très importantes
Conséquences financières				X		
Dommages corporels					X	
Atteinte à la réputation				X		
Entrave aux processus opérationnels			X			
Conséquences environnementales						

Illustration 11: Évaluation globale des conséquences

Les mesures de réduction du risque déjà appliquées sont prises en compte dans l'évaluation des conséquences (principe de l'***évaluation nette***).

La matrice définit uniquement l'échelle d'évaluation au niveau de la Confédération et des départements / de la ChF. Les UA peuvent utiliser des échelles d'évaluation mieux adaptées à leurs besoins (montant du budget, caractéristiques spécifiques des risques, etc.)[33]. L'AFF salue cette personnalisation de l'échelle d'évaluation qui renforce la gestion des risques en tant qu'instrument de conduite et de travail dans les UA.

Étape du processus: analyse et évaluation des risques
Prescriptions de l'AFF:

- Pour chaque risque, les cinq dimensions (conséquences) doivent être évaluées. Les évaluations doivent être documentées et brièvement commentées lorsque cela est nécessaire. Chaque risque est classé globalement, selon la dimension la plus élevée mesurée.
- Les mesures de réduction du risque déjà mise en œuvre sont prises en compte dans l'évaluation.

Recommandation de l'AFF:

- L'AFF recommande aux UA d'utiliser des échelles d'évaluation adaptées à leurs besoins pour classer les conséquences.

3.3.5 Évaluation qualitative ou quantitative

En principe, un risque peut être classé sommairement (sur le plan qualitatif) ou évalué quantitativement à l'aide de niveaux prédéfinis. En général, une évaluation quantitative est judicieuse uniquement si les données disponibles sont très bonnes (par ex. données statistiques sur les sinistres) et si l'on ne doit s'attendre qu'à des conséquences financières.

Étape du processus: analyse et évaluation des risques
Recommandation de l'AFF:

- L'AFF conseille d'effectuer une évaluation *qualitative* des risques en tenant compte des cinq dimensions des conséquences.

3.3.6 Évaluation de la probabilité

Par définition, un risque est un événement incertain dont la probabilité est comprise entre 0 % et 100 %. Ce pourcentage peut être interprété de deux façons:

[33] L'AFF s'occupe de la mise en œuvre technique dans R2C_GRC.

a. Une probabilité de 10 % peut signifier, par exemple, qu'un risque a 10 % de chance d'apparaître au cours d'une année ou qu'il se réalise en moyenne une fois tous les dix ans. On parle de probabilité périodique ou de *probabilité annuelle*. Dans cette interprétation, le risque peut apparaître plusieurs fois sur une période prolongée. C'est notamment le cas de la plupart des risques opérationnels, qui sont souvent déclenchés par des événements.

b. Une probabilité de 10 % peut également être interprétée comme une *probabilité ponctuelle*: un risque peut apparaître ou pas, mais il ne peut pas apparaître plusieurs fois. C'est, par exemple, le cas des risques politico-stratégiques, qui résultent d'une évolution négative. Compte tenu de l'environnement dynamique, ces risques présentent fréquemment un caractère unique. De plus, la probabilité qu'un projet spécifique échoue doit, elle aussi, être considérée comme ponctuelle.

Il faut tenir compte de ces interprétations différentes lorsque l'on compare des risques, par exemple en précisant dans la description si un risque peut apparaître plusieurs fois et, le cas échéant, sur quelle période. Pour garantir la pertinence de la matrice des risques en la matière, il convient de séparer strictement les risques présentant une probabilité périodique et ceux dont la probabilité est ponctuelle. On renoncera à cette distinction au niveau du Conseil fédéral pour des raisons pratiques: la probabilité sera considérée comme ponctuelle *et* annuelle et devra être interprétée différemment en fonction du risque.

Les conséquences financières des *événements connus pour se produire plusieurs fois par an* (dommages fréquents tels que ceux aux véhicules à moteur qui sont déclarés à une assurance) doivent être budgétées à l'aide d'une moyenne annuelle. Le risque prend la forme d'un dépassement éventuel de la valeur inscrite au budget pour l'année concernée. C'est un événement incertain qui affiche donc une probabilité inférieure à 100 %.

La matrice d'évaluation de la gestion des risques de la Confédération présente l'échelle de la probabilité qui est utilisée dans l'administration fédérale. On renonce aux échelles spécifiques aux UA pour garantir la vue d'ensemble et la comparabilité.

3.3.7 Interactions entre les risques

Il faut déterminer pour chaque risque si son apparition engendre d'autres conséquences sur d'autres risques, en plus de ses principaux effets. Ainsi, la concrétisation d'un risque peut accroître sensiblement la probabilité d'un autre risque (corrélation positive) ou, à l'inverse, la diminuer (corrélation négative). De manière générale, il convient d'examiner s'il existe un lien avec d'autres risques recensés, qui peuvent le cas échéant se situer dans une autre UA ou un autre département. Les interactions entre les risques doivent être identifiées, comprises de manière optimale et présentées dans la description des risques. L'analyse d'un risque individuel est l'occasion d'une première vérification des interactions. Étant donné que les départements / la ChF et le Conseil fédéral ont une meilleure vue d'ensemble de tous les risques identifiés, les responsables de la gestion des risques des départements, le service de coordination de l'AFF et la CSG procèdent à un autre examen détaillé des interactions entre les principaux risques de l'administration fédérale (voir le ch. 4.5).

Étape du processus: analyse et évaluation des risques
Prescription de l'AFF:

- Pour chaque risque, au niveau de l'UA, du département / de la ChF et du Conseil fédéral, on examinera les interactions éventuelles avec d'autres risques.

Retombées de l'analyse et de l'évaluation des risques: description compréhensible de chaque risque et évaluation de sa probabilité et de ses conséquences.

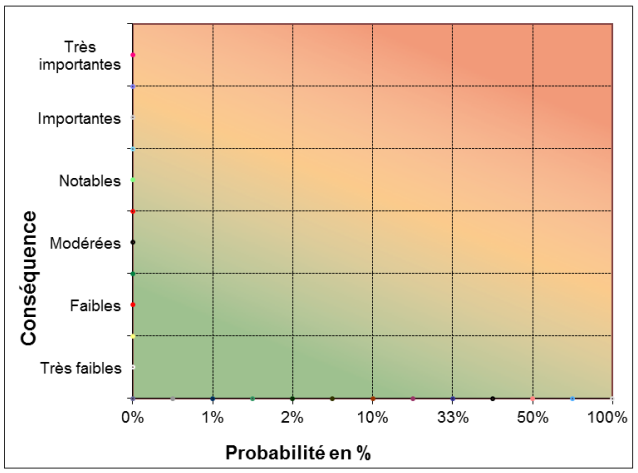
Moyens auxiliaires: matrice d'évaluation de la gestion des risques de la Confédération.

3.4 Appréciation des risques

Une fois les risques évalués, l'étape suivante du processus consiste à apprécier leur importance et leur portée. Il s'agit de déterminer, d'une part, à partir de quel échelon hiérarchique un risque sera géré et des mesures seront envisagées et, d'autre part, si les risques peuvent être maîtrisés avec les propres ressources de l'entreprise en cas d'apparition.

Tolérance au risque

Les six niveaux de conséquences (de «très faibles» à «très importantes») qui sont définis dans la matrice d'évaluation de la Confédération permettent de classer sommairement les risques en fonction de leur importance. Concrètement, cette dernière dépend du contexte dans lequel survient le risque et de la taille de l'UO examinée [34]; elle devrait être déterminée individuellement au niveau de l'UA. De plus, les directions des UA, des départements / de la ChF et le Conseil fédéral doivent fixer leur seuil de tolérance au risque en **respectant toutes les directives légales et réglementaires**. L'illustration suivante présente une répartition *possible* des risques en trois niveaux de tolérance:



	Appréciation
Risque important	Le risque constitue un danger considérable qui doit être géré par la direction. Celle-ci examine les mesures envisageables et décide de leur mise en œuvre. Le risque est surveillé régulièrement tant qu'il demeure à ce niveau.
Risque moyen	Le risque constitue un danger sérieux. La direction doit en être informée et le comprendre. L'évolution du risque est surveillée et des mesures sont mises en œuvre si cela est judicieux.
Risque faible	Le risque est acceptable. Il est géré au sein du service et des mesures sont mises en œuvre si cela est judicieux.

Illustration 12: Exemple de niveaux de tolérance au risque

La tolérance au risque est définie en dehors du processus de gestion des risques, qui se borne à mesurer et à apprécier ces derniers en fonction de cette tolérance. Il va de soi que les niveaux de tolérance aident uniquement à se faire une *vague* idée de la manière dont il faut traiter un risque. Avant d'appliquer une quelconque mesure de maîtrise du risque, il faut évaluer au cas par cas si les coûts de sa mise en œuvre sont raisonnables par rapport à la réduction du risque obtenue.

L'administration fédérale apprécie un risque principalement en fonction de son niveau (conséquences et probabilité), tout en tenant compte de la taille de l'UA concernée et de ses tâches. Dans des cas particuliers, d'autres dimensions peuvent contribuer à l'appréciation du risque:

- La relation entre le risque et le rendement constitue la norme pour les risques liés aux marchés financiers. Autrement dit, le risque supporté doit être opportun par rapport au rendement obtenu.
- En matière de sécurité, on compare fréquemment le risque et les avantages (concernant les personnes). Par exemple, le risque résiduel d'un médicament (effets secondaires) est mis en relation avec les bénéfices que ce dernier apporte aux patients afin d'en apprécier raisonnablement le risque.

[34] Par exemple, les dépenses annuelles totales de l'UA peuvent permettre d'évaluer sommairement le montant du risque *financier*.

Capacité financière à supporter le risque

Dans le cadre de son activité, l'administration fédérale s'appuie sur ses tâches et ses objectifs. Son risque global est largement lié aux tâches qu'elle doit exécuter. Elle ne peut cependant pas prévenir des risques en renonçant à certaines d'entre elles. Par conséquent, le risque global de l'administration fédérale est principalement géré à travers les différents risques individuels. C'est la raison pour laquelle on renonce à agréger tous les risques de la Confédération et à les mettre en parallèle avec le capital disponible[35].

La Trésorerie fédérale de l'AFF veille à ce que l'administration fédérale ait les liquidités et la capacité de paiement requises. Grâce aux placements de trésorerie, elle peut compenser les fluctuations mensuelles des recettes et des dépenses jusqu'à plusieurs milliards de francs. Elle est donc en mesure de couvrir des risques financiers très élevés dans le cadre de la gestion des risques (> 1 milliard de francs), même en cas de sorties de fonds rapides. Les liquidités et l'obtention de capitaux par la Confédération doivent être analysées de manière spécifique pour les événements de grande ampleur en Suisse qui représenteraient un dommage financier considérable pour la Confédération (par ex. fusion du réacteur d'une centrale nucléaire, tremblement de terre).

3.5 Maîtrise des risques

3.5.1 Actions possibles

La maîtrise des risques englobe, pour l'essentiel, les possibilités suivantes d'agir:

- ***Prévention du risque:*** l'administration fédérale ne peut pas toujours prévenir totalement un risque, car cela impliquerait de renoncer à une activité ou à une tâche et nécessiterait dans la plupart des cas une révision législative correspondante.
- ***Réduction du risque:*** différentes mesures permettent de réduire la probabilité de nombreux risques ou leurs conséquences éventuelles en cas de concrétisation du risque. Elles peuvent, d'une part, agir de manière préventive ou, d'autre part, contribuer à maîtriser aussi rapidement et avantageusement que possible un risque qui apparaît, par exemple grâce à l'élaboration et à l'application d'une gestion des crises ou de la continuité (voir les ch. 6.2 et 6.3).
- ***Transfert du risque:*** certains risques peuvent être assurés et, dès lors, transférés à des tiers. Cela peut être judicieux dans certaines circonstances (motifs économiques, notamment; voir le ch. 0). Les dérivés, les contrats et les garanties constituent d'autres possibilités de transférer un risque.

Il est fréquent qu'un *risque net* reste à la charge de l'administration fédérale même après la mise en œuvre de mesures. La prise en charge du risque par ses propres moyens peut être décidée pour des motifs économiques. Par ailleurs, certains risques doivent être supportés par la Confédération, car ils relèvent d'un mandat légal et ne peuvent pas être réduits.

3.5.2 Définition, sélection et application des mesures

En partant des causes d'un risque, le propriétaire du risque doit, avec l'aide du responsable de la gestion des risques de l'UA et de spécialistes, rechercher des mesures permettant de le réduire. Bien comprendre les causes et le rapport de cause à effet contribue à prendre des

[35] Dans l'économie privée, la capacité à supporter les risques s'appuie fréquemment sur les capitaux (propres) disponibles. En d'autres termes, les risques agrégés doivent pouvoir être couverts par un volume suffisant de capitaux propres et de liquidités. Tout risque global qui excède ce seuil menace l'existence de l'entreprise et n'est dès lors pas supportable. Il peut être réduit en renonçant à certaines activités ou opérations ou en diminuant leur ampleur ou en obtenant des capitaux supplémentaires pour couvrir ces risques.

mesures appropriées. Celles-ci doivent être décrites de manière claire et, si nécessaire, subdivisées en étapes individuelles. De plus, il faut nommer un responsable des mesures et fixer un délai pour leur mise en œuvre. Au besoin, des étapes intermédiaires seront définies.

Après avoir été identifiées, puis décrites, les mesures envisageables font l'objet d'une évaluation. Les *coûts* de leur mise en œuvre sont alors mis en relation avec les avantages qu'elles apportent, à savoir *la réduction ou le transfert du risque*. Si les conséquences sont purement financières, on peut, en tant qu'approche globale, comparer la réduction de la valeur attendue du risque[36] avec les coûts des mesures. Pour les risques présentant des conséquences non financières, il faut impérativement estimer de manière subjective le rapport entre les coûts et les avantages. Cette estimation devrait incomber au propriétaire du risque, qui, dans l'idéal, collaborera avec des spécialistes disposant du savoir-faire requis et tiendra compte de la tolérance au risque.

Les mesures considérées comme judicieuses sont ensuite classées par ordre de priorité et leur mise en œuvre est décidée par le propriétaire du risque ou, selon le montant des coûts, par une instance supérieure. Le responsable des mesures est chargé de les mettre en œuvre.

Étape du processus: maîtrise des risques
Prescriptions de l'AFF:

- Les coûts des mesures prises dans le cadre de la gestion des risques sont inscrits au budget de la Confédération.
- Il faut définir un responsable des mesures et un délai de mise en œuvre pour chacune d'elles et effectuer une analyse sommaire du rapport entre leurs coûts et leurs avantages.

Retombées de la maîtrise des risques: listes de mesures au niveau de l'UA, du département ou de la ChF et du Conseil fédéral.

3.6 Surveillance

La surveillance des risques et des mesures engagées constitue une étape importante du processus de gestion des risques, car elle garantit l'efficacité de cette dernière.

3.6.1 Surveillance des risques

La surveillance constante des risques permet de s'assurer que les connaissances relatives aux risques de l'administration fédérale sont toujours d'actualité. Elle vise, d'une part, à identifier les modifications contextuelles qui pourraient se traduire par une nouvelle appréciation des risques déjà recensés et, d'autre part, à détecter précocement les nouveaux risques. Dans l'administration fédérale, la surveillance des risques incombe en premier lieu aux propriétaires des risques, qui doivent également s'informer des risques inhérents à leur domaine de tâches, conformément à leur cahier des charges.

Risques déjà recensés

Les risques déjà recensés doivent faire l'objet d'une surveillance permanente pour que leur évolution puisse être gérée au moyen de mesures appropriées. Si un risque n'évolue pas pendant une certaine période, il convient d'examiner s'il n'est plus d'actualité et peut être retiré du portefeuille des risques. On peut par exemple retirer un risque du portefeuille lorsque son niveau a été réduit au point que le risque résiduel peut être accepté. Typiquement, un tel risque

[36] La valeur attendue d'un risque correspond au produit des conséquences financières et de la probabilité.

ne fait plus l'objet de nouvelles mesures depuis assez longtemps (coût marginal des mesures > utilité marginale d'une réduction du risque). Dans les cas suivants, il est néanmoins judicieux de garder un risque même s'il est plutôt stable:

- L'exposition au risque est labile, une certaine incertitude subsiste quant à l'évolution d'influences internes et externes (par ex. causes, interdépendances, vulnérabilité);
- Le risque résiduel est élevé. Il faut avant tout s'assurer que les mesures visant à réduire les dommages sont régulièrement surveillées et (si possible) améliorées (par ex. en ce qui concerne les ouvrages d'accumulation ou les risques de séisme; maintien de l'attention).

Nouveaux risques

Concernant la détection précoce de risques, l'administration fédérale dépend de la vigilance de ses cadres et de ses collaborateurs, qui doivent suivre les changements internes et externes et identifier leurs conséquences possibles sur la situation de la Confédération en matière de risques. Pour ce faire, ils sont mis en relation avec des spécialistes du domaine.

3.6.2 Surveillance des mesures

Le propriétaire du risque, qui a la responsabilité de ce dernier, doit surveiller la mise en œuvre des mesures de réduction du risque. Le responsable des mesures les applique et informe le propriétaire du risque des progrès réalisés et des problèmes éventuellement rencontrés lors de la mise en œuvre. De plus, les mesures prises sont intégrées dans les instruments de planification et de rapport de l'administration fédérale.

Étape du processus: surveillance des risques et des mesures
Prescription de l'AFF:

- Le propriétaire du risque surveille les risques et les mesures.

4 Rapport sur les risques

Le rapport sur les risques analysés est une retombée importante du processus de gestion des risques. Il présente les résultats correspondants, qui contribuent à la prise de décisions dans ce domaine.

4.1 Contenu du rapport sur les risques

Le rapport sur les risques comprend au moins les éléments suivants:

- une *matrice des risques*, qui expose la situation d'une UO en matière de risques et compare ces derniers;
- l'*évolution* des risques depuis le dernier rapport sur les risques;
- une *liste des mesures*, qui fournit notamment des renseignements sur la mise en œuvre des mesures engagées et sur les bases décisionnelles des nouvelles mesures qui peuvent être envisagées;
- les principales *interactions* entre les risques recensés (voir le ch. 4.5).

Rapport sur les risques
Prescription de l'AFF:

- Les rapports sur les risques dans l'administration fédérale comprennent au moins une matrice des risques, l'évolution de ceux-ci, les principales interactions entre les risques ainsi qu'une liste des mesures qui peuvent être envisagées ou qui sont en cours de mise en œuvre.
- Les rapports sur les risques sont établis à l'aide de l'application R2C_GRC. Les formats standard sont le rapport détaillé et le rapport compact. Alors que le rapport détaillé à l'attention de la direction des UA et des départements/ChF ainsi qu'à l'attention du « groupe de travail *gestion des risques de la Confédération* des deux CdG » fournit des informations complètes sur chaque risque, le rapport succinct à l'attention du Conseil fédéral résume les informations clés sur chaque risque [voir les modèles commentés à l'annexe 2].

4.2 Principes régissant l'établissement des rapports

Un rapport sur les risques compréhensible, clair et à jour aide les décideurs à identifier rapidement les informations pertinentes et à prendre des décisions optimales en matière de risques. Voici quelques principes en la matière:

- sélection d'un nombre adéquat de risques (concentration sur les risques que les destinataires du rapport peuvent influencer; voir le ch. 0);
- description des risques brève, précise et compréhensible par des tiers (ni trop ni trop peu d'informations, pas de jargon technique).

4.3 Agrégation des risques transversaux

Dans les grandes organisations comme l'administration fédérale, il est fréquent que des risques *identiques ou similaires* soient identifiés dans plusieurs départements ou UA ou qu'un risque recensé concerne plusieurs UO. Par exemple, la panne d'un système informatique central affecte souvent plusieurs UA. Il peut être judicieux de gérer centralement (du moins en partie) ces risques transversaux et de les agréger à un niveau supérieur (département ou Conseil fédéral) dans le rapport. Lorsqu'un risque est agrégé, il est analysé au ni-

veau supérieur et les interactions sont mises en évidence. La probabilité et les conséquences (du scénario du pire cas crédible) sont de nouveau évaluées, tout en tenant compte des estimations et des hypothèses retenues aux échelons inférieurs.

Les principes suivants de l'agrégation des risques visent à garantir une compréhension commune et une procédure aussi uniforme que possible dans l'administration fédérale[37].

4.3.1 Décision d'agrégation

Les risques sont agrégés uniquement si cela apporte une valeur ajoutée, comme l'illustrent les exemples suivants:

- L'agrégation de risques partiels au niveau supérieur révèle l'importance globale d'un risque ou la nécessité d'agir.

  Exemple: l'impact négatif total d'une panne de serveur informatique n'est identifiable que si l'on tient compte de *toutes* les conséquences liées à la défaillance des applications dans les UA.

- Le risque peut être géré de manière plus efficace ou plus économique grâce à des mesures pilotées centralement (exploitation des effets d'échelle).

  Exemple: une campagne de sensibilisation concernant l'utilisation sûre des mots de passe coûte moins cher si elle est réalisée à l'échelle de la Confédération plutôt que dans chaque UA.

- La fixation d'un ordre des priorités en ce qui concerne les mesures de réduction du risque dans le cadre d'une agrégation permet de répartir plus efficacement les ressources disponibles.

  Exemple: les moyens budgétés pour améliorer la sécurité parasismique seront utilisés plus efficacement si, après vérification de *tous* les bâtiments fédéraux (approche agrégée), des priorités sont définies.

- L'agrégation à un niveau supérieur favorise l'identification et la compréhension des interactions et des interfaces.

  Exemple: les interactions entre la troisième réforme de l'imposition des entreprises / le Projet fiscal 2017 (AFC), les conséquences sur le budget de la Confédération (AFF) et les relations avec l'UE (SFI) peuvent être analysées et gérées au niveau du département (DFF).

En l'espèce, il convient de formuler une mise en garde, car l'agrégation peut parfois entraîner une banalisation des risques. Elle ne devrait donc pas être réalisée dans le seul but d'obtenir une meilleure vue d'ensemble thématique à un échelon hiérarchique supérieur. Il est en effet possible que des informations pertinentes sur le risque soient perdues lors d'une agrégation et que le risque agrégé doive être présenté de manière si générale que la menace et la nécessité d'agir ne soient plus manifestes.

- *Exemples négatifs:* agrégation d'un crash aérien, d'un déraillement et d'un incendie dans un tunnel sous «Accidents majeurs»; perte de savoir-faire, corruption, absence de motivation au travail et abus de confiance regroupés sous «Risques liés au personnel»; retards dans plusieurs projets indépendants rassemblés sous «Projets retardés».

4.3.2 Compétences en matière d'agrégation

La responsabilité concernant *l'agrégation* d'un risque transversal doit être clarifiée dans le cadre du processus de gestion des risques. Elle diffère de la responsabilité concernant *la gestion* du risque transversal (voir le ch. 4.3.3).

[37] Voir également l'annexe 10, qui présente les interactions et les structures de certains groupes de risques potentiels au niveau de la Confédération.

À l'échelon du Conseil fédéral, les responsabilités pour l'agrégation d'un risque transversal sont fixées par la CSG[38][39]. Il existe en principe deux possibilités d'affectation:

- Une UA ou un groupe de travail interdépartemental (voire une direction de projet) a déjà un ***mandat concret de pilotage et de gestion centralisés*** d'un risque transversal pour toute l'administration fédérale (loi, ordonnance sur l'organisation, mandat délivré, par ex., par le Conseil fédéral, etc.). Cette entité est responsable de la gestion du risque agrégé et obtient les informations nécessaires auprès des UA concernées. Le service de coordination Gestion des risques de la Confédération ou les responsables de la gestion des risques des départements la soutiennent sur le plan méthodologique.
- Si l'agrégation d'un risque transversal est opportune (voir le ch. 4.3.1) mais qu'il n'existe pas encore de service désigné pour assumer le pilotage centralisé, cette agrégation incombe aux responsables concernés de la gestion des risques des départements ou au service de coordination Gestion des risques de la Confédération, qui font appel aux spécialistes requis et aux UO chargées de la gestion des risques. La CSG ou la direction compétente se fonde ensuite sur cette agrégation pour attribuer les responsabilités.

4.3.3 Clarification des responsabilités en matière de gestion

La désignation du propriétaire d'un risque transversal repose, en principe, sur les mêmes critères que pour un risque individuel (règle de base: adéquation des tâches, des compétences et des responsabilités [TCR]. En d'autres termes, la personne responsable peut influer sur le risque et le modifier).

En général, plusieurs UA participent à la gestion des risques transversaux, en particulier lors de la mise en œuvre de mesures de réduction du risque (par ex. mesures de protection contre les cyberattaques). Les tâches des UA concernées permettent normalement de déterminer à quelle UO il est le plus judicieux de confier la responsabilité d'un aspect de la gestion des risques (identification, évaluation, mesures [évaluation, décision, mise en œuvre], surveillance). Il faut définir les interfaces destinées à la collaboration et les responsabilités pour éviter les doublons ou les lacunes dans la gestion des risques transversaux.

La gestion des risques transversaux est complexe[40]. Cette complexité est notamment due au fait que, souvent, le propriétaire du risque transversal n'a pas le pouvoir de donner des directives aux propriétaires des risques sources et aux responsables des mesures (principe de l'administration décentralisée). À l'échelon du Conseil fédéral, on tient compte de cette situation en organisant tous les six mois (dans le cadre des processus concernant les rapports sur les risques) une séance de coordination pour chaque risque transversal à laquelle participent le propriétaire du risque transversal et les propriétaires des risques sources. Dans ce contexte, on s'accorde sur la description du risque, sur le scénario du pire cas, sur l'évaluation du risque transversal et des risques sources ainsi que sur les mesures à mettre en œuvre. Le contrôle de gestion centralisé des mesures effectué par le propriétaire du risque transversal revêt une importance majeure. D'éventuelles divergences doivent être transmises par le service de coordination Gestion des risques de la Confédération à la CSG puis, si nécessaire, au Conseil fédéral.

L'agrégation des risques transversaux est essentiellement un processus descendant, raison pour laquelle les risques sources sont généralement déterminés dans le cadre de la séance de coordination mentionnée plus haut ou par le propriétaire du risque transversal. En dernière instance, c'est la CSG (ou la direction du département ou de l'UA) qui se prononce.

[38] Ch. 5, al. 2, let. b, des directives du CF sur la politique de gestion des risques

[39] Au niveau du département et des UA, ces responsabilités incombent généralement à la direction.

[40] Voir également le ch. 6 du rapport du CDF n°17476 «La gestion des risques de la Confédération en tant qu'instrument de pilotage» du 3 mai 2018

4.3.4 Rapport

En principe, les risques transversaux figurent dans le rapport sur les risques tant au niveau de l'UA (s'ils sont pertinents pour elle) qu'à un niveau supérieur (sous une forme agrégée)[41].

4.3.5 Échange d'informations

Un échange régulier d'informations entre le propriétaire du risque transversal et les responsables des risques sources est indispensable pour réussir à gérer un risque transversal. Les propriétaires des risques sources doivent connaître notamment les grandes lignes des mesures visant à réduire le risque.

Généralement, un échange entre les responsables de la gestion des risques des départements et des UA et les propriétaires des risques qui s'occupent de risques transversaux est essentiel[42]. Il permet d'échanger les expériences et d'élaborer de nouvelles idées pour traiter les risques transversaux.

Principes de l'agrégation des risques
Prescriptions de l'AFF:

- En cas de risques transversaux, il faut vérifier si une agrégation est judicieuse, voire nécessaire et à quel niveau (UA, département, Confédération).
- La compétence ou la responsabilité en matière d'agrégation des risques doit être définie.
- Il convient de clarifier ou de définir les tâches et les responsabilités des différents acteurs (identification, analyse, évaluation, mesures, surveillance). Les informations manquantes pour la gestion d'un risque agrégé doivent être demandées.
- Le risque agrégé est présenté de manière claire, compréhensible et aussi complète que possible dans le rapport sur les risques.
- L'échange d'informations entre tous les acteurs doit être encouragé activement.

4.4 Sélection des risques

Lorsque de nombreux risques existent, il est judicieux de se concentrer dans le cadre du rapport sur quelques risques pertinents pour les décideurs. Cela facilite la lisibilité de la matrice des risques et permet aux cadres de se focaliser sur la gestion des principaux risques. En ce qui concerne la densité des informations, plus le niveau hiérarchique est élevé, plus l'information doit être condensée.

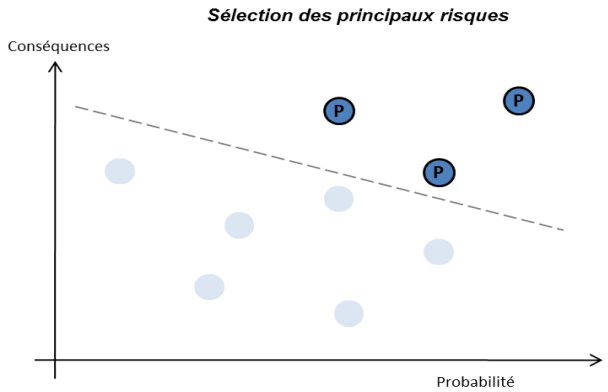


Illustration 13: Sélection des principaux risques

[41] Les risques initiaux qui sont agrégés ne figurent pas dans la matrice des risques si l'agrégation des risques à un niveau supérieur est effectuée dans R2C_GRC au moyen de la fonction «Risques agrégés».

[42] Le service de coordination Gestion des risques de la Confédération encourage l'échange d'informations et d'expériences entre les UA et les départements par l'intermédiaire de manifestations, de notes d'information, etc.

Dans l'administration fédérale, les règles suivantes garantissent l'établissement de rapports en fonction des échelons:

Les risques présents au niveau des UA sont recensés, analysés et évalués dans le cadre du processus de gestion des risques. En parallèle, le Secrétariat général des départements applique le même processus aux risques du département (approche descendante). Certains de ces risques sont exposés à la direction des UA. Les directives ne précisent pas comment la direction consolide les risques au sein d'une UA. Le service de coordination de l'AFF recommande toutefois de fixer un seuil pour l'établissement des rapports au niveau de l'UA ou un nombre approximatif de risques principaux, en accord avec le responsable de l'UA.

Ensuite, chaque UA déclare ses trois principaux risques au responsable de la gestion des risques du département. Si plus de trois risques dépassent le seuil pour l'établissement des rapports du département, ils sont également communiqués. Défini par la direction du département, ce seuil doit répondre aux prescriptions à l'échelon du Conseil fédéral. Les risques qui ne sont pas annoncés au département *relèvent du domaine de l'UA*. Ceux que cette dernière notifie au département constituent les *risques du département*.

Chaque département et la ChF communiquent leurs trois principaux risques au service de coordination de l'AFF en vue du rapport au Conseil fédéral. La direction du département / de la ChF définit les trois principaux risques de son UO. Les autres risques qui présentent des conséquences très importantes ou importantes et sont probables ou très probables (probabilité comprise entre 33 % et 100 %) doivent également être déclarés. Les risques qui ont été notifiés par chaque département et par la ChF sont appelés *risques majeurs*. Vérifiés par le service de coordination de l'AFF, ils font l'objet d'un premier examen de plausibilité, d'une comparaison croisée et d'une harmonisation. Un entretien avec le secrétaire général de chaque département permet d'éclaircir certains points, voire d'adapter les risques. La version remaniée est ensuite soumise à la CSG, qui contrôle l'exhaustivité des risques et agrège les éventuels risques transversaux. Les risques les plus importants sont alors sélectionnés pour le rapport au Conseil fédéral, qui en comprend entre dix et quinze (*risques du Conseil fédéral*).

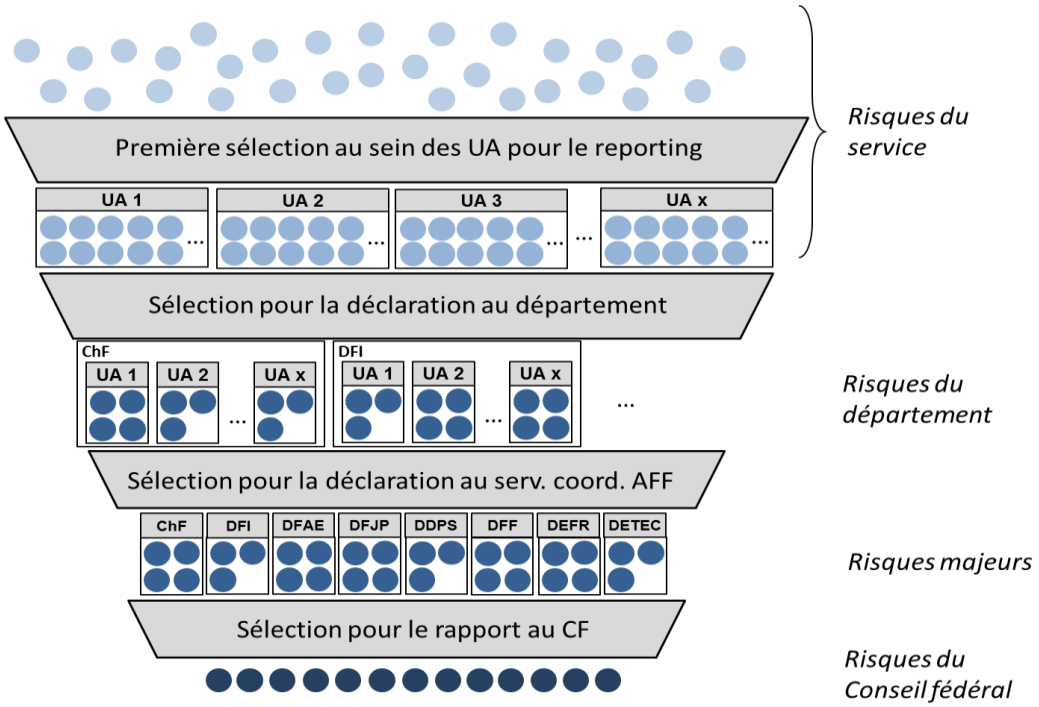


Illustration 14: Sélection des risques dans l'administration fédérale

4.5 Interactions

4.5.1 Traitement organisationnel des interactions

Au *niveau du Conseil fédéral*, la Conférence des secrétaires généraux est chargée de vérifier les interactions des risques déclarés par les départements et la ChF. Le service de coordination de l'AFF lance et suit la concertation interdépartementale requise à cet effet.

Au *niveau du département*, le responsable correspondant de la gestion des risques coordonne la concertation requise pour analyser et gérer les interactions entre les unités du département.

Si le risque d'une UA présente des interactions avec un risque d'une UA d'un *autre* département / de la ChF, le service de coordination de l'AFF lance et suit la concertation entre ces deux UA.

4.5.2 Représentation des interactions

Une définition précise du mécanisme d'action est nécessaire à l'agrégation quantitative de tous les risques. Lors d'une approche qualitative (comme celle qui est appliquée par l'administration fédérale au niveau du département / de la ChF et du Conseil fédéral), une analyse et la compréhension des interactions éventuelles sont essentielles pour:

- identifier la menace potentielle posée par les risques liés;
- élaborer des approches afin de rompre ces liens le cas échéant.

Les interactions avec d'autres risques sont *mentionnées* et exposées dans la description du risque. Elles peuvent également être représentées graphiquement.

Rapports sur les risques
Prescriptions de l'AFF:

- Les UA communiquent au département tous les risques dépassant le seuil défini par celui-ci, mais au moins leurs trois risques principaux.
- Les départements et la ChF communiquent au service de coordination de l'AFF tous les risques dépassant le seuil fixé au niveau de la Confédération (risques ayant des conséquences «très importantes» et risques ayant des conséquences «importantes» qui sont considérés comme «probables» ou «très probables»), mais au moins leurs trois risques principaux.
- Les interactions entre les risques sont analysées et exposées dans les rapports sur les risques sous forme de texte ou de graphiques.
- Au besoin les risques transversaux sont agrégés au niveau hiérarchique supérieur.

5 Communication

Les flux d'information et la communication entre les différents acteurs de la gestion des risques sont importants. Au besoin, ils doivent faire partie de chaque phase du processus de gestion des risques (voir le ch. 3.1). Une communication interne et externe bien conçue est nécessaire et utile pour

- analyser les risques à l'aide des meilleures connaissances spécialisées disponibles, en considérant plusieurs aspects (issus de différents domaines);
- garantir la prise en compte des intérêts, des besoins d'information et des avis de tous les groupes d'interlocuteurs et renforcer ainsi la confiance dans la gestion des risques;
- garantir une réaction appropriée et rapide à l'évolution de la situation en matière de risques.

La communication sur les risques dans des situations exceptionnelles (urgences et crises) est organisée et pilotée par la ChF. Elle n'est donc pas exposée dans la section suivante.

Les flux d'information entre les différents acteurs du processus de gestion des risques sont présentés en détail au ch. 3.1. Le ch. 5.1 expose d'autres éléments de la communication interne sur les risques. La communication externe sur les risques de l'administration fédérale est abordée au ch. 5.2, tandis que le ch. 5.3 est consacré au principe de la transparence, à la classification et à l'archivage des informations dans la gestion des risques.

5.1 Communication interne et formations

Des formations, des manifestations et des canaux d'information internes permettent de s'assurer que les collaborateurs de l'administration fédérale sont sensibilisés et formés à la gestion des risques. Il en découle une amélioration de la culture du risque, un échange de savoir sur la gestion des risques et un renforcement des connaissances dans ce domaine.

5.1.1 Formations

L'administration fédérale propose régulièrement les cours suivants sur la gestion des risques:

Formation	Durée	Fréquence	Public cible
Risikomanagement für Topkader (gestion des risques pour les cadres supérieurs)	½ jour	Selon la demande	Propriétaire du risque
«Les clés de la gestion des risques»	1 jour	Env. 2 fois par an	Personnes intéressées (délégués à la BCM, juristes, responsables de projet etc.)
«Umsetzung Risikomanagement» (mise en œuvre de la gestion des risques)	3 jours	Env. 2 fois par an	Responsables de la gestion des risques des départements et responsables des UA (obligatoire pour ces personnes)
Cours Risk to Chance (R2C_GRC)	½ jour	Env. 2 à 3 fois par an	Responsables de la gestion des risques des départements et des UA

5.1.1.1 Cours «Umsetzung Risikomanagement» (mise en œuvre de la gestion des risques)

Ce cours expose les principaux éléments de la gestion des risques dans l'administration fédérale et forme à leur application pratique. Les participants étudient la mise en place d'un système de gestion des risques, les méthodes d'évaluation des risques et le processus de gestion des risques, et sont en mesure d'appliquer ces connaissances dans leur UO. Les principaux éléments du présent manuel sont traités et expliqués pendant le cours, qui est obligatoire pour les responsables de la gestion des risques des départements et des UA.

5.1.1.2 Formation R2C_GRC

Proposé par la société allemande Schleupen AG[43], le logiciel de gestion des risques utilisé dans l'administration fédérale s'appelle Risk to Chance (R2C_GRC). Toutes ses fonctions sont expliquées dans un guide[44]. Le service de coordination de l'AFF gère l'application R2C_GRC au sein de l'administration fédérale. C'est le premier interlocuteur en cas de questions ou de problèmes et pour l'octroi des autorisations. En principe, les risques enregistrés dans le système sont gérés par les responsables de la gestion des risques des départements / de la ChF et des UA, qui ont uniquement accès aux risques de leur propre UO. Certains collaborateurs peuvent également bénéficier d'un droit de consultation.

La structure, la navigation et les principales fonctions de R2C_GRC sont présentées lors d'un cours d'une demi-journée. Les participants peuvent s'exercer au maniement du logiciel sur un PC individuel et poser des questions.

Le cours est organisé par le service de coordination de l'AFF. Il est obligatoire pour les responsables de la gestion des risques des départements et des UA, car le logiciel R2C_GRC est utilisé pour gérer les risques au sein de la Confédération.

5.1.1.3 Cours de formation destiné aux cadres (propriétaires des risques)

Ce cours de formation sensibilise les propriétaires des risques de l'administration fédérale à leurs responsabilités dans le traitement des risques.

Prescription de l'AFF:

- La formation R2C_GRC et le cours «Umsetzung Risikomanagement» (mise en œuvre de la gestion des risques; en allemand) sont obligatoires pour les responsables de la gestion des risques des départements et des UA.

5.1.2 Manifestations

Réseau Management des risques

L'association «Réseau Management des risques» propose aux participants à un processus de gestion des risques une plate-forme consacrée aux contacts professionnels, à l'échange d'expériences et au perfectionnement, ainsi que des manifestations et des publications axées sur la pratique. Elle prévoit d'organiser une à deux manifestations par an sur un thème concret de la gestion des risques. Le cercle des participants englobe, en premier lieu, toutes les personnes intéressées de l'administration fédérale qui ont un lien avec la gestion des risques et d'autres personnes intéressées par cette thématique.

De plus, d'autres manifestations, parfois plus spécifiques, sur des sujets concrets en matière de risques sont organisées dans les départements / à la ChF et dans les UA.

Souhaité au sein de l'administration fédérale, l'échange des connaissances sur la gestion des risques est piloté et soutenu par le service de coordination de l'AFF.

5.1.3 Canaux d'information internes

Un *sharepoint*[44] a été spécialement mis en place pour faciliter les échanges professionnels entre les responsables de la gestion des risques des départements et des UA. Il comprend des instructions, des directives et le manuel concernant la gestion des risques de la Confédération, des documents méthodologiques sur la gestion des risques ainsi que des moyens auxiliaires et instruments spécifiques pour mettre en œuvre le processus correspondant.

[43] Elle propose également une assistance technique.
[44] https://portal.collab.admin.ch/sites/601-Risikomanagement-Bund/RC/SitePages/Homepage.aspx

5.2 Communication externe

Le Conseil fédéral informe le public sur la gestion des risques de la Confédération.

5.2.1 Rapport de gestion

Chaque année, le Conseil fédéral établit un rapport sur son activité à l'attention de l'Assemblée fédérale, qui est publié sur le site Internet de la ChF[45]. Le volume I «Points essentiels de la gestion du Conseil fédéral» comprend une partie sur la gestion des risques de la Confédération, qui présente en premier lieu les nouveautés conceptuelles et organisationnelles dans ce domaine. Certains risques de la Confédération y sont exposés de manière très générale uniquement.

5.2.2 Compte d'État et budget

Les comptes d'État[46] et les budgets[47] sont également accessibles au public. Ils comprennent différentes informations issues de la gestion des risques.

1. Le *chapitre général* «Gestion des risques et situation en matière de risques» figure dans l'«annexe au compte annuel» (compte d'État, tome 1) et le budget. Il fournit des informations sur le traitement des risques, sur les instruments et les mesures de gestion des risques, sur la situation générale de la Confédération en matière de risques et sur la publication de ces derniers. Pour des raisons de confidentialité, on renonce à une description précise et détaillée des différents risques s'ils ne sont pas inscrits au bilan ou n'apparaissent pas dans les engagements conditionnels.
2. Les frais de mise en œuvre des *mesures* décidées et à réaliser dans le cadre de la gestion des risques doivent être pris en compte lors de l'établissement du budget.
3. La loi sur les finances de la Confédération[48] et son ordonnance[49] définissent les conditions juridiques de la gestion des risques dans le budget et les comptes (voir le ch. 6.5 et l'aperçu à l'annexe 6). Il faut respecter les dispositions en vigueur énoncées dans les «Directives et instructions relatives à la gestion budgétaire et comptable de la Confédération»[50].

Le service de coordination de l'AFF rédige la section générale de l'annexe au compte annuel qui est consacrée à la gestion des risques. Les propriétaires des risques et les UA compétentes sont en premier lieu chargés de répertorier les mesures prises et les engagements légaux (provisions et engagements conditionnels) dans le budget et le compte d'État.

5.2.3 Prise de position du Conseil fédéral sur les rapports parlementaires concernant la gestion des risques

Depuis plusieurs années, les CdG et la Délégation des finances des Chambres fédérales suivent attentivement la gestion des risques de la Confédération. Elles rendent compte de leurs activités en la matière dans leurs rapports annuels et dans des rapports distincts, qui sont publiés dans la Feuille fédérale, généralement assortis d'un avis du Conseil fédéral. Ces rapports traitent généralement les questions de principes en lien avec la mise en œuvre de la gestion des risques de la Confédération et non pas les risques individuels de la Confédération[51].

---

[45] https://www.bk.admin.ch/dokumentation/publikationen/00290/00929/index.html?lang=fr

[46] http://www.efv.admin.ch/f/dokumentation/finanzberichterstattung/staatsrechnungen.php

[47] http://www.efv.admin.ch/f/dokumentation/finanzberichterstattung/budget.php

[48] Art 49, al. 3, LFC

[49] Art. 3, let. b et d, et art. 56, al. 2, OFC

[50] http://intranet.accounting.admin.ch/; en particulier les chap. *5.3.4 Provisions* et *10.2 Créances et engagements conditionnels* du manuel

[51] En général, le rapport sur les risques à l'attention du Conseil fédéral est examiné en avril, par un groupe de travail des CdG.

5.3 Classification, principe de la transparence et archivage

5.3.1 Protection des informations dans le cadre de la gestion des risques de la Confédération; principe de la transparence

Classification

La classification et le traitement des informations de la Confédération sont réglés dans l'ordonnance concernant la protection des informations[52]. En fonction du degré de protection requis, soit les informations sont classifiées, soit elles sont attribuées aux échelons de classification suivants: SECRET, CONFIDENTIEL ou INTERNE (art. 4, al. 1, OPrI).

L'établissement d'informations classifiées, leur communication et le fait de les rendre accessibles doivent être limités à un strict minimum; il n'est permis de communiquer ou de rendre accessibles des informations classifiées qu'aux personnes qui doivent en avoir connaissance (art. 13, al. 1 et 2, OPrI). Selon les prescriptions de traitement des informations classifiées figurant dans l'annexe à l'OPrI, les informations classifiées CONFIDENTIEL doivent être sauvegardées électroniquement sous forme chiffrée et conservées physiquement dans un conteneur de sécurité. L'envoi de telles informations par courriel se fait sous forme chiffrée.

Une partie des informations qui figurent sur la feuille de risques sont connues de tous (par ex. la tâche légale de la Confédération, les problèmes qui peuvent entraver l'exécution des tâches par l'administration fédérale, les causes des risques). En revanche, les informations portant par exemple sur l'estimation de la survenance et des conséquences possibles d'un risque établie par les spécialistes compétents ainsi que la description des mesures prévues pour réduire les risques peuvent être classifiées CONFIDENTIEL si l'une des conditions de l'art. 6, al. 1, OPrI, est remplie.

Une feuille de risques, mais surtout un rapport sur les risques aux niveaux des unités administratives, des départements ou du Conseil fédéral doivent être considérés comme un recueil au sens de l'art. 4, al. 2, OPrI. Chaque document regroupe des informations plus ou moins sensibles. Il s'agit de décider si un recueil doit être classifié *dans son intégralité* et à quel échelon il peut être attribué.

Dans le cadre de la classification d'une information, il faut tenir compte du fait qu'une application excessivement restrictive de la protection des informations peut entraver considérablement la communication interne sur les risques et par conséquent le dialogue sur les risques. La distribution de l'information classifiée ne doit pas non plus être limitée inutilement. En revanche, la confidentialité des informations réellement sensibles doit être absolument garantie, sinon elles ne peuvent pas être mises à la disposition de la gestion des risques.

Classification
Recommandation de l'AFF:

D'après le service de coordination Gestion des risques de la Confédération, il n'est guère possible – du moins aux niveaux de la Confédération et des départements – de décider au cas par cas, pour chaque information sur un risque, si une classification se justifie. En vertu de l'art. 4, al. 2, OPrI («recueil»), il estime qu'il est judicieux de classifier CONFIDENTIEL tous les documents et informations qui portent sur des risques spécifiques (feuilles de risques, rapports sur les risques, données contenues dans le logiciel de gestion des risques utilisé au sein de la Confédération) et de n'évaluer la possibilité de lever (partiellement ou entièrement) la classification que si les circonstances le justifient dans un cas précis, par exemple si une demande d'accès est déposée selon la loi sur la transparence.

[52] OPrI; RS **510.411**

Principe de la transparence

La LTrans vise à promouvoir la transparence quant à la mission, à l'organisation et à l'activité de l'administration en garantissant l'accès aux documents officiels (art. 1 LTrans). On entend par document officiel toute information qui a été enregistrée sur un quelconque support, qui est détenue par l'autorité ou qui concerne l'accomplissement d'une tâche publique, ou encore tout document pouvant être établi par un traitement informatisé simple sur la base d'informations enregistrées (art. 5, al. 1 et 2, LTrans). Le principe de la transparence s'applique aussi aux documents officiels de la gestion des risques de la Confédération (art. 2 à 4 LTrans).

Les documents qui n'ont pas atteint leur stade définitif d'élaboration ne sont pas considérés comme des documents officiels au sens de la LTrans (art. 5, al. 3, let. b, LTrans). Un droit d'accès n'existe que pour un document dont la rédaction est terminée par son auteur, qui l'a définitivement remis au destinataire notamment à titre d'information ou pour que celui-ci prenne position ou une décision (art. 1, al. 2, de l'ordonnance sur la transparence[53]). Les documents liés à la gestion des risques de la Confédération ne sont donc concernés par la LTrans qu'à partir de la phase de reporting.

Le droit d'accès peut être limité, différé ou refusé, notamment lorsque l'accès à un document officiel:

- est susceptible de porter notablement atteinte au processus de la libre formation de l'opinion d'une autorité fédérale, de l'Assemblée fédérale ou du Conseil fédéral;
- entrave l'exécution de mesures concrètes prises par une autorité conformément à ses objectifs;
- risque de compromettre la sûreté intérieure ou extérieure de la Suisse;
- risque de compromettre les intérêts de la Suisse en matière de politique extérieure et ses relations internationales;
- risque de compromettre les relations entre la Confédération et les cantons ou les relations entre cantons;
- risque de compromettre les intérêts de la politique économique ou monétaire de la Suisse (art. 7, al. 1, LTrans).

La prise de position sur une demande d'accès à un document relève en principe de l'autorité qui l'a élaboré. L'art. 11 OTrans règle les cas spéciaux. Selon le ch. 2 de la décision du Conseil fédéral du 1er avril 2015 concernant l'évaluation de la loi sur la transparence[54], lorsqu'une demande d'accès est adressée à plusieurs autorités, la Chancellerie fédérale (Conférence des services d'Information, Section du droit) assure la coordination entre les autorités en collaboration avec le Département fédéral de justice et police (Office fédéral de la justice). Lorsque des documents concernent la gestion des risques de la Confédération, la compétence dépend généralement du type de document ou de l'autorité qui l'a établi:

- feuille de risques: l'unité administrative qui a identifié le risque;
- rapport de l'unité administrative: l'unité administrative;
- rapport du département: le département;
- risques transversaux au niveau du département (y c. risques initiaux): le département;
- rapport à l'intention de la Conférence des secrétaires généraux, du Conseil fédéral et du groupe de travail des Commissions de gestion: service de coordination Gestion des risques de la Confédération (AFF);
- risques transversaux au niveau du Conseil fédéral (y c. risques initiaux) à l'intention de la Conférence des secrétaires généraux, du Conseil fédéral et du groupe de travail des Commissions de gestion: service de coordination Gestion des risques de la Confédération (AFF).

[53] OTrans; RS **152.31**

[54] EXE 2015.0216

Procédure à suivre en cas de demande d'accès à un document classifié
Recommandation de l'AFF:

1. Il convient d'éclaircir la question de la compétence pour la prise de position sur la demande: l'auteur du document classifié est compétent (art. 11, al. 5, OTrans en relation avec art. 13, al. 3, OPrI).
2. L'auteur examine si le document demandé entre dans le champ d'application de la LTrans, et notamment s'il a atteint son stade définitif d'élaboration (art. 5, al. 3, let. b, LTrans; art. 1, al. 2, OTrans).
3. Il examine, indépendamment de l'éventuelle mention de classification, s'il y a lieu d'autoriser, de limiter, de différer ou de refuser l'accès conformément à la LTrans (art. 13, al. 3, OPrI).
4. Il examine si la classification du document selon les critères énoncés à l'art. 6, al. 1, OPrI est encore justifiée. Si ce n'est plus le cas, le document est déclassifié (entièrement ou en partie en application du principe de la proportionnalité; art. 11, al. 5, OTrans).

5.3.2 Archivage

Les documents établis (ou reçus) dans le cadre de la gestion des risques de la Confédération sont soumis aux dispositions de la loi fédérale sur l'archivage (LAr)[55]. Les départements, la ChF et les UA sont responsables de l'archivage de leurs documents.

De plus, les différents risques sont enregistrés et archivés *électroniquement* dans l'application de gestion des risques Risk to Chance (R2C_GRC). Ils sont recensés ou actualisés au moins une fois par an, puis font l'objet d'un historique au sein de R2C_GRC. Lorsque des risques *apparaissent*, les dommages subis et les enseignements tirés sont également consignés dans R2C_GRC. Pour des questions de traçabilité, les risques *qui ont été réglés* ne sont pas supprimés dans R2C_GRC, mais acquièrent le statut «Terminé».

[55] RS **152.1**

6 Interfaces

Les UO, les projets et les fonctions de l'administration fédérale qui ont une interface avec la gestion des risques sont présentés ci-après. L'objectif est d'expliquer brièvement les tâches de chaque fonction ou organisation, de les distinguer des tâches relevant de la gestion des risques et de définir les interfaces et les flux d'information. On contribue ainsi à obtenir une gestion des risques efficiente, sans redondances ni gaspillages.

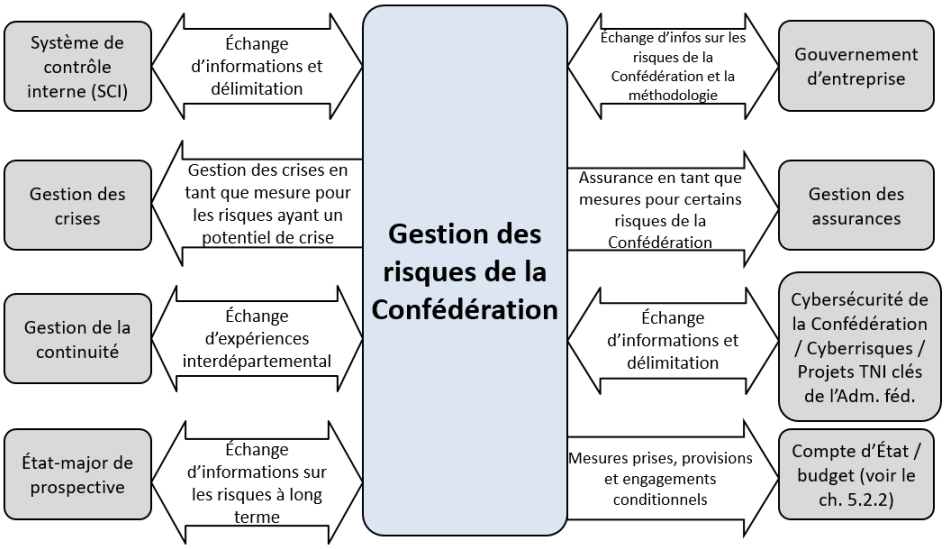


Illustration 15: Interfaces avec la gestion des risques (liste non exhaustive)

6.1 Système de contrôle interne (SCI)

Le système de contrôle interne (art. 39 LFC, art. 36 OFC) identifie les risques opérationnels liés aux finances. Il décrit et évalue les risques identifiés et fixe des mesures de contrôle réglementaires, organisationnelles et techniques réduisant les risques. Tant les risques identifiés et évalués que l'efficacité des contrôles visant à réduire les risques font l'objet d'une vérification périodique. Le SCI opère une distinction entre les contrôles automatisés (par ex. autorisations et validations) et les contrôles manuels (par ex. vérification / contrôle de plausibilité, principe du double contrôle). En l'espèce, il faut si possible introduire des contrôles automatisés.

Alors que la gestion des risques se caractérise par sa large portée, le SCI se concentre sur l'identification des risques opérationnels affectant les processus qui ont une incidence financière et sur la description et la mise en œuvre de mesures de contrôle propres à réduire ces risques. Le SCI fait donc partie intégrante de la gestion des risques de l'administration fédérale.

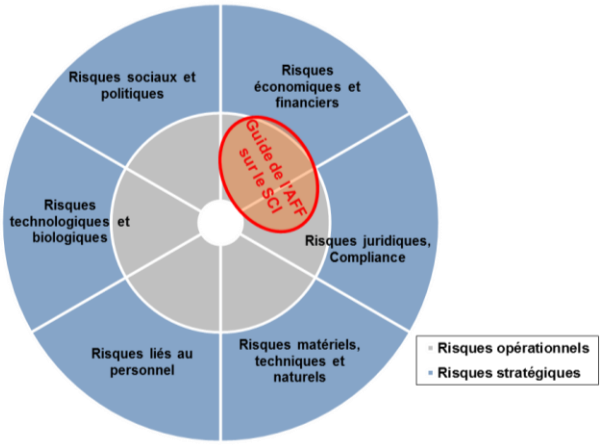


Illustration 16: SCI et gestion des risques

Interfaces avec la gestion des risques:

L'identification et l'évaluation des risques opérationnels affectant les processus qui ont une incidence financière ainsi que l'élaboration des mesures de contrôle font théoriquement partie des tâches tant du responsable de la gestion des risques de l'UA que du responsable du SCI. Pour optimiser la répartition du travail, le responsable de la gestion des risques de l'UA se concentre, dans le cadre du processus de gestion des risques, sur l'identification de tous les autres risques de l'UA, mais complète sa liste des risques avec les risques pertinents identifiés dans le cadre du processus SCI.

Échange d'informations requis:

Un échange régulier doit avoir lieu au niveau des UA entre le responsable de la gestion des risques de l'UA et le responsable du SCI. À cet égard, il convient d'analyser si:

- les risques identifiés dans le cadre de la gestion des risques impliquent des adaptations du SCI ou de nouvelles mesures de contrôle;
- les risques identifiés dans le cadre du processus SCI doivent être recensés par la Gestion des risques et faire l'objet d'un rapport.

6.2 Gestion des urgences et des crises (détection précoce, maîtrise)

La gestion des risques comprend une gestion appropriée des urgences, des crises et de la continuité[56], qui sert à maîtriser les risques majeurs lorsque ceux-ci se concrétisent. En présence de risques ayant des conséquences majeures, il est important de disposer d'organes, d'installations et de processus permettant de remédier aussi rapidement que possible au dommage (gestion des urgences) ou de défendre la réputation, la marge de manœuvre ou l'existence de l'organisation concernée (gestion des crises)[57]. De plus, selon la durée de la phase de rétablissement, les processus clés de cette organisation doivent être conservés (gestion de la continuité[58]). En ce sens, la gestion des urgences, des crises et de la continuité est chargée des mesures contribuant à la maîtrise des dommages et à l'atténuation des conséquences lorsque des risques se concrétisent. Ces tâches incombent en principe aux supérieurs hiérarchiques. La gestion des risques donne certes l'impulsion pour mettre en place des mesures destinées à gérer les situations d'urgence, les crises et la continuité et elle est également chargée de prendre les mesures qui s'imposent, mais elle ne s'occupe pas directement de la préparation de ces dernières ni de la résolution des crises.

Surveiller les risques signifie aussi en suivre et en déterminer l'évolution en fonction du contexte. La détection précoce de situations d'urgence ou de crises fait donc partie intégrante de la gestion des risques. Elle permet aussi de mettre en place à temps une gestion adéquate de l'urgence ou de la crise (création préventive d'une organisation de crise, exercices basés sur des scénarios d'urgence ou de crise, etc.).

Le service de détection précoce des crises de la ChF (section Aide à la conduite stratégique)[59] opère selon une stratégie à court terme (jusqu'à un an et demi). Elle complète les instruments existants par un regard extérieur sur la situation actuelle et collabore avec la gestion des risques de la Confédération. À l'aide d'une analyse continue des principales sources externes à la Confédération, le service de détection précoce des crises de la ChF identifie les nouveaux risques et les crises qui se profilent et vérifie les risques figurant dans le rapport sur les risques en tenant compte de l'évolution de la situation. Les nouvelles observations ou les différences d'évaluation sont communiquées au département concerné par l'intermédiaire du service de

[56] Ch. 4, al. 6, des directives du CF sur la politique de gestion des risques

[57] Voir les définitions d'«urgence» et de «crise» à l'annexe 1

[58] Les dispositifs de la gestion de la continuité sont également élaborés à l'avance et permettent à cet égard de maîtriser les risques dans le cadre de leur gestion (voir le ch. 6.3).

[59] Mandat légal selon l'art. 32, let. g et 33, al. 1bis, LOGA (en vigueur depuis le 1er janvier 2015)

coordination Gestion des risques. La coopération entre le service de détection précoce de la ChF et la gestion des risques de la Confédération est réglée dans un concept détaillé. En cas de différences d'évaluation entre les sources de la détection précoce des crises de la ChF et le département (responsable des risques), la ChF peut, en accord avec le département concerné, en informer le Conseil fédéral de manière appropriée.

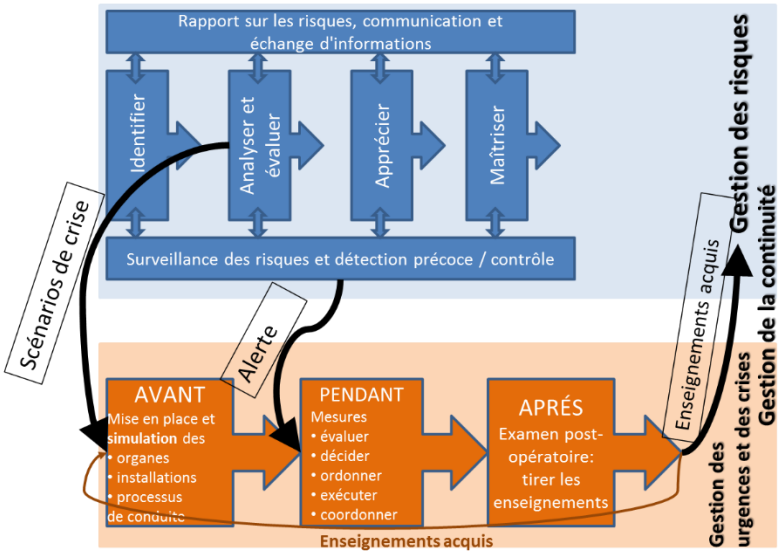


Illustration 17: Interfaces entre la gestion des risques et la gestion des crises

L'illustration ci-après présente un aperçu des instruments et des UO de l'administration fédérale qui sont concernés par les situations d'urgence et de crise. Certains s'occupent en permanence de la détection précoce des crises (partie gauche du tableau), tout en ayant des priorités et un horizon temporel différents. Ils se complètent et permettent aux échelons hiérarchiques supérieurs d'avoir une vue d'ensemble plus large. Dans la partie droite du tableau figurent les organes qui interviennent ponctuellement, lorsqu'une crise survient (maîtrise de situations particulières et extraordinaires).

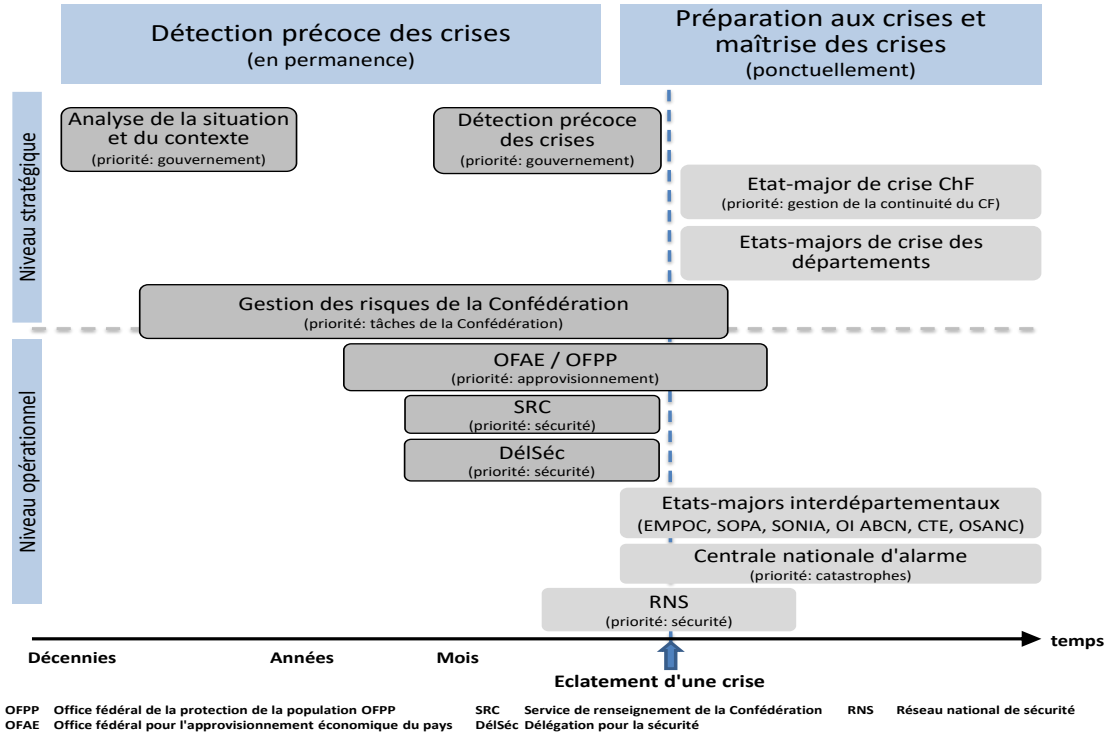


Illustration 18: Vue d'ensemble des organisations de gestion des crises

Interfaces avec la gestion des risques

Une gestion pertinente des urgences et des crises fait partie de la gestion des risques. Celle-ci veille à ce que la gestion des urgences et des crises puisse être activée rapidement.

Échanges d'informations requis

1. Échange semestriel avec les autres organes de détection précoce des crises.
2. En cas de risques pouvant avoir des conséquences majeures, la hiérarchie est sensibilisée à sa responsabilité dans la préparation de la gestion des urgences et des crises. Ces risques doivent être abordés dans le cadre de cette gestion en tant que scénarios d'exercice.
3. La détection précoce des crises permet d'alerter rapidement la gestion des urgences et des crises.
4. Les enseignements tirés de la maîtrise des urgences et des crises sont pris en compte dans la gestion des risques.

6.3 Gestion de la continuité (BCM)

Un système intégré de gestion des risques comprend la gestion de la continuité (*Business Continuity Management*, BCM). La gestion des risques examine en amont les dangers pour l'exécution des tâches et l'atteinte des objectifs et veille à ce que des mesures soient prises pour prévenir ces risques. La BCM se concentre quant à elle sur un événement et s'emploie à réduire l'*impact* d'un risque sur les prestations et processus opérationnels essentiels. Du point de vue de la gestion des risques, la BCM est donc considérée comme une mesure qui agit sur les conséquences.

La BCM est le cadre dans lequel toutes les mesures nécessaires sont prises afin que, même dans des situations extraordinaires, le Conseil fédéral et l'administration fédérale soient en mesure de s'acquitter de leurs tâches principales dans les délais. Pour chaque UA, la BCM est mise sur pied en quatre étapes[60]:

- **Étape 1 – établir une BIA:** l'analyse d'impact sur les activités (*Business Impact Analysis*, BIA) permet d'identifier les prestations et processus opérationnels dont l'interruption ou la suppression conduiraient à des dommages matériels ou immatériels considérables. La BIA comprend quatre phases: (1) répertorier les prestations et processus des UA, (2) fixer les critères visant à évaluer le caractère essentiel des prestations et processus, (3) évaluer l'ensemble des prestations et processus sur la base des critères fixés, et (4) identifier les ressources nécessaires aux prestations et processus essentiels[61].
- **Étape 2 – définir une stratégie:** la stratégie fixe le but et les principes de la mise en œuvre de la BCM. Elle définit notamment les compétences des UA dans le cadre de la BCM, les scénarios de menace, les mesures, l'établissement des rapports et la communication, la formation ainsi que l'exécution de tests.
- **Étape 3 – élaborer et appliquer les mesures:** dans le plan de continuité des activités (*Business Continuity Plan*, BCP), des mesures et des plans sont développés pour maintenir le plus longtemps possible les prestations et processus essentiels ou rétablir le plus rapidement possible le bon fonctionnement de l'UA. Il s'agit de réduire au minimum l'impact négatif d'une panne ou d'une défaillance, c'est-à-dire d'en diminuer la gravité ou la durée. Les postes de travail et l'infrastructure de substitution pour le personnel indispensable, les plans d'intervention en cas de pénurie de personnel, la garantie de l'approvisionnement en ressources essentielles (par ex. stockage, garantie contractuelle en vue d'une livraison rapide, conventions avec les fournisseurs) comp-

[60] Elles s'appuient sur les normes British Standard BS 25999 et ISO 22301.

[61] Il est possible qu'une UO ne présente pas de prestations ou processus essentiels. Dans un tel cas, les étapes 2 à 4 ne s'appliquent que partiellement.

tent parmi les principaux éléments d'un BCP. Les coûts liés au maintien de la continuité des processus opérationnels (par ex. redondances) doivent être comparés aux avantages que les mesures apportent.

- **Étape 4 – garantir la disponibilité:** pour que le BCP puisse être utilisé en cas d'incident, des *tests* sont nécessaires pour vérifier les mesures et leurs interactions. Il faut également *former* les responsables et *exercer* leur collaboration. Les tâches et les conditions-cadres d'une UA pouvant évoluer au cours du temps, l'actualité et l'efficacité de la BIA et du BCP doivent faire l'objet d'un contrôle périodique, ces derniers devant être *mis à jour* le cas échéant.

Les fonctions et responsabilités du BCM au sein de l'administration fédérale sont définies dans la *directive sur la gestion de la continuité de l'activité* qui a été adoptée par la CSG au printemps 2017[62] et sert de norme pour les directives des différents départements et de la ChF. Selon cette directive, la *direction d'une UA* est responsable du développement et du contrôle régulier de la BCM. Comme dans l'organisation de la gestion des risques de la Confédération, des délégués à la BCM sont nommés dans les départements et les UA. Le service de coordination Gestion des risques de la Confédération est chargé de coordonner la BCM de manière centralisée, de promouvoir la mise en œuvre de la BCM dans l'administration fédérale et de remettre une fois par année à la CSG, dans le cadre du rapport sur les risques, un compte rendu de l'état de la mise en œuvre de la BCM.

Interfaces avec la gestion des risques

La BCM établit les mesures et les plans permettant de gérer les conséquences de risques spécifiques. L'existence et l'efficacité de ce dispositif doivent être décrits brièvement dans les feuilles sur les risques correspondantes.

Échange d'informations requis

Si les départements et la ChF mettent sur pied leur BCM au sein de l'organisation de la Confédération en matière de gestion des risques, aucun échange d'information n'est spécialement requis. Si ce n'est pas le cas, un échange est nécessaire entre les responsables de la gestion des risques des départements et des UA, notamment au cours de la préparation du rapport sur les risques. Les responsables des risques des UA s'assurent que les mesures liées à la BCM soient correctement saisies et actualisées dans le système informatisé de gestion des risques (R2C_GRC).

6.4 Analyse de la situation et du contexte

Selon l'art. 32, let. c^{ter}, de la loi sur l'organisation du gouvernement et de l'administration, la ChF veille à ce qu'une analyse continue et à long terme de la situation et du contexte soit établie et en rend régulièrement compte au Conseil fédéral. Après avoir supprimé l'état-major de prospective[63], le Conseil fédéral a fixé la procédure suivante:

Premièrement, un rapport dresse tous les quatre ans un état des lieux des principaux thèmes et tendances qui pourraient influencer et marquer la Suisse dans les dix à quinze années qui suivent. Le recours à des experts issus des milieux scientifique, économique, culturel, politique et administratif permettra de déterminer les défis à venir et les perspectives. Ce rapport sera présenté pour la première fois fin 2018 au Conseil fédéral, qui s'en servira pour définir les priorités politiques (programme de la législature).

Deuxièmement, en complément à ce rapport, la ChF procèdera à partir de 2017 à une analyse des sources d'information internes et externes. Elle communiquera au Conseil fédéral à un rythme semestriel les nouveaux développements, événements et tendances qui, selon leur importance, devront être pris en compte dans les objectifs annuels du Conseil fédéral.

[62] Séances de la CSG du 24 février et 31 mars 2017

[63] Voir l'arrêté fédéral du Conseil fédéral du 7 septembre 2017

Par rapport à la gestion des risques, l'analyse de la situation et du contexte se concentre surtout sur des sujets de stratégie politique qui sont directement liés à l'activité gouvernementale et sur les défis à moyen et long terme (voir l'ill. 17). Identifiés par l'analyse de la situation et du contexte, ces derniers peuvent, au fil du temps, constituer des risques concrets pour les tâches de la Confédération, voire engendrer des crises. Un échange d'informations entre cet état-major et la gestion des risques de la Confédération est donc indispensable.

Interfaces avec la gestion des risques

Au moment de leur identification, les défis recensés dans le cadre de l'analyse régulière et à long terme de la situation et du contexte constituent des dangers encore abstraits du point de vue de la gestion des risques. Au fil du temps, ils peuvent générer des risques concrets devant figurer dans le rapport sur les risques de l'administration fédérale.

Échange d'information requis

L'échange d'informations est assuré par la ChF, qui intègre le service de coordination Gestion des risques lorsque cela est nécessaire et informe ce dernier sur les résultats de ses analyses.

6.5 Présentation des comptes (engagements conditionnels)

Les *engagements conditionnels* constituent une interface entre la gestion des risques et la présentation des comptes. Des normes strictes concernant la présentation des comptes (par ex. IFRS, IPSAS[64]) exigent des entreprises privées et des collectivités publiques qu'elles publient leurs engagements conditionnels dans le cadre de leurs comptes annuels[65]. Un engagement conditionnel est une obligation résultant d'un événement passé qui, à l'avenir et dans certaines conditions, peut engendrer une sortie de fonds. La probabilité de cet événement est de moins de 50 %. On peut distinguer deux cas.

a) **Cas 1:** une obligation légale ou factuelle *existe*. On ne peut exclure une sortie de fonds découlant de cette obligation, mais elle est réputée peu probable à la date de la saisie (la probabilité estimée de la sortie de fonds est inférieure à 50 %)[66]. Il peut par exemple s'agir de cautionnements ou de garanties.

b) **Cas 2:** une obligation pourra *éventuellement* exister à l'avenir. L'événement a déjà eu lieu, mais l'entreprise ou la collectivité publique ne peut pas décider s'il va en découler ou non une obligation. Sa probabilité est inférieure à 50 %, et/ou la sortie de fond ne peut pas être estimée précisément. Il peut s'agir de procédures juridiques en cours ou d'un besoin d'assainissement latent dans un portefeuille immobilier, par exemple en raison de sols contaminés ou de danger lié à l'amiante.

La publication des engagements conditionnels permet d'informer en toute transparence les groupes concernés et les milieux intéressés (investisseurs, créanciers ou contribuables) sur les charges auxquelles l'entreprise ou la collectivité publique devront peut-être faire face à l'avenir.

La Confédération subdivise les engagements conditionnels en quatre groupes[67]:

- *cautionnements et garanties* (par ex. les cautionnements en faveur d'organisations œuvrant dans la construction de logements d'utilité publique);

[64] International Financial Reporting Standards; International Public Sector Accounting Standards

[65] La Confédération présente ses engagements conditionnels conformément à la norme IPSAS 19, voir le compte d'État 2016, tome 1, chiffre 63, p. 120 s. Le principe correspondant en matière de présentation des comptes figure dans le manuel de gestion budgétaire et de tenue des comptes de la Confédération (chap. 10.2; https://intranet.accounting.admin.ch/accounting/fr/home/404.html).

[66] Si la sortie de fonds est considérée comme probable (supérieure à 50 %), une *provision* doit être comptabilisée dans le bilan.

[67] En 2016, la Confédération présentait des engagements conditionnels pour quelque 23 milliards de francs au total (sans les engagements en matière de prévoyance et les prestations en faveur de l'employé), dont plus de 90 % provenant de cautionnements et garanties (voir le compte d'État 2016, tome 1, chap. 63, p. 120).

- *engagements de capital* en faveur des banques de développement (capitaux de garantie qui n'ont pas été versés, mais pour lesquels la Confédération s'est fermement engagée);
- *procédures judiciaires* (litiges judiciaires en cours, dont l'issue pourrait avoir des conséquences financières pour la Confédération);
- *autres* engagements conditionnels (par ex. l'assainissement d'immeubles).

Les engagements conditionnels ont en commun avec les risques le fait qu'ils peuvent, avec une certaine probabilité, avoir des conséquences financières négatives pour la Confédération. Mais leur contrôle sert à des fins diverses: tandis que l'état des engagements conditionnels, en tant qu'élément de la *présentation des comptes*, contribue à donner une image juste de la situation patrimoniale d'une entreprise ou d'une collectivité, la *gestion des risques* vise à contrôler les risques de façon systématique et, partant, à améliorer le pilotage des tâches d'une UO. La présentation des comptes et la gestion des risques s'adressent donc à des *groupes distincts de destinataires* poursuivant des *intérêts différents* (d'une part, les investisseurs ou, plus exactement, le Parlement et les contribuables et, de l'autre, les responsables de la conduite). En raison de ces différences, une reproduction à l'identique dans les deux systèmes serait non seulement redondante mais encore objectivement erronée[68]. Aussi convient-il de décider au cas par cas des situations dans lesquelles il y a lieu d'opter pour un engagement conditionnel à la gestion des risques[69].

Il est notamment indiqué de présenter un engagement conditionnel comme un risque si cela est utile au pilotage des tâches d'une UO, concrètement lorsque

- l'accomplissement des tâches et la réalisation des objectifs de cette UO sont menacés (risque),
- la probabilité et les conséquences du risque sont jugées importantes (importance) et que
- le risque peut être contrôlé, c'est-à-dire que des mesures adéquates peuvent être prises pour réduire la probabilité du risque ou venir à bout de ses conséquences (possibilité de le piloter).

Interfaces avec la gestion des risques

Dans certaines conditions, un engagement conditionnel peut constituer un risque (influence négative sur les tâches et les buts, importance, pilotage).

Échange d'information requis

Les responsables des risques des départements et des UA connaissent les engagements conditionnels de leur(s) UA et décident avec la hiérarchie compétente si l'engagement conditionnel doit être géré comme risque selon les principes décrits plus haut.

[68] Le cas inverse, à savoir quand un risque pourrait constituer un engagement conditionnel, est en général sans importance dans la pratique car la présentation des comptes obéit à des critères nettement plus rigoureux pour l'enregistrement d'engagements conditionnels.

[69] Les délimitations entre engagements conditionnels et risques s'appliquent surtout à ce qu'il est convenu d'appeler des provisions. Les provisions sont constituées et comptabilisées au bilan lorsqu'une sortie de fonds aisément quantifiable apparaît comme très probable (à plus de 50 %) au vu d'une situation concrète. Un enregistrement et un pilotage dans le cadre de la gestion des risques ne sont plus indiqués du fait de cette réalisation probable.

6.6 Gouvernement d'entreprise[70]

Certaines tâches fédérales sont exécutées par des entités devenues autonomes sur le plan juridique, organisationnel et financier, mais qui appartiennent intégralement ou en partie à la Confédération et que cette dernière contrôle (entreprises et établissements de la Confédération). Pour pouvoir assumer son rôle de propriétaire et de garant de l'exécution des tâches[71] vis-à-vis de ces entités, le Conseil fédéral fixe des objectifs stratégiques[72] qui font partie intégrante du gouvernement d'entreprise de la Confédération[73] et portent généralement sur une période de quatre ans.

Dans le cadre de ces objectifs stratégiques, une obligation spécifique contraint l'organe de direction suprême (conseil d'administration) à mettre en place une gestion des risques (*Enterprise Risk Management*, ERM) et de la conformité (CMS) et à l'exploiter efficacement. Elle est formulée comme suit de manière standard:

> Objectif XY: «<L'entreprise> dispose d'un système de gestion des risques (ERM) basé sur la norme ISO 31000 et d'un système de gestion de la conformité (CMS) basé sur la norme ISO 37301. Elle informe le propriétaire des principaux risques d'entreprise et des priorités du CMS.»[74]

Le Conseil fédéral évalue la réalisation des objectifs grâce à un audit qui (1) doit être exécuté une fois par période stratégique par une société d'audit externecompétente en la matière, (2) est mandaté par l'organe de direction suprême de l'entreprise, et (3) fait l'objet d'un rapport que cet organe transmet au Conseil fédéral. Les principaux éléments de l'exécution de l'audit, à savoir l'étendue de celui-ci, ses objectifs et ses critères, sont consignés par le propriétaire dans un «document de référence» à l'intention de l'organe de direction suprême. Les objectifs majeurs de l'audit englobent notamment la confirmation que la gestion des risques et de la conformité est implémentée de manière adéquate, conformément à la norme appliquée (*design effectiveness*), et une évaluation du bon fonctionnement de ces systèmes dans la pratique (*operating effectiveness*). L'état et la mise en œuvre de l'ERM et du CMS ainsi que les questions d'actualité correspondantes sont abordés lors des entretiens avec le propriétaire réunissant les départements compétents/l'AFF et la direction de l'entreprise, en général dès le premier entretien de l'année.

Si la Confédération assume des responsabilités, des garanties, des cautionnements et des engagements conditionnels spécifiques envers certaines entités devenues autonomes, elle doit définir des exigences strictes quant à la gestion des risques (par ex. prescriptions pour prévenir ou réduire les risques existants, obligation d'assurance, constitution de réserves) et surveiller leur respect de manière régulière[75].

La gestion des risques de la Confédération se tient à la disposition des entreprises et établissements de la Confédération pour toute question méthodologique ou interrogation sur la gestion des risques et de la conformité. Un échange d'expériences régulier contribue à l'amélioration de ces systèmes de gestion tant dans les entreprises de la Confédération que dans l'administration fédérale.

---

[70] Concernant le gouvernement d'entreprise de la Confédération: voir le rapport du Conseil fédéral du 13 septembre 2006 sur l'externalisation et la gestion de tâches de la Confédération (rapport sur le gouvernement d'entreprise, FF **2006** 7799); le rapport du Conseil fédéral du 25 mars 2009 complétant le rapport sur le gouvernement d'entreprise – Mise en œuvre des résultats des délibérations au sein du Conseil national (rapport complémentaire, FF **2009** 2299) et le rapport explicatif de l'Administration fédérale des finances du 13 septembre 2006 concernant le rapport du Conseil fédéral sur le gouvernement d'entreprise (rapport explicatif de l'AFF sur le gouvernement d'entreprise); rapport du Conseil fédéral du 26 mai 2021 en réponse au postulat Abate 18.4274 (la stratégie du propriétaire pour les entités de la Confédération devenues autonomes).

[71] Rapport complémentaire, ch. 6.2, principe n° 16

[72] Art. 8, al. 5, LOGA

[73] Concernant la définition: rapport explicatif de l'AFF sur le gouvernement d'entreprise, ch. II/2

[74] Cette formulation souple («…basé…») accorde une certaine marge de manœuvre pour cet objectif, de sorte que d'autres normes internationalement reconnues, notamment la norme américaine COSO (Committee of Sponsoring Organizations of the Treadway Commission), peuvent être appliquées. Conformément à l'approche «appliquer ou expliquer», ces exceptions doivent être justifiées.

[75] Rapport sur le gouvernement d'entreprise, fin du ch. 4.2.4, principe n° 12; rapport explicatif de l'AFF sur le gouvernement d'entreprise, ch. I/5.4. Le cas échéant, cette vérification détaillée peut être réalisée par l'organe de révision dans le cadre d'un mandat correspondant.

Interfaces avec la gestion des risques

Sur le plan organisationnel, il n'existe aucune interface entre la gestion des risques de la Confédération et les systèmes de gestion des entreprises et établissements de la Confédération. Les compétences et les responsabilités sont clairement distinctes. Le contenu peut néanmoins se recouper:

- Si la Confédération assume des responsabilités, des garanties et des cautionnements spécifiques (par ex. en relation avec sa responsabilité subsidiaire en vertu de l'art. 19 LRCF) envers des entités devenues autonomes, ils relèvent clairement de sa gestion des risques.
- Même en l'absence de responsabilités, de garanties et de cautionnements spécifiques de la Confédération, celle-ci peut être contrainte, au cas par cas, de renforcer la capacité des entités devenues autonomes à supporter le risque (par ex. recapitalisation) si leur situation en la matière change.
- Eu égard à son rôle de propriétaire et de garant de l'exécution des tâches ainsi qu'aux tâches de pilotage et de contrôle qui en découlent, le Conseil fédéral demeure au final entièrement responsable, sur le plan politique, de la performance économique et de l'exécution des tâches confiées et assume les risques correspondants du propriétaire, même après qu'une entreprise soit devenue autonome[76].

Échange d'informations requis

Un échange sur les éléments suivants est judicieux:

- méthodologie concernant la gestion des risques et de la conformité (au niveau technique);
- état de la mise en œuvre en vue de la réalisation des objectifs ERM et CMS, et risques de la Confédération qui découlent directement de son rôle de propriétaire et de garant de l'exécution des tâches et de la responsabilité politique globale du Conseil fédéral (entretiens avec le propriétaire).

6.7 Gestion des assurances

La Confédération, qui applique le principe de l'auto-assurance, assume le risque pour les dommages causés à son patrimoine et supporte les conséquences de son activité[77]. Un risque peut exceptionnellement être géré en souscrivant un contrat d'assurance ou un contrat de règlement des sinistres avec un tiers, en particulier lorsque son potentiel de dommage est élevé, lorsque les connaissances dans l'administration fédérale sont insuffisantes pour régler les sinistres ou lorsqu'un transfert du risque est rentable[78]. Lors de la conclusion d'assurances, il faut veiller à ce que les conditions contractuelles présentent un rapport optimal entre le prix et les prestations et à ce qu'elles respectent les conditions du marché. Dans l'administration fédérale, le service de coordination de la gestion des risques (AFF) assure également la gestion centralisée des assurances. La mesure visant à réduire les risques en les transférant lui incombe donc. En outre, les demandes de conclusion de contrats d'assurance déposées par les UO fournissent au service de coordination des indications utiles sur l'expositions aux risques au sein de l'administration fédérale.

Interfaces avec la gestion des risques

Le service de coordination de la gestion des risques (AFF) assure également la gestion centralisée des assurances.

[76] Art. 8, al. 4, LOGA
[77] Art. 50, al. 2, OFC
[78] Voir les directives de l'AFF du 11 septembre 2015 applicables à la prise en charge des risques et au règlement des sinistres à la Confédération, ch. 1.2

6.8 Centre national pour la cybersécurité (NCSC)

Le Centre national pour la cybersécurité (NCSC) est le centre de compétences en matière de cybermenaces en Suisse. Chargé de la cybersécurité de la Confédération, il élabore des directives en matière de sécurité informatique, conseille les unités administratives lors de leur application et vérifie le niveau de sécurité informatique au sein des départements et de la ChF.

Le NCSC veille à coordonner la gestion des cyberrisques à l'échelle de la Confédération. Dans ce cadre, il gère le cyberrisque stratégique de cette dernière en tenant compte des enseignements tirés des cyberrisques individuels gérés par les différents prestataires informatiques . En outre, le NCSC prend en considération les mesures définies dans la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC).

Le délégué à la cybersécurité (directeur du NCSC) est le propriétaire du cyberrisque stratégique. En tant que tel, il est chargé de présenter les principales cybermenaces au Groupe Cyber[79], où elles sont traitées sur le plan stratégique, tous départements confondus. Il veille également à la visibilité des activités de la Confédération en matière de cyberrisques.

Cybersécurité de la Confédération

Les exigences requises en matière de cybersécurité pour assurer une protection adéquate de la confidentialité, de la disponibilité, de l'intégrité et de la traçabilité des objets à protéger relevant de l'informatique de l'administration fédérale sont énoncées dans l'ordonnance sur la protection contre les cyberrisques dans l'administration fédérale (ordonnance sur les cyberrisques, OPCy)[80] et dans les prescriptions correspondantes du NCSC sur le processus de sécurité. Les mesures de sécurité s'appuient sur les normes ISO en vigueur concernant les processus de sécurité informatique. La mise en œuvre opérationnelle de ces exigences incombe aux différentes UA. Les risques inhérents aux projets et à l'exploitation informatiques sont identifiés, évalués et réduits ou éliminés grâce à des mesures appropriées, dans le cadre du processus de sécurité. La direction de l'UA doit être informée des risques résiduels et en tenir compte. Dans le cadre d'une enquête structurée, les délégués à la sécurité informatique des départements (DSID) et de la ChF indiquent quel y est l'état de la sécurité informatique. Leurs indications sont vérifiées par le NCSC, qui rédige ensuite à l'attention du Conseil fédéral un rapport annuel sur l'état de la sécurité informatique dans l'administration fédérale. Il faut veiller à ce que les principaux risques figurant dans ce rapport soient analysés dans le cadre de la gestion des risques.

Interfaces avec la gestion des risques

Les écarts par rapport aux directives en matière de sécurité informatique peuvent mettre en péril l'exécution des tâches ou l'atteinte des objectifs de l'administration fédérale. Le rapport régulier du NCSC sur l'état de la sécurité informatique dans l'administration fédérale peut comporter des informations précieuses pour la gestion des risques de la Confédération. À l'inverse, il arrive aussi que les rapports sur les risques permettent de compléter le rapport du NCSC.

Échange d'informations requis

Rapprochement régulier entre le service de coordination Gestion des risques de la Confédération, le responsable de la gestion des risques du département et le conseiller en gestion des risques du NCSC (état de la sécurité informatique dans l'administration fédérale), information mutuelle sur des incidents particuliers, garantie d'un transfert de savoir et traitement interdépartemental des principaux cyberrisques par le Groupe Cyber.

[79] Sont représentés dans le Groupe Cyber le NCSC (présidence), fedpol, le SRC et le SG-DDPS.

[80] RS **120.73** – Ordonnance du 27 mai 2020 sur la protection contre les cyberrisques dans l'administration fédérale (ordonnance sur les cyberrisques, OPCy) (admin.ch)

6.9 Transformation numérique et gouvernance de l'informatique (TNI)

En tant que centre de compétence pour les questions de numérisation, le Secteur Transformation numérique et gouvernance de l'informatique (TNI) de la ChF donne des instructions, lance ses propres projets ou soutient ceux des départements et des offices. Il assure une vue d'ensemble supradépartementale sur les projets, les ressources et les prestations administratives de la transformation numérique et de l'informatique dans l'administration fédérale.

Projets TNI clés de l'administration fédérale

Les projets TNI clés de l'administration fédérale sont des projets ou programmes informatiques qui requièrent une conduite, un pilotage, une coordination et un contrôle renforcés en raison des ressources qu'ils mobilisent, de leur importance stratégique, de leur complexité et de leurs répercussions ou de leurs risques. Les tâches et les responsabilités en relation avec les projets informatiques clés sont réglementées dans les directives du Conseil fédéral du 16 mars 2018 concernant les projets informatiques de l'administration fédérale et le portefeuille informatique de la Confédération[81]. C'est le chancelier de la Confédération qui a compétence pour définir les projets clés, après consultation de la CSG.

Les responsables des projets clés remettent semestriellement au secteur TNI un rapport sur l'avancement de ces derniers, qui comprend des informations pertinentes pour la haute surveillance. Le secteur TNI établit sur cette base un rapport consolidé sur l'état d'avancement de l'ensemble des projets clés, lequel est transmis à la CSG pour qu'elle en prenne acte, puis aux Commissions de gestion et à la Délégation des finances des Chambres fédérales. Le secteur TNI peut proposer des mesures. Après consultation de la CSG, le chancelier de la Confédération décide s'il soumet ces mesures au Conseil fédéral pour décision.

Conformément au ch. 4.4 des directives du Conseil fédéral du 16 mars 2018 concernant les projets informatiques de l'administration fédérale et le portefeuille informatique de la Confédération, l'UA compétente identifie, analyse et évalue les risques de ses projets clés selon les prescriptions de la Gestion des risques de la Confédération. Elle annonce et surveille les risques pouvant avoir des conséquences négatives majeures sur l'atteinte des objectifs et l'exécution des tâches de l'administration fédérale. On s'assure ainsi que les problèmes graves liés à ces projets soient également traités du point de vue de la Gestion des risques de la Confédération, le service de coordination Gestion des risques de la Confédération, qui est rattaché à l'AFF, signalant aussi rapidement que possible aux responsables de la gestion des risques des départements concernés tous les projets «critiques» qui figurent dans le rapport du secteur TNI sur le contrôle de gestion. Ces responsables vérifient si les projets en question sont recensés en tant que risques, analysés correctement et comment ils doivent être évalués. Ils informent ensuite le service de coordination Gestion des risques de la Confédération de l'état des projets du point de vue de la gestion des risques de la Confédération.

Interfaces avec la gestion des risques

Les problèmes liés aux grands projets informatiques et de numérisation peuvent mettre en péril l'exécution des tâches ou l'atteinte des objectifs de l'administration fédérale. Le rapport semestriel sur l'avancement des projets TNI clés peut comporter des informations précieuses pour la gestion des risques de la Confédération, car il se concentre sur les projets informatiques qui sont les plus vastes et potentiellement les plus risqués. À l'inverse, il est possible que les rapports sur les risques mettent en évidence des lacunes dans ce rapport du secteur TNI.

[81] Directives du Conseil fédéral concernant les projets informatiques de l'administration fédérale et le portefeuille informatique de la Confédération

Échange d'informations requis

Rapprochement régulier entre le service de coordination Gestion des risques de la Confédération, les responsables de la gestion des risques des départements concernés et les rapports TNI (rapport sur l'avancement des projets TNI clés de l'administration fédérale), information mutuelle sur des incidents particuliers, garantie d'un transfert de savoir.

6.10 Contrôle fédéral des finances (CDF)

Le Contrôle fédéral des finances (CDF) est l'organe suprême de la Confédération en matière de surveillance financière. Il assiste le Parlement et le Conseil fédéral, est indépendant et n'est assujetti qu'à la Constitution et à la loi. Son domaine des tâches est défini dans la loi sur le Contrôle des finances. Le CDF examine la gestion financière de l'administration fédérale et de nombreuses organisations semi-étatiques et internationales. Il mène ses audits selon les critères de la rentabilité, de l'efficacité, de la régularité et de la légalité.

Dans leur rapport concernant le projet informatique INSIEME, les Commissions des finances et les Commissions de gestion ont recommandé au Conseil fédéral d'intégrer de manière appropriée le rapport annuel du CDF sur les importantes révisions en suspens, c'est-à-dire toutes les recommandations majeures qui sont encore en suspens, dans le rapport sur les risques de la Confédération et dans son rapport annuel aux CdG. Dans son avis[82], le Conseil fédéral reconnaît que les comptes rendus annuels du CDF au sujet des recommandations pendantes peuvent révéler des lacunes dans l'accomplissement des tâches ou l'atteinte des objectifs par l'administration fédérale. Il a donc accepté la recommandation des Commissions, qui sera mise en œuvre à partir de 2015.

Dans le cadre du processus de gestion des risques, chaque UA ou chaque département est responsable de la prise en compte des (principales) révisions en suspens dans la gestion des risques (processus normal). Celles-ci seront discutées une fois par an entre le CDF et le service de coordination Gestion des risques de la Confédération, en tant qu'outil supplémentaire du contrôle de gestion. Les résultats de cet entretien seront ensuite communiqués aux UA ou aux départements correspondants par l'intermédiaire de questions formulées par l'AFF. On garantit ainsi une optimisation des échanges tant lors du processus ordinaire qu'à travers les questions du service de coordination Gestion des risques de la Confédération.

Interfaces avec la gestion des risques

Les révisions en suspens du CDF peuvent révéler des lacunes dans l'accomplissement des tâches ou l'atteinte des objectifs des UA et des départements. Elles doivent donc être prises en compte dans le cadre du processus de gestion des risques.

Échange d'informations requis

Rapprochement avec le rapport annuel du CDF sur les principales révisions en suspens (celles indiquées comme «priorité A»).

6.11 Autres interfaces

D'autres projets de l'administration fédérale portent également sur des thèmes particuliers de la gestion des risques. L'échange d'informations et la délimitation sont exposés à l'annexe 8, qui est mise à jour régulièrement.

[82] Voir FF **2015** 6193

7 Amélioration de la gestion des risques de la Confédération

La gestion des risques au sein de l'administration fédérale est régulièrement développée et améliorée[83]. Les responsables de la gestion des risques des départements et des UA ainsi que le service de coordination de l'AFF utilisent les enseignements issus de leur activité de gestion des risques au sein de l'administration fédérale pour proposer des améliorations en la matière et, le cas échéant, les mettre en œuvre. Au niveau du Conseil fédéral, le service de coordination de l'AFF est chargé de décider des mesures d'amélioration de la gestion des risques et de les appliquer. Des informations externes à l'administration fédérale (par ex. manifestations sur la gestion des risques) contribuent également à identifier le potentiel d'amélioration de la gestion des risques de la Confédération. Les directives et le présent manuel seront adaptés régulièrement en cas de besoin.

7.1 Évaluation des prestations

Pour pouvoir améliorer la gestion des risques dans l'administration fédérale, il faut évaluer régulièrement ses prestations. À cet égard, il convient de distinguer deux dimensions: l'amélioration du contenu, c'est-à-dire la modification du profil de risque (ensemble des risques) de l'administration fédérale, et l'amélioration organisationnelle, c'est-à-dire l'instauration et la mise en œuvre d'un système efficace de gestion des risques.

L'amélioration *du contenu* vise à déterminer dans quelle mesure un risque individuel ou le potentiel d'un risque agrégé a pu être réduit dans l'administration fédérale. Celle-ci renonçant à une agrégation quantitative, la gestion des risques de la Confédération se concentre sur les principaux risques individuels et sur leur degré de réduction. Les rapports présentent les modifications des risques au niveau de la Confédération, des départements / de la ChF et des UA.

L'amélioration *organisationnelle* vise à vérifier dans quelle mesure un système efficace de gestion des risques a été réalisé et s'il est mis en œuvre dans la pratique. Cet examen s'effectue généralement par l'intermédiaire d'un audit. De plus, on contrôle régulièrement si les structures générales et les particularités d'une organisation affectent l'efficacité du processus de gestion des risques et peuvent favoriser le développement progressif de risques (voir l'annexe 9).

7.2 Audit

L'exécution d'un audit constitue une mesure importante en vue de la consolidation et de l'amélioration du système de gestion des risques. Les organes de contrôle qui entrent en considération sont en principe les services internes ou externes de révision. En fonction des ressources, on peut aussi recourir à un prestataire externe spécialisé dans les audits. L'audit du système de gestion des risques portera principalement – comme une évaluation du degré de maturité du système – sur les questions suivantes:

- La haute direction s'engage-t-elle à mettre en œuvre la gestion des risques?
- La gestion des risques englobe-t-elle tous les domaines de l'administration fédérale?
- Existe-t-il une politique de gestion des risques qui est approuvée par la direction?
- Les propriétaires des risques et les responsables de la gestion des risques des départements et des UA ont-ils été nommés et exécutent-ils leurs tâches?
- Existe-t-il une communication interne et externe appropriée sur les risques?

[83] Ch. 4, al. 8, des directives du CF sur la politique de gestion des risques

- Les responsables de la gestion des risques des départements et des UA ont-ils les capacités, la formation et l'expérience requises?
- Les principaux processus de l'administration fédérale intègrent-ils la gestion des risques?
- Les méthodes utilisées conviennent-elles aux champs d'application?
- Les évaluations des risques sont-elles documentées et validées par les propriétaires des risques?
- Les mesures de maîtrise du risque sont-elles mises en œuvre et leur efficacité est-elle vérifiée?
- Un service indépendant évalue-t-il régulièrement l'efficacité de la gestion des risques (y c. l'exécution des tâches par le service de coordination de l'AFF)?
- Le système de gestion des risques est-il bien documenté? Les documents sont-ils faciles à trouver et à jour?

7.3 Certification

L'ISO 31000:2018 est une directive (*guideline*), et non une norme pouvant déboucher sur une certification.

Annexe 1: Définitions (glossaire)

La présente annexe définit par ordre alphabétique les termes utilisés dans le cadre de la gestion des risques de la Confédération. Concernant les fonctions et les responsabilités en la matière, il est renvoyé au ch. 2.2. Ces termes sont employés de manière uniforme dans la gestion des risques de la Confédération, ce qui améliore la communication et favorise la compréhension commune. Les définitions ci-après s'appuient, en général, sur les normes en vigueur, qui en comprennent d'autres auxquelles cette annexe peut également faire référence.

Acceptation du risque: décision de prendre en charge un risque déterminé (voir aussi → *tolérance au risque*).

Administration fédérale: subordonnée au Conseil fédéral, elle se compose des départements et de la ChF. Les départements sont organisés en offices, qui peuvent être réunis en groupements. Ils disposent chacun d'un secrétariat général. À teneur des dispositions régissant son organisation, l'administration fédérale comprend en outre des unités administratives décentralisées[84].

Agrégation (quantitative) des risques[85]***:*** procédure qui détermine et met en évidence les interactions de plusieurs risques individuels dépendant éventuellement les uns des autres pour former un risque global (*value at risk*).

Agrégation des risques: procédure qui regroupe plusieurs risques à un niveau supérieur. Le compte rendu et, dans une certaine mesure, la gestion du risque agrégé (mesures transversales) sont également réalisés au niveau supérieur. *Exemple:* une panne informatique à l'AFF et une autre à l'AFC peuvent être agrégées si ces deux risques ont la même cause (par ex. panne de courant dans les bâtiments où les deux systèmes sont exploités).

Appréciation du risque: processus comparant les résultats de l'évaluation du risque avec la tolérance au risque pour déterminer si le niveau de risque est acceptable ou tolérable (divergence par rapport à la norme ÖNORM 4900).

Approche ascendante: méthode d'appréciation des risques dans laquelle tous les éléments du niveau hiérarchique le plus bas d'une organisation font l'objet d'une identification et d'une analyse des risques. Ceux-ci sont ensuite notifiés en remontant la ligne hiérarchique, où ils sont consolidés.

Approche descendante: méthode d'appréciation des risques dans laquelle l'ensemble de l'organisation ou du système fait l'objet d'une identification et d'une analyse des risques.

Brainstorming: méthode consistant à collecter, à évaluer et à classer de nombreuses idées dans le cadre d'un groupe. Les idées sont collectées sans la moindre restriction; toute critique est interdite. L'évaluation et le classement visent à trier les idées qui sont éloignées du problème et à regrouper celles qui sont liées thématiquement.

Catégorie de risque: subdivision des risques en groupes thématiques.

Communication sur les risques: processus durable ou récurrent pour échanger des informations sur la gestion des risques avec les parties intéressées.

Conséquence: impact d'un événement ou d'une évolution qui affecte les objectifs ou l'exécution des tâches de l'administration fédérale (divergence par rapport à la norme ÖNORM 4900). Les dimensions d'une conséquence sont expliquées en détail au ch. 3.3.4.

[84] Art. 2 LOGA

[85] Par ex. au moyen d'une simulation Monte-Carlo

Consolidation des risques: procédure qui agrège, regroupe ou sélectionne en fonction de leur type ou de leur importance plusieurs risques individuels identifiés séparément.

Crise: situation qui requiert des mesures extraordinaires à l'échelle de l'organisation. Contrairement à une urgence, une crise se réfère à une organisation: celle-ci (ou un système / une institution) est confrontée à une crise lorsque sa réputation (crédibilité, confiance), sa marge de manœuvre ou son existence sont menacées.

Culture du risque: climat professionnel dans lequel tous les collaborateurs et les cadres ont conscience des risques et entretiennent une culture positive de l'erreur.

Danger: source de risque potentielle qui peut entraîner un dommage soudain.

Spécialistes de la gestion des risques: terme collectif désignant les responsables de la gestion des risques des UA et les responsables de la gestion des risques des départements.

Détection précoce d'une crise: examen des événements et des tendances qui sont déjà visibles et qui sont généralement susceptibles de se transformer en crise dans un laps de temps allant de quelques mois à un an et demi au plus.

Directives sur la gestion des risques: prescriptions obligatoires de l'AFF sur la mise en œuvre et l'amélioration constante de la gestion des risques dans l'administration fédérale.

Évaluation du risque: recherche et exploitation systématiques d'informations pour comprendre un risque ainsi que pour estimer sa probabilité et ses conséquences pour l'administration fédérale (divergence par rapport à la norme ÖNORM 4900).

Événement: concrétisation soudaine d'un ensemble précis de circonstances.

Évolution: modification progressive des circonstances.

Gestion de la continuité (Business Continuity Management, BCM): prise de toutes les mesures nécessaires pour que l'administration fédérale et le Conseil fédéral puissent exécuter à temps leurs tâches principales, même dans des situations exceptionnelles (divergence par rapport à la norme ÖNORM 4900).

Identification du risque: processus consistant à rechercher des risques et à les décrire à l'aide de leurs causes et de leurs conséquences.

Incertitude: absence d'informations sur la concrétisation d'événements ou d'évolutions futurs, sur leurs conséquences et sur leur probabilité.

Interactions: interdépendances ou influences mutuelles entre plusieurs risques.

Maîtrise du risque: sélection et mise en œuvre de mesures pour prévenir ou atténuer un risque. La gestion des urgences, des crises et de la continuité font également partie intégrante de la maîtrise du risque.

Matrice des risques: représentation graphique des risques en fonction de leurs conséquences et de leur probabilité.

Menace: source de risque potentielle qui peut engendrer une évolution défavorable.

Niveau de risque: ampleur estimée ou mesurée d'un risque qui tient compte des conséquences et de la probabilité.

Politique de gestion des risques: intentions et objectifs du Conseil fédéral concernant la gestion des risques. Cette politique a été édictée par le Conseil fédéral sous la forme de directives contraignantes.

Probabilité: fréquence relative de la concrétisation des événements ou évolutions futurs (définition objective). Incertitude des déclarations ou du degré de conviction personnelle concernant l'apparition d'un événement ou une évolution (compréhension subjective). La probabilité d'un risque peut se rapporter à une période (par ex. probabilité annuelle) ou à un nombre de cas (probabilité ponctuelle).

Processus de gestion des risques: application systématique de principes, de procédures et d'activités pour communiquer sur les risques, échanger des informations, créer des liens et pour identifier, analyser, apprécier, maîtriser et surveiller les risques.

Propriétaire du risque: personne ayant la compétence décisionnelle et la responsabilité de gérer le risque. Si cette exigence est remplie, cette personne peut se situer à tous les niveaux hiérarchiques (des cadres) de l'administration fédérale.

Réduction du risque: décision relative aux mesures et à leur mise en œuvre pour influer favorablement sur la probabilité ou les conséquences d'un risque.

Responsable de la gestion des risques de l'UA: personne qui applique le processus de gestion des risques au niveau d'une UA et est chargée d'y intégrer la gestion des risques.

Responsable de la gestion des risques du département: personne qui applique le processus de gestion des risques au niveau d'un département / de la ChF et est chargée d'y intégrer la gestion des risques.

Responsable des mesures: personne chargée de la mise en œuvre concrète d'une mesure de réduction d'un risque, sur la base d'un mandat correspondant du propriétaire du risque.

Risque: événements et évolutions qui ont une certaine probabilité de se produire et qui ont des conséquences négatives majeures d'ordre financier et non financier sur l'atteinte des objectifs et l'exécution des tâches dans l'administration fédérale (divergence par rapport à la norme ÖNORM 4900)[86].

Risque accepté: risque qui ne peut (plus) être réduit, par exemple, pour des raisons techniques, pratiques ou économiques et qui est dès lors pris en charge.

Risque inconnu: risque d'une organisation qui reste inconnu malgré une identification adéquate des risques et qui ne peut donc pas être géré.

Risque initial: risque individuel agrégé avec d'autres risques à un niveau supérieur pour former un risque transversal.

Risque net: part résiduelle d'un risque après la mise en œuvre de mesures de maîtrise du risque.

Risque résiduel[87]***:*** la gestion des risques de la Confédération utilise des termes plus précis pour les trois cas d'application usuels (divergence par rapport à la norme ÖNORM 4900): -> risque accepté -> risque net -> risque inconnu

Risques du Conseil fédéral: principaux risques pour le Conseil fédéral qui, après un examen, lui sont annoncés par la CSG dans le cadre d'un processus de consolidation de tous les risques de l'administration fédérale.

Risques du département: tous les risques déclarés par les UA au département. Il s'agit des principaux risques de chaque UA et de tous les risques dépassant un niveau défini.

Risques du service: tous les risques identifiés et gérés au niveau d'une UA.

---

[86] Ch. 2, al. 1, des directives du CF sur la politique de gestion des risques

[87] Voir Bruno Brühwiler (2011). *Risikomanagement als Führungsaufgabe* (3e édition revue et actualisée). Berne: éditions Haupt

Risques majeurs: tous les risques déclarés par les départements et la ChF au service de coordination de l'AFF. Il s'agit des principaux risques de chaque département et de la ChF ainsi que de tous les risques dépassant un niveau défini.

Risques transversaux: événements ou évolutions qui, lorsqu'ils se produisent, peuvent affecter simultanément plusieurs UA ou avoir des conséquences négatives similaires ou identiques indépendantes sur l'exécution des tâches et l'atteinte des objectifs de plusieurs UA. *Exemples: panne informatique de grande ampleur, pandémie, tremblement de terre, corruption,* etc.

Scénario: présentation concrète et imagée d'un risque qui comprend des hypothèses sur les liens possibles entre des causes et des événements ou des évolutions et qui indique comment des menaces ou dangers peuvent se concrétiser dans l'administration fédérale.

Seuil d'acceptation du risque: niveau de risque défini par UO à partir duquel des mesures de maîtrise du risque doivent être envisagées.

Système de contrôle interne (SCI): il englobe toutes les mesures réglementaires, organisationnelles et techniques qui sont prises pour réduire les risques identifiés dans une organisation. Dans l'administration fédérale, le SCI se concentre notamment sur les processus opérationnels ayant une incidence financière.

Tolérance au risque: acceptation d'un risque dans le cadre des directives légales et réglementaires.

Type de risque: subdivision des risques selon différents critères.

Unité administrative (UA): offices de l'administration fédérale qui traitent les dossiers[88].

Unité d'organisation (UO): groupe de personnes et d'équipements avec des responsabilités, des prérogatives et des relations structurées. Ce terme peut désigner l'administration fédérale dans son ensemble, un département, la ChF, une UA ou des entités plus petites.

Urgence: événement soudain et imprévisible qui a de graves conséquences négatives et requiert une intervention rapide. Contrairement à une crise, une urgence se réfère à un événement délimité géographiquement, qui doit être éliminé ou maîtrisé aussi vite que possible.

Value at risk: niveau de dommage maximum en cas de probabilité précise suffisamment élevée (par ex. 95 % ou 99 %).

[88] Art. 43, al. 1, LOGA

Annexe 2-1: Modèle de rapport détaillé

R1	<Titre > Dénomination précise et parlante du risque	< Propriétaire > Personne gérant la tâche/le risque	<UA>	<Dpt>
<type de risque> p.ex. risque important, risque du Conseil Fédéral→ inséré automatiquement			Date :	<Date>

Remarques générales

Méthode: les tâches et les objectifs de la Confédération sont déterminants (définition du risque). Délimiter le risque de manière appropriée **en vue de sa gestion** (cadrage). Analyser et comprendre précisément le contexte et les facteurs de risque. Informations détaillées dans le manuel (chap. 3.2).

Forme: texte succinct et pertinent. Éviter le jargon technique. Développer les abréviations lors de la première utilisation. **Le texte doit aussi pouvoir être compris rapidement et facilement par des personnes extérieures.** Principaux destinataires: directeurs d'office, secrétaires généraux, chefs de département, Chambres fédérales.

Tâche / obejctif — max. 700 caractères

- Brève description des tâches/objectifs suprêmes concernés par le risque (indiquer loi, ordonnance, ACF)

→ **But:** définir la compétence (TCR)

Pire cas crédible — max. 1100 caractères

- Brève description du pire cas possible en cas de survenance du risque. **La compréhension et la plausibilité sont particulièrement importantes.**

→ **But:** objet de l'évaluation du risque

Causes

- Nouvelle indication, sous forme de mots-clés, des principales causes, qui figurent généralement déjà dans l'analyse du risque. Bref commentaire le cas échéant.
- **Forme:** cause du risque 1, év. bref commentaire)

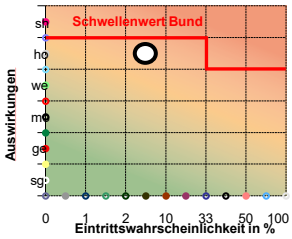
→ **But:** les causes permettent de prendre les mesures visant à réduire la probabilité d'un risque. Les mots-clés en donnent un aperçu rapide.

Analyse — max. 2500 caractères

- Bref commentaire sur le risque, ses causes, ses conséquences et ses facteurs d'influence
- Exemples de questions clés: quel événement/développement peut se produire à cause de quels motifs? Quelles sont les causes principales? Quels facteurs et conditions sont importants? À quelles conséquences financières et/ou non financières faut-il s'attendre si le risque survient et quels seront les effets si les tâches ou objectifs ne peuvent plus être réalisés?

→ **But:** comprendre le risque

Évaluation du pire cas crédible



- **Remarques générales:** évaluation du pire scénario en tenant compte de toutes les mesures actives (risque net!) → les conditions réelles existantes sont déterminantes.
- Si un événement primaire (par ex. crue) est à la base d'un risque, seul le risque identifié **pour la Confédération** est évalué. Les conséquences se réfèrent à celle-ci (exceptions: dommages corporels et environnementaux).

→ **But des explications:** mieux comprendre l'évaluation

Explication de la probabilité d'occurrence — max. 700 caractères

- Bref commentaire des bases, des hypothèses ou des comparaisons sur lesquelles repose la probabilité

Explications des conséquences — max. 600 caractères par dimension

[dimensions : financier, dommages corporel, réputation/confiance, processus opérationnels, dommages à l'environnement]

- Bref commentaire des bases, des hypothèses ou des comparaisons sur lesquelles reposent les conséquences
- Évaluer / décrire toute dimension pertinente des conséquences. Celle qui a l'évaluation la plus élevée est déterminante pour évaluer les conséquences du risque (principe du maximum).
- Impératif: conséquences financières et au moins une conséquence non financière

Explication de la modification de l'évaluation — max. 700 caractères

- Si la probabilité et/ou les conséquences financières et/ou une conséquence non financière ont été modifiées: brève justification

Mesures actives

- **Remarques générales:** des mesures sont prises pour réduire la probabilité du risque (prévention des causes) et/ou l'ampleur des dommages (raccourcissement et atténuation des conséquences). L'analyse, le pire scénario, l'évaluation et les mesures forment un ensemble logique.
- **Statut des mesures actives: introduite** = mesure en cours; **décidée** = mesure acceptée, mais pas encore lancée; **possible** = projet, mais aucune décision; **récurrente** = exécution régulière. **Mesures inactives: mise en œuvre** = achevée; **rejetée** = vérifiée et abandonnée.
- **Évaluation et commentaire: mise en œuvre** = comparaison avec le plan; **efficacité** = appréciation réaliste et transparente des effets recherchés

1. <Titres de la mesure> Nom précis et parlant	<Responsable> Personne responsable de la mesure	<Délai>	<Statut>

- **Description succincte:** en quoi consiste la mesure? Focalisation sur ses principaux éléments; aucun détail/débat/calendrier de projet. Permet aux lecteurs de comprendre et de catégoriser rapidement la mesure.

Appréciation	1	2	3	4	Commentaire de la personne responsable de la mesure
Mise en œuvre 1 = conforme au plan; 2 = légèrement retardé 3 = considérablement retardé.; 4 = fortement retardé	☒	☐	☐	☐	▪ Bref commentaire de l'évaluation. Motifs de l'évaluation (critique), propositions d'amélioration, actions recommandées (mots-clés). ▪ Important: se baser autant que possible sur des faits sans chercher à enjoliver les choses; commentaire transparent.
Efficacité 1 = élevé; 2 = plutôt élevé; 3 = plutôt faible; 4 = faible	☐	☐	☒	☐	

Annexe 2-2: Modèle de rapport succinct

1

R4	<Titre du risque > Dénomination précise et parlante du risque	<Nom Propriétaire >	<VE>	<Dept>

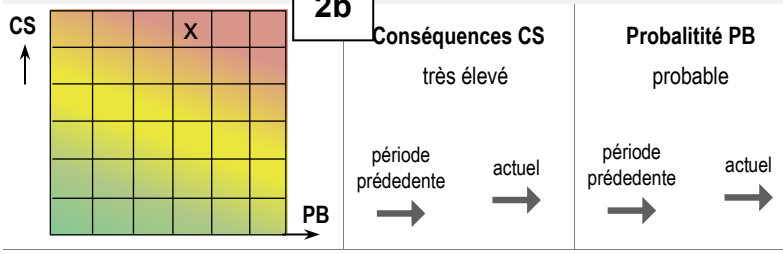
2

Risque

Pire cas credible — **2a**

- **But:** comprendre les principaux éléments du risque
- **Contenu:** présentation du risque survenant dans le pire des scénarios
- **Forme:** concise et compréhensible, accent mis sur l'essentiel
- **Nombre de caractères:** 1100 max.

Evaluation — **2b**



Commentaire du/de la propriétaire du risque — **2c**

- **But:** commentaire du propriétaire du risque
- **Contenu:** commentaire sur l'évolution du risque, autres faits importants pour comprendre le risque, particularités, etc.
- **Forme:** concise et compréhensible ; donner les éléments significatifs et travailler en comptant le nombre de caractères
- **Nombre de caractères:** 1100 max.

3

Ensemble des mesures

Appréciation du/de la propriétaire (1 = entièrement vrai; 4 = pas du tout vraiu) — **3a**

	1	2	3	4
Mise en œuvre conforme au plan	☒	☐	☐	☐
Mesures sont efficaces et suffisantes	☐	☒	☐	☐

Commentaire du/de la propriétaire du risque

- **But:** commentaire du propriétaire du risque
- **Contenu:** appréciation, commentaire de l'évaluation en 3a (mise en œuvre, efficacité)
- **Forme:** concise et compréhensible ; donner les éléments significatifs et travailler en comptant le nombre de caractères
- **Nombre de caractères:** 1100 max.

Explications

Cette présentation montre le nouveau format de rapport au Conseil fédéral, qui se concentre sur les principales informations relatives au risque et aux mesures correspondantes. Des textes concis, adaptés au niveau hiérarchique, permettent au Conseil fédéral et aux membres des CdG d'obtenir et de comprendre rapidement les points essentiels. Remaniée, la page de titre donne un aperçu de tout le portefeuille de risques grâce à la matrice et à la liste des risques. Le rapport 2021 expose pour la première fois les risques du Conseil fédéral exclusivement sous cette forme à la CdG et au Conseil fédéral.

Remarques sur les différents champs:

1 **Titre** indiquant le numéro et le nom du risque, le propriétaire du risque, l'UA et le département

2 **Partie consacrée au risque**

2a **Pire cas crédible:** présentation succincte du scénario si le risque (événement ou développement) se produit. Exposé des principaux éléments du risque. Les CdG et le Conseil fédéral doivent pouvoir comprendre le risque, ses composantes et son déroulement. [max.1100 caractères]

2b **Évaluation:** le logiciel fournit automatiquement des informations sur l'évaluation à partir des saisies correspondantes.

2c **Commentaire du propriétaire du risque:** le propriétaire du risque expose et commente les principaux faits et les particularités du risque (par ex. son développement et sa dynamique, s'il s'agit d'un risque transversal avec x risques initiaux → mentionner le commentaire au début). [max.1100 caractères]

3 **Partie consacrée aux mesures**

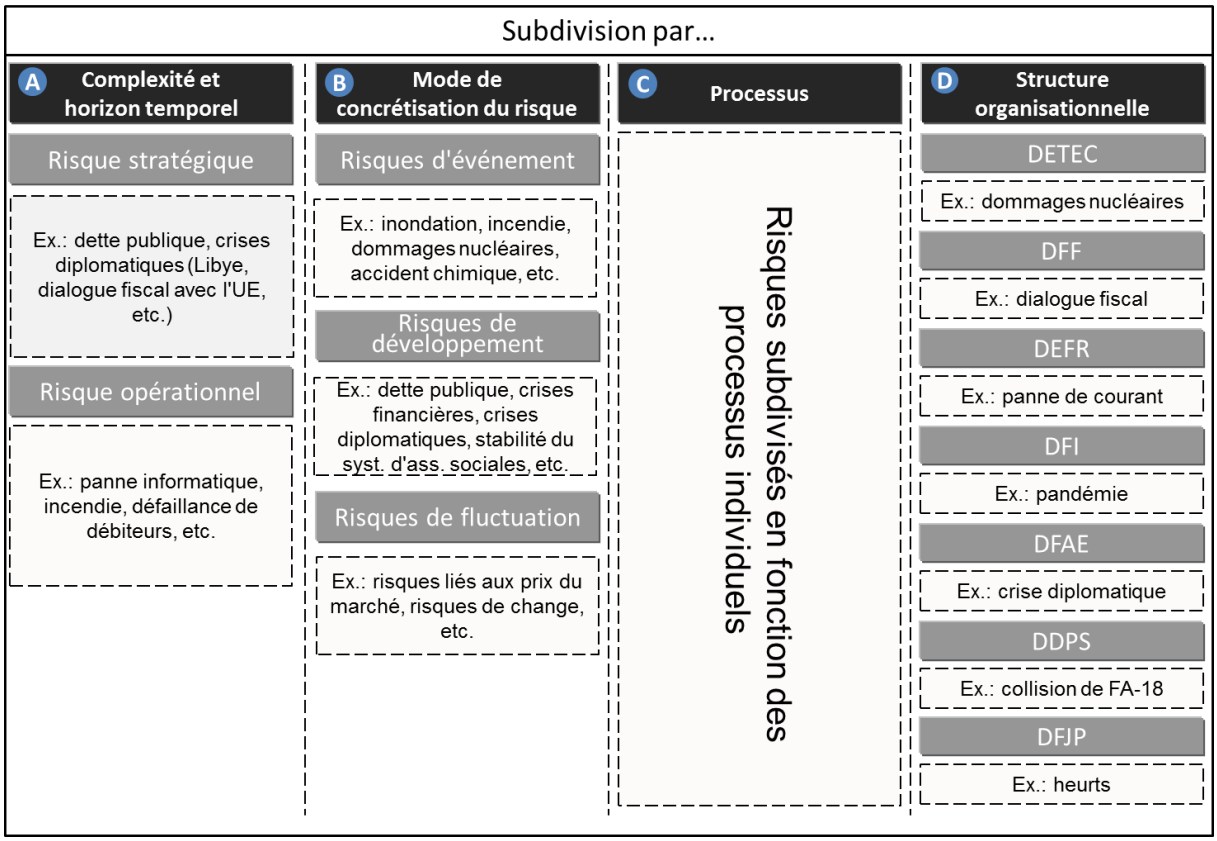
Le propriétaire du risque présente et commente ici toutes les mesures actives.

3a **Évaluation des mesures:** la mise en œuvre (conforme aux prévisions ou divergente) et l'efficacité des mesures (portent-elles leurs fruits et suffisent-elles pour maîtriser le risque comme convenu?) sont évaluées globalement sur une échelle de 4.

3b **Commentaire du propriétaire du risque:** l'évaluation des mesures (3a) est exposée et commentée ici (particularités, difficultés, lacunes, besoin d'intensification, etc.). [max.1100 caractères]

Annexe 3: Structure des risques

Les subdivisions suivantes peuvent être utiles, en plus des catégories de risques, pour obtenir une vue d'ensemble et systématiser les différents risques. Cette section entend promouvoir la compréhension commune et fournir un point de départ pour déterminer les méthodes d'analyse et d'évaluation du risque.



a. ***Complexité et horizon temporel:*** de nombreuses organisations font une distinction théorique et pratique entre les risques stratégiques et les risques opérationnels, qui se différencient à plusieurs égards: les risques stratégiques sont généralement plus complexes (nombreux liens avec d'autres facteurs) et plus abstraits (moins tangibles) que les risques opérationnels. Ils portent davantage sur le long terme et sont gérés par les échelons hiérarchiques supérieurs d'une organisation. Le niveau ou l'importance d'un risque constitue parfois un critère supplémentaire: les grands risques sont plutôt considérés comme d'ordre stratégique et relèvent de la responsabilité de l'échelon hiérarchique le plus élevé. De plus, les risques stratégiques ont souvent un mode de concrétisation différent de celui des risques opérationnels, puisqu'ils tendent à présenter les caractéristiques d'un risque d'évolution.

   On distingue parfois les risques stratégiques des risques opérationnels pour permettre l'établissement de rapports adaptés aux niveaux de responsabilité: l'échelon hiérarchique le plus élevé a tendance à se concentrer sur les risques stratégiques de l'organisation, tandis que les échelons hiérarchiques inférieurs sont chargés de gérer les risques opérationnels dans leur domaine.

   Des méthodes d'analyse et d'évaluation différentes doivent être utilisées selon le type de risque: les analyses d'indicateurs et de scénarios, notamment, conviennent mieux aux risques stratégiques, alors que toutes les méthodes d'analyse peuvent être judicieuses pour les risques opérationnels, en fonction de leur nature. Les méthodes d'analyse et d'évaluation des risques sont présentées au ch. 0.

b. ***Mode de concrétisation du risque:*** les risques peuvent se concrétiser de plusieurs manières. Un *risque d'événement* apparaît de façon relativement rapide et soudaine, voire imprévue. En revanche, un *risque d'évolution* reflète la détérioration d'une situation et l'accroissement des conséquences négatives au fil du temps; il est donc difficile à délimiter dans le temps et concerne souvent le long terme. En général, ce risque ne survient pas inopinément, car il se développe progressivement et peut être identifié au préalable grâce à des indicateurs. Un *risque de fluctuation* se caractérise par le fait qu'il survient toujours, même si l'ampleur et le type de fluctuation (chance ou risque) demeurent inconnus dans un premier temps. Les risques des marchés financiers sont des risques de fluctuation classiques.

   Des méthodes d'analyse et d'évaluation différentes doivent être utilisées selon le type de risque: les analyses statistiques, en particulier, sont pertinentes pour les risques de fluctuation, alors que les analyses de scénarios sont préférables pour les risques d'événement et les analyses d'indicateurs pour les risques d'évolution (voir le ch. 0).

c. ***Processus:*** une subdivision des risques par processus est judicieuse si, par exemple, une unité administrative met en œuvre une gestion de la qualité et exécute ses tâches selon des processus clairement définis.

d. ***Structure organisationnelle:*** fréquente dans la pratique, une subdivision des risques suivant la structure organisationnelle permet d'affecter clairement un risque à une organisation et à sa direction.

Annexe 4: Cahiers des charges des responsables de la gestion des risques des départements et des UA

Cahier des charges des responsables de la gestion des risques des départements

Mise en œuvre du processus de gestion des risques dans le département / à la ChF
▪ Planification temporelle et organisationnelle et communication du processus de gestion des risques au niveau du département / de la ChF, en tenant compte des délais fixés par le service de coordination de l'AFF ▪ Exécution du processus de gestion des risques dans le cadre de sa fonction de responsable de la gestion des risques au secrétariat général (accent mis sur les tâches du département / de la ChF)
Application uniforme de la gestion des risques au sein du département / de la ChF
▪ Identification de la nécessité éventuelle d'élaborer une instruction départementale sur la gestion des risques qui tienne compte des prescriptions énoncées dans les directives sur la gestion des risques menée par la Confédération, et rédaction éventuelle de cette instruction au niveau du département / de la ChF
Coordination et pilotage des responsables de la gestion des risques des UA au sein du département
▪ Organisation des échanges entre les responsables de la gestion des risques des UA au sein du département grâce à des réunions régulières ▪ Organisation et pilotage de la coordination relative aux risques transversaux au sein du département
Établissement du rapport sur les risques au niveau du département / de la ChF
▪ Regroupement des risques du département déclarés par les UA (y c. le secrétariat général), vérification des interactions entre les risques ▪ Analyse et pilotage des discussions, des vérifications et de la comparaison croisée des risques du département au sein de celui-ci / de la ChF et entre les UA ▪ Rédaction d'un rapport pour le chef et la direction du département / de la ChF ▪ Envoi du rapport au service de coordination de l'AFF en vue du rapport au Conseil fédéral ▪ Proposition pour la sélection des risques majeurs du département / de la ChF (décision du chef de département)
Coordination de l'analyse des interactions entre les risques des différentes UA Soutien technique des propriétaires des risques du niveau du département / de la ChF et des responsables de la gestion des risques des UA
▪ Réponses aux questions des propriétaires des risques au niveau du département / de la ChF qui concernent la méthodologie de la gestion des risques ▪ Réponses aux questions sur R2C_GRC et aux questions techniques des responsables de la gestion des risques des UA
Interface et interlocuteur pour le service de coordination de l'AFF
▪ Participation régulière aux ateliers sur la gestion des risques au niveau de la Confédération (organisés par le service de coordination de l'AFF) ▪ Collaboration avec le service de coordination de l'AFF pour l'examen des risques du Conseil fédéral au niveau du département / de la ChF
Communication adéquate des décisions du Conseil fédéral, de la CSG et du service de coordination de l'AFF aux responsables de la gestion des risques du département et des UA Intégration de la gestion des risques dans d'autres processus de conduite du département/de la ChF
▪ Intégration de la gestion des risques dans d'autres processus de conduite, notamment le SCI, la gestion de la qualité, la gestion de la sécurité informatique, etc.

Amélioration de la gestion des risques au sein du département / de la ChF et de l'administration fédérale
▪ Élaboration d'idées pour améliorer et développer la gestion des risques dans l'administration fédérale à partir des expériences acquises dans ce domaine ▪ Participation aux manifestations sur la gestion des risques, notamment à celles dont le sujet concerne le département / la ChF ▪ Contribution à la prise de conscience des risques au niveau du département / de la ChF et du secrétariat général

Cahier des charges des responsables de la gestion des risques des UA

Mise en œuvre du processus de gestion des risques au niveau de l'UA
▪ Planification temporelle et organisationnelle et communication du processus de gestion des risques au sein de l'UA, en tenant compte des délais fixés au niveau du département (instructions du responsable de la gestion des risques du département) ▪ Exécution du processus de gestion des risques dans l'UA: ateliers avec la direction de l'UA ou les détenteurs appropriés de connaissances, entretiens individuels, etc.
Application uniforme de la gestion des risques au sein de l'UA
▪ Identification de la nécessité éventuelle d'élaborer une instruction spécifique à l'UA sur la gestion des risques qui tienne compte des prescriptions énoncées dans les directives sur la gestion des risques de la Confédération ou de l'instruction du département
Élaboration d'un rapport adéquat sur les risques au niveau de l'UA
▪ Regroupement des risques identifiés et analysés dans les divisions et les sections, y compris les mesures proposées ▪ Pilotage des discussions, des vérifications et de la comparaison croisée des risques des différentes divisions ▪ Rédaction d'un rapport pour le responsable de l'UA ▪ Rédaction d'un rapport pour le responsable de la gestion des risques du département
Soutien technique des propriétaires des risques du niveau de l'UA
▪ Réponses aux questions des propriétaires des risques et de la direction de l'UA qui concernent la méthodologie de la gestion des risques et la structure des risques
Interface et interlocuteur pour le responsable de la gestion des risques du département
▪ Participation aux réunions du département sur la gestion des risques (organisées par le responsable de la gestion des risques du département) ▪ Collaboration et échanges concernant les risques de l'UA qui feront partie des risques du département
Communication adéquate des décisions du Conseil fédéral, de la CSG, du service de coordination de l'AFF et du responsable de la gestion des risques du département à la direction de l'UA et aux propriétaires des risques de l'UA Intégration de la gestion des risques dans d'autres processus de conduite de l'UA
▪ Intégration de la gestion des risques dans d'autres processus de conduite de l'UA, notamment le SCI, la gestion de la qualité, la gestion de la sécurité informatique, etc.
Amélioration de la gestion des risques au sein de l'UA et de l'administration fédérale
▪ Élaboration d'idées pour améliorer et développer la gestion des risques dans l'UA et dans l'administration fédérale à partir des expériences acquises dans ce domaine ▪ Participation aux manifestations sur la gestion des risques, notamment à celles qui concernent l'UA ▪ Contribution à la prise de conscience des risques au sein de l'UA

Annexe 5: Exemple de refus d'une demande de consultation de la base de données des risques R2C_GRC concernant la gestion des risques de la Confédération

Recommandé
xxx
xxx
xxx

Berne, le xxx

Votre demande de consultation du xxx

Monsieur,

Par votre courriel du xxx, vous avez demandé à consulter la «base de données R2C_GRC (système de gestion des risques destiné au recensement des risques de la Confédération)» en vertu de la loi sur la transparence (LTrans; RS *152.3*).

Après un examen de la situation, nous ***nous prononçons*** comme suit:

1. L'accès est refusé.
2. Aucun émolument ne sera perçu (art. 17, al. 2, let. a, Ltrans).

Motifs:

L'Administration fédérale des finances (AFF) met l'application informatique commune R2C_GRC à la disposition des départements et de la Chancellerie fédérale (ChF) pour la gestion de leurs risques et l'établissement de rapports correspondants. Les principaux risques de la Confédération sont identifiés, analysés et évalués en détail dans cette application. De plus, les trains de mesures et leur degré de mise en œuvre y sont consignés. Un rapport sur les risques est établi (au moins) une fois par an; il est classé CONFIDENTIEL à tous les échelons (UA, département, ChF, Conférence des secrétaires généraux, Conseil fédéral). Pour préserver la confidentialité des informations, les Commissions de gestion ont également pris des mesures particulières lors de l'examen du rapport sur les risques destiné au Conseil fédéral.

Le niveau de classification a été vérifié sur la base de la présente demande (art. 11, al. 5, de l'ordonnance sur la transparence [OTrans; RS *152.31*] en relation avec l'art. 13, al. 3, de l'ordonnance concernant la protection des informations [OPrI; RS *510.411*]); il est justifié.

La Confédération a tout intérêt à maintenir la confidentialité des informations enregistrées dans l'application R2C_GRC. Leur consultation pourrait notamment affecter la libre formation de l'opinion et de la volonté en rapport avec la gestion des risques et les mesures à prendre. De plus, l'exécution conforme aux objectifs des mesures concrètes prises par les autorités pourrait être entravée. Dans certaines circonstances, la sécurité intérieure et extérieure de la Suisse pourrait même être gravement menacée.

En l’espèce, la consultation ne présente pas un intérêt supérieur.

Pour ces motifs, l’accès aux informations enregistrées dans R2C_GRC est refusé sur la base notamment de l’art. 7, al. 1, let. a à c, LTrans.

Veuillez agréer, Monsieur, nos salutations les meilleures.

xxx
Conseillère à la transparence AFF

Informations sur la procédure de médiation (voir l’art. 13 LTrans)

[1] *Toute personne peut déposer une demande en médiation:*

a. lorsque sa demande d’accès à des documents officiels est limitée, différée ou refusée;

b. lorsque l’autorité n’a pas pris position sur sa demande dans les délais;

c. lorsque l’autorité, après l’avoir entendue selon l’art. 11, entend accorder l’accès aux documents malgré son opposition.

[2] *La demande en médiation est déposée par écrit auprès du Préposé fédéral à la protection des données et à la transparence dans un délai de 20 jours à compter de la date de réception de la prise de position de l’autorité ou à l’échéance des délais fixés à l’autorité pour prendre position.*

Annexe 6: Interface « Gestion des risques – établissement des comptes » à la Confédération

Cas, exemples		Probabilité (sortie de fonds)		Présentation des comptes		Gestion des risques
				Termes[1]	Mention dans les comptes annuels	
Engagement existant (ch. 6.5, cas 1)	**Engagement futur** (ch. 6.5, cas 2)	100 %	Probable (100 %)[2]	**«Engagement»** (art. 49, al. 2 et 4, LFC)	Inscription au passif du bilan (art. 56 OFC)	**Aucune saisie d'un risque** (événement probable ou presque certain)
• Cautionnements et garanties • Engagements de capital en faveur des banques de développement	• Procédures judiciaires en cours • Besoin d'assainissement latent		Relativement probable (> 50 % et < 100 %)	**«Provision»** (art. 49, al. 3, LFC)		
			Plutôt improbable (10 % à < 50 %)	**«Engagement conditionnel»** (IPSAS 19, manuel de gestion budgétaire et de tenue des comptes de la Confédération, ch. 10.2)	Publication dans l'annexe des comptes annuels (IPSAS 19, manuel de gestion budgétaire et de tenue des comptes de la Confédération, ch. 10.2)	**Saisie d'un risque possible,** si cela améliore le pilotage des tâches, notamment si: • le pilotage des tâches et l'atteinte des objectifs sont mis en danger, • le risque est important, et • des mesures pour réduire le risque peuvent être prises.
		0 %	Très improbable (< 10 %)	–	Aucune mention	

[1] Voir le message du 24 novembre 2004 concernant la révision totale de la loi fédérale sur les finances de la Confédération (FF **2005** 5, p. 15, 57, 61 s., 85 s., 104 s. et 107)

[2] En vertu de l'art. 49, al. 2, LFC, une sortie de fonds est *prévisible* (probabilité = 100 %) lorsque sa réalisation est *pratiquement certaine*. En revanche, un événement futur ne présente aucune *certitude absolue*

Annexe 7: Organisations en dehors de l'administration fédérale

Dans l'optique de la gestion des risques de la Confédération, des risques très divers peuvent découler des relations entre la Confédération et des organisations extérieures à l'administration fédérale. La présente annexe examine en détail les exemples suivants:

1. Prêts, cautionnements, garanties, etc. accordés à une organisation par la Confédération
2. Fonction de surveillance ou de révision de l'organisation exercée par un service de la Confédération
3. Responsabilité subsidiaire de la Confédération selon l'art. 19 de la loi sur la responsabilité (LRCF)[89] et autres risques financiers
4. Responsabilité de la Confédération pour ses représentants au sein d'organes de direction ou de gestion d'une organisation
5. Risques dans des entités devenues autonomes qui pourraient se répercuter sur la Confédération en tant que propriétaire

1. Prêts, cautionnements, garanties, etc.[90]

L'octroi à des tiers de prêts, de cautionnements, de garanties ou d'autres sûretés similaires par la Confédération requiert une base légale formelle. La loi établit à quels destinataires, dans quelles circonstances, dans quel but, dans quelle mesure et dans quelles conditions de telles prestations peuvent (ou doivent) être fournies. En octroyant de telles prestations, la Confédération entend promouvoir l'exécution de tâches qui servent ses intérêts car ces dernières peuvent être financées à moindres frais.

Dans l'optique de la gestion des risques de la Confédération, un risque peut par exemple survenir lorsque:

- le tiers détourne les prestations de la Confédération de leur destination;
- le remboursement ou la rémunération prévus n'ont pas lieu, ou
- la Confédération doit fournir des prestations supplémentaires qui n'étaient pas prévues pour pouvoir garantir l'exécution des tâches souhaitée (par ex. en cas de défaillance du bénéficiaire par suite d'une faillite).

Dans la plupart des cas, les conséquences de ces risques sont d'ordre financier, mais la réputation de la Confédération peut également être fortement entachée. Le service compétent de la Confédération doit surveiller constamment et de manière adéquate l'exécution des tâches par les bénéficiaires ainsi que la direction et la situation financière de ces derniers. Si nécessaire, il faut garantir en temps utile l'exécution des tâches au moyen de mesures appropriées et, le cas échéant, exiger un assainissement. Il est également essentiel de vérifier de temps à autre si l'aide de la Confédération au moyen des instruments utilisés est encore nécessaire et efficace.

[89] RS **170.32**
[90] Une description de ces cas selon les règles de l'établissement des comptes figure au ch. 6.5 et à l'annexe 6.

2. Activités de surveillance ou de révision exercées par la Confédération

Selon les art. 3 et suivants de la LRCF, la Confédération répond du dommage causé sans droit à un tiers par un de ses employés dans l'exercice de ses fonctions, sans égard à la faute de l'employé. Cette responsabilité de l'État s'étend également aux cas dans lesquels un tiers fait valoir un dommage dû au fait que le service fédéral compétent n'a pas suffisamment rempli son obligation de surveillance ou que le CDF a manqué de diligence dans la révision[91]. Dans l'optique de la gestion des risques de la Confédération, ces risques mentionnés en exemple sont surtout financiers. Les personnes lésées ne pouvant que difficilement prouver juridiquement le dommage, la probabilité du risque est relativement faible pour la Confédération. Il faut décider au cas par cas si un risque subsiste.

3. Responsabilité subsidiaire de la Confédération selon l'art. 19 LRCF et autres risques financiers

En ce qui concerne la responsabilité subsidiaire de la Confédération selon l'art. 19 LRCF, les critères suivants doivent être remplis:

- une organisation est *indépendante de l'administration ordinaire*; elle est dotée de la personnalité propre et tient sa propre comptabilité;
- une loi *charge* cette organisation d'exécuter *des tâches de droit public de la Confédération* (tâches de l'administration fédérale);
- des organes ou des employés de l'organisation causent sans droit, *dans l'exercice de l'activité qui a été déléguée à cette organisation*, un dommage à un tiers;
- l'organisation répond en premier lieu envers le lésé du dommage causé. La Confédération n'est responsable envers le lésé que si l'organisation n'est pas en mesure de réparer le dommage (responsabilité subsidiaire).

Il est très difficile de tenir adéquatement compte dans la gestion des risques de la Confédération de cette situation en matière de responsabilité. Un cas de responsabilité qui n'est pas assuré conformément à l'art. 19 LRCF peut générer des difficultés financières dans une organisation à laquelle une tâche de droit public a été confiée. Indépendamment de leur origine, ces difficultés (manque de liquidité ou surendettement imminents) nuisent à l'exécution de la tâche concernée, alors que la Confédération tient à ce que la tâche qu'elle a déléguée soit exécutée. La plupart du temps, il n'est pas possible de remplacer rapidement l'organisation. La Confédération risque alors de fait (et non de jure) de devoir refinancer l'organisation afin d'assurer l'exécution de la tâche en question, par exemple en contribuant financièrement à l'assainissement de l'organisation à laquelle elle l'a confiée. Le risque de responsabilité subsidiaire selon l'art. 19 LRCF n'est donc qu'un risque financier. Lors de son évaluation, il faut aussi prendre en considération les couvertures d'assurance de l'organisation.

[91] Si, dans des cas exceptionnels, la fonction de surveillance ou l'activité de révision de la Confédération devaient reposer sur une base de droit privé, les éventuelles prétentions d'un tiers en matière de responsabilité devraient être examinées en se fondant sur la norme correspondante de droit privé.

4. Responsabilité de la Confédération pour ses représentants au sein d'organes de direction ou de gestion d'une organisation

Les statuts des sociétés anonymes peuvent prévoir que la Confédération délègue un représentant au sein du conseil d'administration. Dans de tels cas, la Confédération assume la responsabilité vis-à-vis de la société, des actionnaires et des créanciers si son représentant occasionne un dommage en violant ses obligations de manière intentionnelle ou par négligence[92]. En ce qui concerne les représentants de la Confédération qui sont nommés membres d'un conseil d'administration parce que la Confédération détient des parts dans une société et non pas parce que la Confédération leur demande de la représenter, des bases légales ou contractuelles spécifiques régissent la responsabilité de la Confédération (pour les employés de la Confédération, dans leur contrat de travail; pour les tiers mandatés par la Confédération, dans leur mandat ou dans les instructions qu'ils ont reçues). Ces bases doivent être définies au cas par cas (mandat écrit et instructions) et examinées en cas de dommage. Il faut aussi vérifier si les sociétés ont conclu des assurances de responsabilité civile pour leurs organes.

5. Risques dans des entités devenues autonomes

En tant que propriétaire unique ou copropriétaire, la Confédération possède des entreprises auxquelles elle a confié l'exécution de tâches fédérales[93] (Poste, CFF, Swisscom, Skyguide et RUAG, mais aussi les EPF, Swissmedic, etc.). Le Conseil fédéral assure le pilotage de la stratégie de propriétaire de ces entreprises. Si une de ces dernières rencontre des difficultés financières (par ex. en raison d'erreurs de gestion, d'investissements risqués en Suisse et à l'étranger ou de variations du marchés qui n'ont pas été reconnues en temps utile), les conséquences pour la Confédération peuvent être graves: perte de dividendes, dépréciation de la valeur des participations dans le bilan de la Confédération, soutien financier par la Confédération en vue d'assurer la fourniture de la tâche fédérale qui a été déléguée voire, à l'extrême, de sauver l'existence de l'entreprise. Dans l'optique de la gestion des risques de la Confédération, le pilotage de la stratégie de propriétaire des entreprises de la Confédération est une tâche fédérale complexe liée à de nombreux défis. Il requiert une collaboration intense entre la gestion des risques et les services propriétaires.

[92] Art. 762, al. 4, CO en relation avec l'art. 754 CO. Cela vaut également pour les coopératives (voir l'art. 926, al. 3, CO).
[93] Voir l'art. 8, al. 5, LOGA

Annexe 8: Autres activités liées à la gestion des risques

Les activités suivantes présentent parfois des liens étroits et des interfaces avec la gestion des risques de la Confédération. Elles sont donc exposées brièvement ici.

I. Protection des infrastructures critiques (PIC)

Par infrastructures critiques (IC) on entend les processus, les systèmes et les installations qui sont essentiels au bon fonctionnement de l'économie ou au bien-être de la population. Il s'agit par exemple de l'approvisionnement en énergie, du transport ferroviaire ou des soins médicaux. Les infrastructures critiques englobent non seulement des bâtiments et des installations, mais également des systèmes d'approvisionnement et des services au sens large. Des défaillances graves (p. ex. une panne de courant à l'échelle nationale) pourraient avoir des conséquences économiques considérables et affecter fortement la population. La protection des infrastructures critiques comprend notamment des mesures architecturales, techniques, organisationnelles ou juridiques qui visent à empêcher autant que possible ces défaillances ou, en cas d'incident, à rétablir aussi rapidement que possible le bon fonctionnement des infrastructures.

En juin 2012, le Conseil fédéral a adopté pour la première fois une stratégie nationale de protection des infrastructures critiques (PIC) afin d'améliorer la résilience de la Suisse en la matière (capacité de résistance, d'adaptation et de rétablissement). Il l'a mise à jour fin 2017, tout en conservant les objectifs et axes prioritaires de la version de 2012. La stratégie a de nouveau été mise à jour fin 2022.

La protection des infrastructures critiques est une tâche commune et transversale qui présente des liens étroits avec différents domaines politiques et domaines de tâches (politique énergétique, politique de sécurité, protection contre les risques naturels, etc.). Cette stratégie PIC est donc mise en œuvre principalement grâce à des structures et compétences décentralisées, les compétences des services fédéraux concernés, des cantons, des communes et des exploitants d'IC étant réservées. La loi fédérale du 20 décembre 2019 sur la protection de la population et sur la protection civile (LPPCi) exige[94] que la Confédération établisse les bases de la PIC, que l'OFPP tienne un inventaire des ouvrages d'infrastructure critique et coordonne les mesures de planification et de protection mises en place par les exploitants d'IC, en étroite collaboration avec eux[95].

La gestion des risques de la Confédération se concentre sur les risques liés à l'exécution des tâches de l'administration fédérale, tandis que la PIC porte sur ceux des infrastructures critiques ou sur le renforcement de la résilience de ces dernières. Il existe à cet égard plusieurs interfaces, car l'administration fédérale fait également partie des infrastructures critiques (sous-secteur Parlement, gouvernement, justice, administration), une défaillance de certaines infrastructures critiques (par ex. électricité, télécommunications) peut aussi avoir de graves conséquences sur l'exécution des tâches de l'administration fédérale et certaines entreprises comptant parmi les infrastructures critiques appartiennent partiellement ou entièrement à la Confédération.

II. Analyse nationale des risques

L'analyse nationale des risques «Catastrophes et situations d'urgence en Suisse» (CaSUS) examine les conséquences des différents dangers naturels, techniques et sociétaux sur la population et ses moyens de subsistance en Suisse. Elle vise principalement à établir une base commune pour préparer la société à surmonter certains événements dommageables.

---

94 Art. 8 LPPCi (RS 520.1)

95 Pour de plus amples informations, voir la stratégie PIC 2018-2022 (FF **2018** 491, page Web Stratégie nationale PIC [admin.ch]).

Une compréhension commune des conséquences, du déroulement et de la dynamique des dangers est indispensable en la matière, car (la préparation à) leur maîtrise requiert une collaboration toujours plus étroite entre les services de la Confédération et des cantons, l'économie, la science et la population. S'appuyant sur la LPPCi, la CaSUS est coordonnée par l'OFPP. À l'occasion des travaux menés dans le cadre de l'analyse nationale des dangers, plusieurs produits ont été développés et seront régulièrement mis à jour[96]:

- le *rapport sur la gestion des risques* et la *brochure* correspondante exposent les résultats des analyses de 44 types de catastrophes et de situations d'urgences qui ont été étudiés et mis en relation;
- la *méthodologie* documente la procédure et la métrique utilisées;
- la *liste des dangers* récapitule les dangers possibles et présente, à l'aide d'exemples, une vue d'ensemble cohérente des événements et évolutions concevables sans les classer par ordre de priorité;
- les *dossiers sur les dangers*: les informations disponibles sur chaque danger identifié sont analysées et des scénarios sont développés systématiquement et réunis dans un dossier spécifique. Ces scénarios constituent la base de l'analyse des risques ou du rapport sur la gestion des risques.

La gestion des risques de la Confédération se concentre sur l'administration fédérale, tandis que les travaux réalisés dans le cadre de l'analyse nationale des risques portent sur les catastrophes, les situations d'urgence ainsi que sur leurs conséquences au niveau de la population et de ses moyens de subsistance.

[96] Voir également www.risk-ch.ch.

Annexe 9: Obstacles à la gestion des risques

Certains obstacles généraux peuvent entraver la mise en œuvre efficace de la gestion des risques, en particulier lorsque ces derniers sont complexes et difficilement identifiables, et favoriser le développement progressif des risques. Ils sont brièvement exposés ci-après[97]. Il incombe aux propriétaires des risques et aux responsables de la gestion des risques des départements et des UA d'identifier et d'atténuer ces problèmes dans leur domaine.

- ***Bureaucratie:*** une application proactive du processus de gestion des risques est décisive pour sa réussite. Après avoir été exécuté de manière similaire pendant quelques années, ce processus risque de se transformer en une routine bureaucratique. Les nouveaux risques et les modifications des risques existants ne seront alors plus recherchés proactivement et le processus sera réalisé aussi rapidement que possible et sans engagement, de sorte que des risques importants ne seront pas identifiés et que les mesures appropriées pour la gestion de ces derniers ne seront pas prises.

- ***Manque d'engagement des parties prenantes:*** la participation de toutes les personnes pertinentes au processus de gestion des risques est essentielle. Elle garantit une information aussi optimale et exhaustive que possible en vue de l'évaluation objective d'un risque. De plus, elle contribue à accroître sensiblement (en interne et à l'extérieur) la confiance dans la gestion des risques et ses résultats. Le manque d'engagement des parties prenantes peut se traduire, au final, par des retards considérables dans l'analyse et la maîtrise des risques.

  Exemple: grands projets de centrales (leur réalisation n'est possible qu'avec une vaste participation des parties prenantes)

- ***Conflits d'intérêts et présentation erronée délibérée des risques:*** Des conflits d'intérêts peuvent entraver le processus de gestion des risques tant lors de l'analyse de ces derniers que de l'application des mesures visant à les maîtriser. Les intérêts spécifiques des parties prenantes peuvent, d'une part, conduire intentionnellement ou non à une présentation et une analyse erronées des risques et, d'autre part, bloquer les décisions pour la mise en œuvre des mesures nécessaires. Ces conflits d'intérêts doivent être identifiés et, si possible, résolus.

  Exemple: études sur les risques du tabagisme pour la santé qui sont financées par l'industrie du tabac

- ***Responsabilités diluées ou floues:*** il est possible que les décisions concernant les mesures requises ne soient pas prises ou soient prises trop tardivement, en particulier dans les organisations complexes où plusieurs acteurs assument conjointement la responsabilité ou lorsque celle-ci n'est pas définie clairement, car personne ne s'estime véritablement responsable.

  Exemple: pénurie de courant en Italie

- ***Équilibre entre transparence et confidentialité:*** dans certains cas, la confidentialité des informations sur les risques (et, dès lors, leur non-communication) se justifie pour préserver la sécurité nationale ou éviter une panique générale. L'absence de transparence en matière de risques peut néanmoins entamer la confiance dans la gestion des risques ou conduire, par manque d'informations, à ne pas accorder la priorité nécessaire à la maîtrise de certains risques.

  Exemple: falsification du bilan d'Enron

[97] Les structures et les caractéristiques exposées ici et d'autres sont présentées plus en détail dans le rapport «Risk Governance Deficits» de l'International Risk Governance Council (IRGC): http://www.irgc.org/-Risk-Governance-Deficits-.html.

- ***Asymétrie des informations:*** dans certains cas, le maintien d'une asymétrie des informations répond aux objectifs de la gestion des risques. Par exemple, certaines informations sur la lutte contre le terrorisme sont gardées secrètes pour renforcer la sécurité nationale. Toutefois, dans de nombreux cas, le maintien et l'existence d'asymétries des informations sont dommageables, car les responsables de la gestion des risques et les décideurs, par exemple, n'ont pas toutes les informations nécessaires pour analyser et évaluer un risque et peuvent dès lors négliger des mesures indispensables à sa maîtrise.

  Exemple: crise des subprimes aux États-Unis (investisseurs et propriétaires fonciers pas suffisamment informés des risques)

- ***Compréhension par le public et tolérance des risques:*** en plus d'une analyse scientifique et objective des risques, l'opinion publique évalue toujours les grands risques sociaux, mais sa perception peut varier de l'appréciation objective. La probabilité, l'ampleur des conséquences et les facteurs suivants jouent un rôle primordial dans la compréhension des risques par le public et la tolérance correspondante: valeurs culturelles, possibilité de contrôler personnellement le risque, répartition des conséquences sur la population, familiarité du risque, responsabilité des activités humaines, prise en charge consciente du risque par la population, etc. Ces réflexions doivent être intégrées à la gestion des risques pour renforcer l'acceptabilité des décisions concernant ces risques.

  Exemple: génie génétique (risques perçus différemment aux États-Unis et dans l'UE), problématiques liées aux déchets radioactifs, changement climatique, etc.

- ***Identification des situations imprévisibles et actions correspondantes:*** d'une part, il existe souvent des barrières cognitives à l'identification de nouveaux risques. En clair, de nombreuses personnes peuvent difficilement identifier des événements sortant des paradigmes habituels. Pour y remédier, il est important de miser sur la créativité et, par exemple, de faire appel à des anticonformistes lors de l'identification des risques. D'autre part, une organisation ne peut pas toujours réagir conformément à la situation en cas de changements rapides. Il faut alors adopter une position et une culture qui encouragent la prise de décisions même dans l'incertitude ainsi que la capacité à se détacher de procédures et de structures qui ne sont plus adaptées.

  Exemple: attentats du 11 septembre au World Trade Center (méthode inattendue)

Annexe 10: Feuille d'information pour les groupes de risques potentiels de la Confédération

Cette annexe présente et analyse quelques groupes de risques potentiels de l'administration fédérale. Leur compréhension claire et commune améliore leur gestion au sein de la Confédération.

Dans ce chapitre, les commentaires des différents groupes de risques sont structurés comme suit:

- *analyse des risques:* terminologie, subdivision éventuelle, interactions, etc.;
- *acteurs* concernés et leurs tâches dans le cadre du processus de gestion des risques;
- *collaboration* entre les acteurs;
- *centres de compétence* pour le groupe de risques, informations complémentaires;
- *mesures envisageables et meilleures pratiques*;
- *recommandations* du service de coordination Gestion des risques de la Confédération.

Les groupes de risques suivants sont analysés dans la présente annexe:

A) Risques liés à l'informatique

B) Risques liés aux infrastructures (hors risques liés à l'informatique)

C) Infractions contre le patrimoine

D) Risques liés au personnel

E) Régularité insuffisante du compte d'État

A) Risques liés à l'informatique

Analyse des risques

Les technologies de l'information et de la communication sont beaucoup utilisées de nos jours. Elles soutiennent les processus opérationnels des départements et des UA en vue de l'exécution des tâches. Tous les événements et évolutions liés à l'informatique qui ont des conséquences négatives sur l'exécution des tâches ou la réalisation des objectifs de la Confédération doivent être considérés comme des risques liés à l'informatique de l'administration fédérale. La défaillance ou le dysfonctionnement d'une infrastructure informatique constitue *en soi* un risque pour un fournisseur de prestations informatiques (FP), car la tâche principale de ce dernier consiste à exploiter des systèmes informatiques en faveur des bénéficiaires de ses prestations (BP). Pour pouvoir garantir une utilisation sûre de ses prestations, le FP dépend de fournisseurs fiables. Les risques liés à l'informatique apparaissent souvent sans distinction d'UA ou de département, ce qui rend leur gestion complexe.

On distingue quatre types d'atteintes aux systèmes informatiques. Concrètement, plusieurs atteintes peuvent survenir simultanément. Toutes interrompent ou entravent des processus opérationnels importants et peuvent avoir des conséquences financières et compromettre la réputation:

a. défaillance d'applications ou indisponibilité des données (risque lié à la disponibilité);
b. sortie de données sensibles (risque lié à la confidentialité);
c. manipulation des données (risque lié à l'intégrité);
d. modification insoupçonnée des données (traçabilité et intégrité).

Ces atteintes peuvent découler de plusieurs causes qui constituent à leur tour des risques. Ceux-ci sont énumérés ci-après de manière non exhaustive:

- activités d'espionnage;
- cyberattaques;
- programmes malveillants ou *malwares* (virus, chevaux de Troie, etc.);
- événements naturels (incendie, inondation, etc.);
- problèmes d'archivage et d'enregistrement;
- incompatibilité des systèmes informatiques;
- performances insuffisantes des systèmes;
- connaissances informatiques déficientes;
- utilisation négligente des données et applications par les collaborateurs;
- solutions informatiques isolées et risques d'interface (notamment en cas d'externalisation des prestations informatiques);
- droits d'accès trop étendus;
- technologies et plates-formes obsolètes ou ne bénéficiant plus d'un support technique;
- projets retardés à cause du développement de nouveaux systèmes informatiques;
- risques de dépendance lors du recours à des prestataires ou conseillers externes.

Normalement, le propriétaire des données analyse le besoin de protection pour chaque application informatique et pour les données qu'elle contient. Si celles-ci requièrent une protection élevée, il faut établir un concept de sûreté de l'information et de protection des données (concept SIPD). En général, le FP et le BP concluent ensuite un *service level agreement* (SLA) sur cette base.

Exemples d'interactions avec les risques liés à l'informatique:

- Les risques liés aux infrastructures informatiques du FP (incendie, inondation, panne de courant, etc.) peuvent entraîner la défaillance des systèmes informatiques et des applications du BP[98].
- Des mesures informatiques appropriées peuvent aussi réduire un risque de détournement de fonds.

[98] En général, la sécurité requise pour l'infrastructure des bâtiments est définie dans le SLA conclu entre le FP et l'Office fédéral des constructions et de la logistique (OFCL) ou armasuisse.

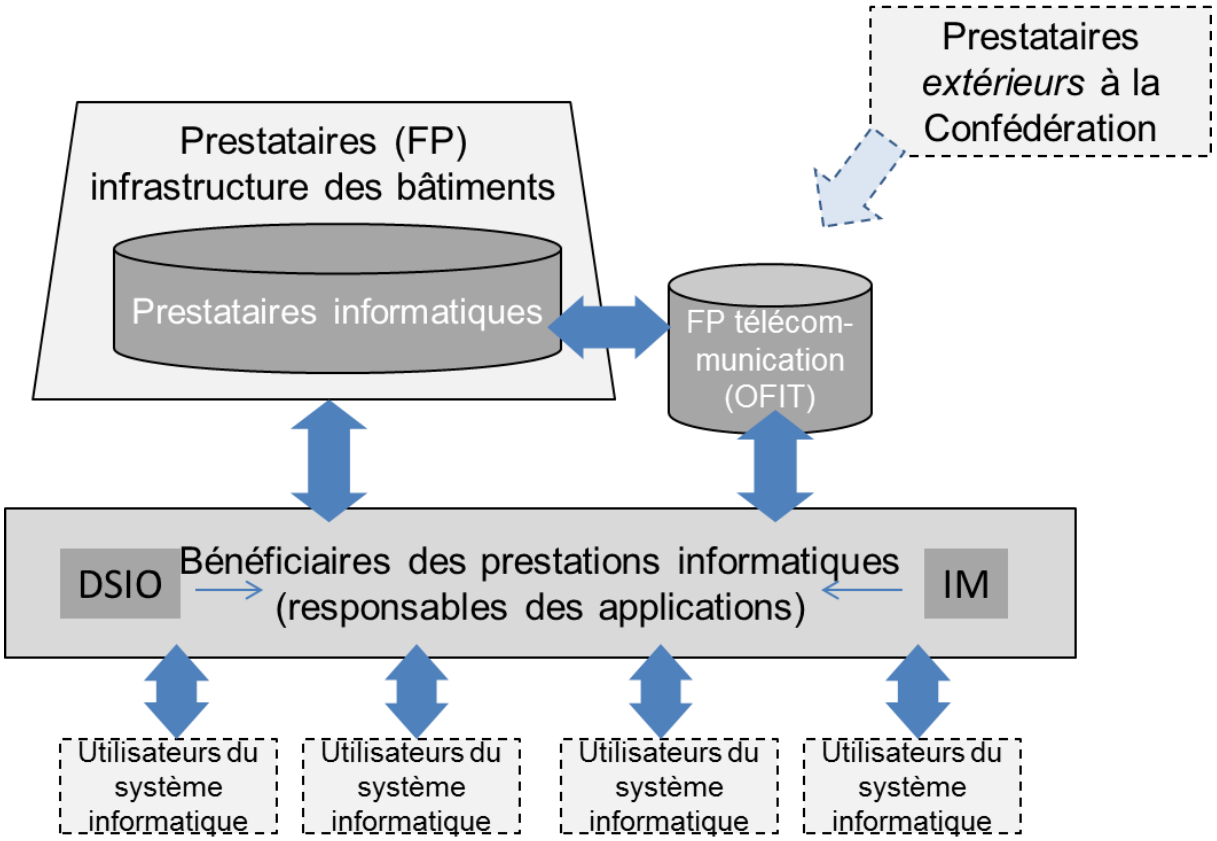
Acteurs et tâches dans le cadre du processus de gestion des risques	
FP (OFIT[99], BAC, CSI-DFJP, ISCeco, Informatique DFAE, CdC)	*Identification des risques:* notamment ceux liés aux infrastructures pour l'exploitation informatique *Évaluation des risques:* en particulier, évaluation de la probabilité et des conséquences sur la fourniture des prestations *Maîtrise des risques:* évaluation des mesures (avec le BP) et mise en œuvre au niveau du FP *Surveillance:* notamment des mesures techniques et des modifications dans l'environnement technique
BP / utilisateurs[100]	*Identification des risques:* notamment au niveau du personnel et de l'organisation *Évaluation des risques:* en particulier, conséquences sur l'exécution des tâches et sur les processus opérationnels de l'UA *Maîtrise des risques:* le BCM du BP comprend l'évaluation des mesures visant à réduire les dommages et à rétablir les processus ainsi que la décision correspondante (y c. définition de la tolérance au risque et des exigences en matière de sécurité); application des mesures par les utilisateurs *Surveillance:* notamment des utilisateurs informatiques
Infrastructure des bâtiments du FP pour l'informatique (OFCL, ar)	*Identification des risques:* en particulier, influence des risques liés aux infrastructures (par ex. coupures de courant) sur les risques liés à l'informatique *Évaluation des risques:* notamment, conséquences sur l'exécution des tâches du FP *Maîtrise des risques:* évaluation et mise en œuvre des mesures architecturales et techniques au niveau du bâtiment *Surveillance:* notamment des mesures architecturales et techniques au niveau du bâtiment
Utilisateurs informatiques[101]	*Identification des risques*: – *Évaluation des risques:* – *Maîtrise des risques:* mise en œuvre des mesures en matière de personnel et d'organisation (mots de passe, etc.) *Surveillance*: –
FP extérieurs à la Confédération (Swisscom, EWB, fournisseurs de logiciels, etc.)	Lorsque des contrats sont conclus avec des FP extérieurs à la Confédération, il est important de prendre en considération leur influence sur les systèmes de la Confédération et les risques inhérents ainsi que de réduire ces derniers dans la mesure du possible (convenir d'un BCM avec les fournisseurs).

[99] L'OFIT est non seulement le FP de plusieurs départements, mais également le principal prestataire de télécommunication (réseaux) de la Confédération. Il est également chargé de générer les certificats numériques (PKI = *public key infrastructure*) pour toute la Confédération.

[100] Les délégués à la sécurité informatique (DSID ou DSIO) et les gestionnaires d'intégration (*integration managers*, IM) sont à la disposition des BP / utilisateurs dans les départements et les offices afin de les conseiller sur la sécurité ou les applications informatiques.

[101] Les utilisateurs des systèmes informatiques peuvent également être extérieurs à l'administration fédérale (entreprises, population ou cantons pouvant accéder à l'informatique de la Confédération). Il faut en tenir compte dans la gestion des risques (notamment en termes de sécurité).

Collaboration entre les acteurs



Centres de compétence et informations complémentaires

Centres de compétence:

- ***Secteur TNI de la Chancellerie fédérale:*** définition et surveillance de la stratégie informatique de la Confédération; transformation numérique de l'administration fédérale; pilotage des services standard[102].
- ***Centre national pour la cybersécurité (NCSC):*** chargé par le Conseil fédéral de protéger les infrastructures vitales[103] contre les dangers du cyberespace. Centre de compétence et plate-forme d'échange sur les sujets concernant la sécurité informatique, notamment les programmes malveillants (virus, chevaux de Troie, etc.) issus d'Internet. *GovCERT.ch*, qui analyse les logiciels malveillants et fournit les résultats aux membres d'un groupe restreint de clients, est rattaché à MELANI[104].
- ***Office fédéral des constructions et de la logistique (OFCL):*** responsable des bâtiments de l'administration fédérale civile, y compris l'infrastructure informatique.
- ***Armasuisse (ar):*** responsable de tous les immeubles du DDPS, y compris l'infrastructure informatique.
- ***Office fédéral pour l'approvisionnement économique du pays (OFAE):*** notamment, examen stratégique des développements informatiques et adoption de mesures correspondantes[105].

[102] Par ex. bureautique, transmission de données

[103] Par infrastructures vitales, on entend les services dont la défaillance pendant plusieurs jours aurait de graves conséquences sur une grande partie de la population.

[104] GovCERT.ch concerne exclusivement la partie civile du réseau de la Confédération et les exploitants des infrastructures vitales, tandis que MilCERT assume certaines fonctions CERT (*computer emergency response team*) dans le domaine militaire.

[105] Le tremblement de terre et le tsunami consécutifs au Japon ont également affecté plusieurs fabricants de disques durs, entraî-

Autres informations et documents:

- ***Stratégie informatique de la Confédération***
- ***Ordonnance sur la transformation numérique et l'informatique (OTNI)***
- ***Ordonnance sur la protection contre les cyberrisques dans l'administration fédérale***

Mesures envisageables et meilleures pratiques

Un concept détaillé (en général, concept SIPD) détermine le besoin de protection requis et les mesures nécessaires. Il doit être mis à jour régulièrement (par ex. lorsqu'une nouvelle version d'une application est disponible). Voici quelques mesures envisageables pour réduire les risques liés à l'informatique:

Mesures concernant l'organisation et le personnel:

- Restriction de l'accès aux applications et aux données
- Restriction de l'accès à l'infrastructure informatique
- Adoption du principe du double contrôle
- Gestion sûre des mots de passe et utilisation de mots de passe forts
- Gouvernance informatique[106] (notamment, règles d'utilisation d'Internet et des logiciels)
- Élaboration d'un plan de continuité des opérations et exercice correspondant au cas où un événement imprévu se produirait

Mesures techniques

- Mise en place d'un pare-feu et d'un antivirus
- Sauvegarde régulière des données
- Enregistrement technique des changements apportés aux données (meilleure traçabilité)
- Chiffrement de données
- Procès-verbaux des événements informatiques (fichiers journaux ou *log files*; meilleure traçabilité de ces événements)
- Mise en place de contrôles automatiques dans les systèmes (contrôles de plausibilité)

Recommandations de l'AFF aux responsables de la gestion des risques des départements et des UA

1. ***Vérifier si une agrégation est nécessaire ou judicieuse:***
   - En général, les risques liés à l'informatique sont agrégés en cas d'interactions et de conséquences touchant plusieurs départements ou unités administratives, en particulier lorsque des processus opérationnels importants sont concernés. On s'assure ainsi de pouvoir comprendre les interactions, de saisir la portée globale et d'appliquer les mesures communes de manière coordonnée. Le service de coordination recommande une agrégation au niveau des prestataires, du département ou de la Confédération.
2. ***Vérifier si un pilotage central existe déjà:***
   - À la Confédération, l'UPIC assume une fonction de pilotage des risques liés à l'informatique dans différents domaines. Si ce n'est pas le cas, il faut procéder à une agrégation sous l'égide des responsables de la gestion des risques des prestataires, des responsables de la gestion des risques des départements ou du service de coordination de la Confédération.
3. ***Obtenir des informations et clarifier les tâches et les responsabilités:***
   - S'assurer que toutes les UA et tous les services concernés ont analysé et évalué

nant une pénurie au niveau mondial. L'OFCL prend des mesures préventives pour des événements de ce type (par ex. constitution de stocks).

[106] Voir ISACA, www.isaca.ch

les risques liés à l'informatique à agréger dans leur domaine.

- Vérifier ou s'assurer que les tâches, les responsabilités, les interfaces, etc. sont définies en ce qui concerne la gestion des risques (par ex. dans un SLA).
- Si nécessaire, diviser les risques liés à l'informatique en risques partiels pour pouvoir attribuer des responsabilités claires.
- Faire preuve d'une certaine réserve dans le regroupement de risques très différents liés à l'informatique. Par exemple, une agrégation sous le nom «Risques liés à l'informatique» n'est pas judicieuse (perte d'informations pertinentes concernant les risques; nécessité d'agir non manifeste).

4. ***Établir un rapport sur le risque agrégé:***
   - Classer les applications informatiques concernées par ordre de priorité, en fonction des conséquences prévisibles en cas d'apparition du risque. Cela permet de déterminer le *credible worst case* et l'ordre de priorité des mesures.
   - S'assurer que les interactions sont mises en évidence et ont été prises en compte dans l'analyse.
5. ***Échanger des informations:***
   - Assurer l'indispensable collaboration entre les délégués à la sécurité informatique des UA (DSIO) et les responsables de la gestion des risques des UA.
   - Veiller à une procédure uniforme pour l'analyse et l'appréciation des risques liés à l'informatique à agréger. Si nécessaire, ateliers avec tous les participants. Soutenir la coordination des mesures.
   - De manière générale, promouvoir l'échange d'informations (notamment entre le FP et le BP).

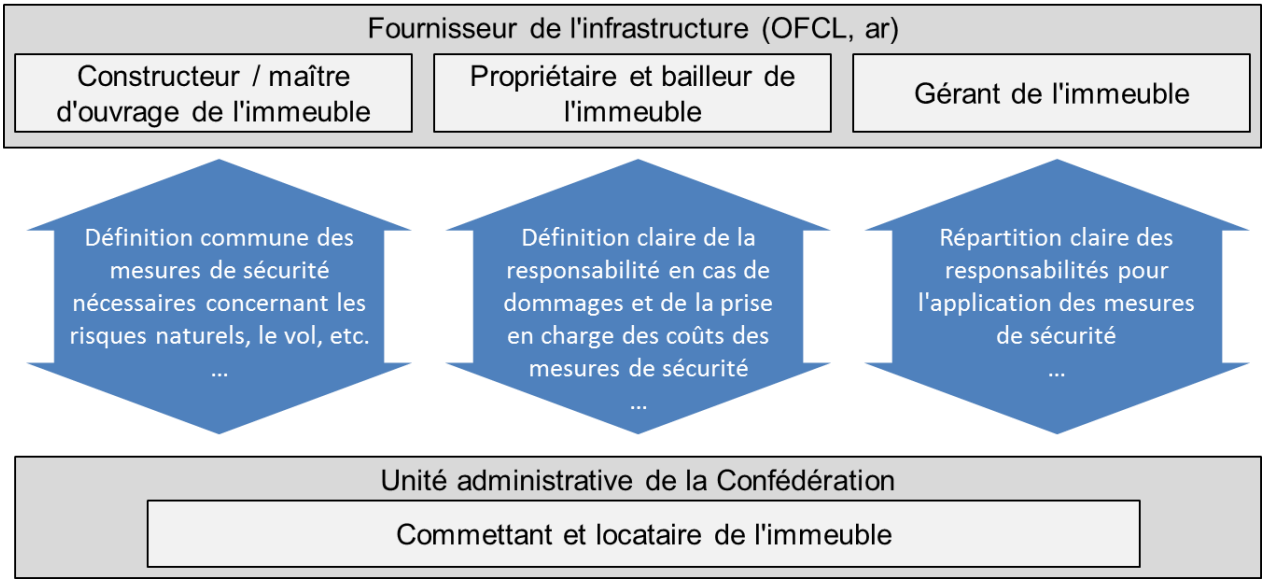
B) Risques liés aux infrastructures (hors risques liés à l'informatique)

Analyse des risques	
Par risques liés aux infrastructures, on entend les risques ayant des conséquences négatives sur l'infrastructure de l'administration fédérale. Cette infrastructure englobe en premier lieu les immeubles de l'administration fédérale, y compris l'infrastructure nécessaire à leur exploitation. Les installations informatiques[107], qui sont souvent exploitées par d'autres UO, sont explicitement exclues. L'expression «risques liés aux infrastructures» regroupe les événements suivants (liste non exhaustive): a. Événements naturels (crues, tremblements de terre, avalanches) b. Incendie c. Pannes de courant d. Effraction et vol e. Accès non autorisé (par. ex. dans les centres de calcul, etc.) f. Vandalisme Les dommages matériels ont des conséquences financières. En outre, il convient de prendre en considération et d'évaluer les interruptions affectant les activités et les processus des UA. Des blessures et des décès peuvent également être préjudiciables à la réputation. Compte tenu de la situation topographique et des utilisations, il faut analyser les risques liés aux infrastructures pour chaque immeuble. Les premières mesures de protection contre les risques liés aux infrastructures peuvent être prévues et appliquées dès la construction d'un immeuble. Cela suppose dès le début du projet une collaboration adéquate entre le maître d'ouvrage et les futurs utilisateurs du bâtiment. Ensuite, il faut définir clairement dans la gestion de l'immeuble qui prend en charge quels risques et qui met en œuvre quelles mesures techniques de protection. Exemples d'interactions avec les risques liés aux infrastructures: ▪ Un dommage aux infrastructures (en particulier, une coupure de courant) déclenche un risque pour les installations informatiques si l'infrastructure informatique principale de l'administration fédérale se trouve dans le bâtiment concerné.	
Acteurs et tâches dans le cadre du processus de gestion des risques	
Fournisseur de l'infrastructure (OFCL, ar)	*Identification des risques*: en particulier, risques à la construction et risques techniques du bâtiment *Évaluation des risques*: notamment, probabilité des risques techniques (incendie, etc.) *Maîtrise des risques*: propositions de mesures techniques et mise en œuvre de ces dernières *Surveillance:* des mesures de construction (et, parfois, d'organisation)
Service fédéral de sécurité (fedpol)	*Identification des risques*: dangers provoqués par des personnes *Évaluation des risques*: en particulier, évaluation de la probabilité d'un risque en fonction de la situation *Maîtrise des risques*: contrôle des accès aux bâtiments de la

[107] À l'exception des installations wi-fi, qui sont fournies par le prestataire de l'infrastructure du bâtiment.

	Confédération, barrières, protection des personnes, collaboration avec des services de sécurité privés et la police cantonale *Surveillance*: surveillance permanente de la situation en matière de sécurité pour les personnes et les bâtiments de la Confédération
UA en tant que locataire	*Identification des risques:* – *Évaluation des risques:* en particulier, conséquences sur les processus opérationnels de l'UA *Maîtrise des risques*: propositions de mesures pour la sécurité du bâtiment et des personnes et mise en œuvre *Surveillance*: des mesures organisationnelles notamment

Collaboration entre les acteurs



Centre de compétence et informations complémentaires

Office fédéral des constructions et de la logistique (OFCL): interne à la Confédération, la plate-forme clients de l'OFCL comprend des informations importantes sur les prestations (par ex. prestations de contrôle et de sécurité).

Mesures envisageables et meilleures pratiques

- Définition des issues de secours et des voies d'évacuation
- Plans de fermeture prédéfinis pour l'immeuble (protection du bâtiment)
- Installation d'alarmes (y c. vidéosurveillance)
- Préparation des procédures d'urgence, exercices d'évacuation[108]
- Contrôle des accès au bâtiment
- Préparation de l'organisation en cas d'urgence
- Extincteurs et sprinklers
- Systèmes de protection du bâtiment, etc.
- Vérification des assurances[109]

[108] Ces mesures sont mises en œuvre par le locataire / l'utilisateur.

[109] De manière générale, la Confédération ne conclut aucune couverture de ce type en raison du principe de l'auto-assurance. L'AFF est chargée des assurances.

Recommandations de l'AFF aux responsables de la gestion des risques des départements et des UA

1. ***Vérifier si une agrégation est nécessaire ou judicieuse:***
   - En général, les risques liés aux infrastructures devraient être agrégés en cas d'interactions touchant plusieurs départements ou unités administratives. Compte tenu de la proximité géographique de nombreux immeubles dans l'agglomération de Berne, le service de coordination recommande en particulier de considérer sur une base agrégée les risques inhérents aux pannes de courant[110] et aux événements naturels.
2. ***Vérifier si un pilotage centralisé existe déjà:***
   - Le pilotage centralisé des infrastructures de la Confédération est exécuté au niveau du prestataire (OFCL, ar). Une agrégation des risques devrait être mise en œuvre à ce niveau dans un premier temps.
3. ***Obtenir des informations et clarifier les tâches et les responsabilités:***
   - S'assurer que toutes les UA et tous les services concernés ont analysé et évalué le risque lié à l'infrastructure à agréger dans leur domaine.
   - Vérifier ou s'assurer que les tâches, les responsabilités, les interfaces, etc. sont définies pour la gestion des risques (par ex. dans un SLA).
4. ***Établir un rapport sur le risque agrégé:***
   - Classer les processus opérationnels concernés par ordre de priorité, en fonction de l'évaluation des conséquences prévisibles en cas d'apparition du risque. Cela permet de déterminer le *credible worst case* et l'ordre de priorité des mesures.
5. ***Échanger des informations:***
   - Promouvoir l'échange d'informations entre les prestataires et les UA en tant qu'utilisateurs.

[110] Le groupe de travail interdépartemental «Priorisation des bâtiments fédéraux en cas de coupure de courant» a été mis en place pour les interruptions prolongées.

C) Infractions contre le patrimoine

Analyse des risques
Par ***corruption***, on entend l'abus d'une position de confiance pour obtenir un avantage matériel ou immatériel injustifié. Les pots-de-vin ainsi que l'acceptation et l'octroi d'avantages constituent des formes concrètes de corruption. Un ***abus de confiance*** désigne la captation illicite de valeurs patrimoniales par des collaborateurs de l'administration fédérale. En cas de ***gestion déloyale des intérêts publics***, les employés lèsent dans un acte juridique les intérêts publics qu'ils ont pour mission de défendre, dans le dessein de se procurer ou de procurer à un tiers un avantage illicite. On parle de ***délit d'initiés*** lorsqu'un collaborateur utilise des informations non publiques pour son enrichissement personnel. Outre les conséquences financières de ces risques (par ex. paiement de prix excessifs pour un marché public), le risque de réputation, notamment, est considérable. Les activités administratives ne sont pas toutes exposées au même risque de corruption ou d'abus de confiance. Par exemple, l'octroi de marchés publics, les contacts avec des États mal notés au niveau international en matière de lutte contre la corruption, la fiscalité, l'adjudication de mandats de révision ou de surveillance, l'attribution de concessions, le contrôle des frontières ainsi que la justice et la police sont des domaines particulièrement exposés à la corruption. Les infractions contre le patrimoine concernent davantage les services où des flux financiers et des paiements sont gérés et déclenchés. Par exemple, l'identification insuffisante d'un collaborateur vis-à-vis de son employeur, son manque de loyauté ou un anonymat accru dans l'organisation, l'insatisfaction au travail, la frustration, l'absence de motivation, des contrôles insuffisants ou une organisation vague des procédures et des processus constituent un terrain fertile en la matière. *Interactions*: ▪ Les cas constatés de corruption et d'abus de confiance peuvent se traduire par un sentiment d'insécurité parmi le personnel; d'autres manquements dans les procédures de l'organisation peuvent également être mis en évidence.

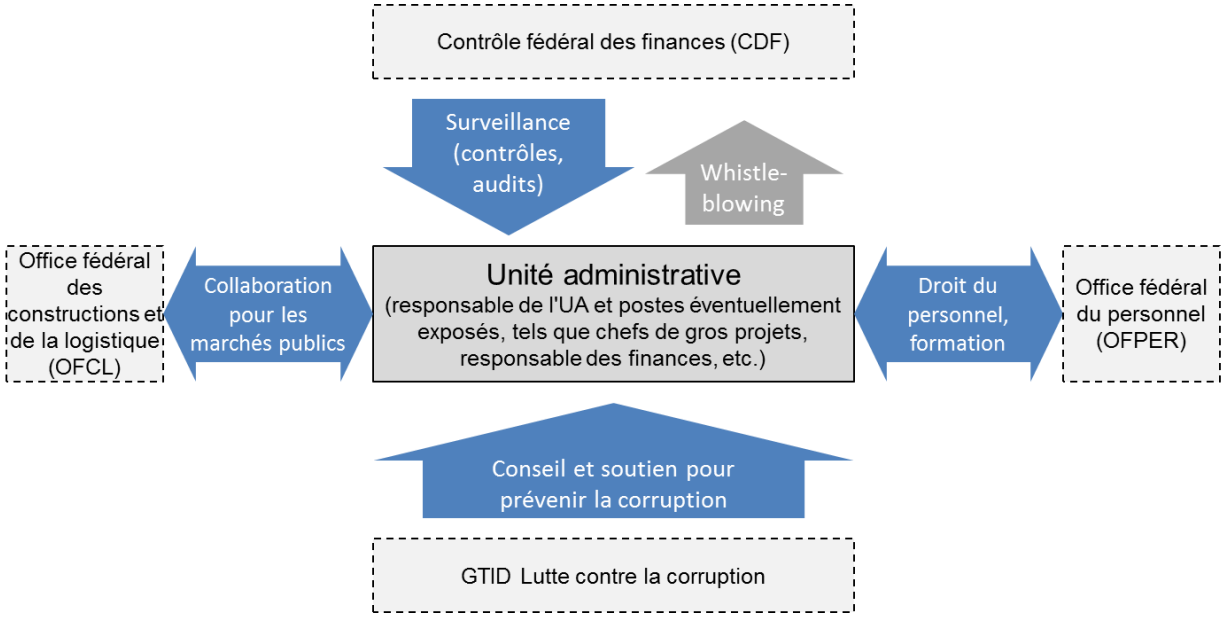
Acteurs et tâches dans le cadre du processus de gestion des risques	
Unité administrative (en particulier responsable de l'UA, mais également chefs de gros projets, responsables des services Finances, Compliance et Risques, etc.)	*Identification des risques:* oui, notamment identification des postes exposés *Évaluation des risques:* oui *Maîtrise des risques:* oui, responsable de la définition et de l'application des mesures *Surveillance:* oui
Contrôle fédéral des finances (CDF)[111]	*Identification des risques:* oui, par exemple en tant que lanceur d'alerte (*whistleblower*) de la Confédération *Évaluation des risques:* oui *Maîtrise des risques:* recommandations pour réduire les risques de corruption et d'abus de confiance *Surveillance:* audits / révisions[112]
GTID Lutte contre la corruption (sous l'égide du DFAE)	*Identification des risques:* - *Évaluation des risques:* -

[111] Voir http://www.efk.admin.ch/index.php?option=com_content&view=article&id=223&Itemid=238&lang=fr

[112] Le CDF effectue des audits non seulement en matière de corruption, mais également dans de nombreux autres domaines (par ex. sécurité informatique, SCI, etc.).

	Maîtrise des risques: en particulier, propositions de *stratégies* concernant les mesures[113] *Surveillance:* oui, comité du GTID
Office fédéral des constructions et de la logistique (OFCL) et armasuisse (ar)	*Identification des risques:* au niveau des marchés publics *Évaluation des risques:* - *Maîtrise des risques:* mise en œuvre des mesures de réduction du risque de corruption au niveau des marchés publics *Surveillance:* -
Office fédéral du personnel (OFPER)	*Identification des risques:* - *Évaluation des risques:* - *Maîtrise des risques:* oui, mesures à l'échelle de la Confédération (directives, formation, etc.) *Surveillance:* -

Collaboration entre les acteurs[114]



Centres de compétence et informations complémentaires

En matière de corruption:

- Le ***Groupe de travail interdépartemental (GTID) pour la lutte contre la corruption*** élabore des stratégies pour combattre la corruption au niveau national et international et lance des campagnes de sensibilisation et d'information.
- Chargé des marchés publics de la Confédération, l'***Office fédéral des constructions et de la logistique*** (OFCL) a de l'expérience dans la prévention de la corruption[115]. Son site Internet comprend des conseils sur les marchés publics ainsi qu'une feuille d'information sur la prévention de la corruption et des conseils correspondants.

[113] Voir le rapport de mars 2011 au Conseil fédéral et les mesures pour prévenir la corruption

[114] L'OFPER informe sur les règles de comportement générales (code de conduite) des employés et des supérieurs hiérarchiques dans le cadre de formations sur le droit du personnel. Les départements et les offices diffusent les informations en leur sein grâce à des directives spécifiques, conformément à l'art. 94*d* OPers.

[115] La Commission des achats de la Confédération (CA) et le Centre de compétence des marchés publics (CCMP) sont également rattachés à l'OFCL.

Informations complémentaires:

- ***GIMAP:*** plate-forme d'information et guide interactif sur les marchés publics
- La ***loi sur le personnel de la Confédération (LPers)*** et l'***ordonnance sur le personnel de la Confédération (OPers)*** fixent des règles de conduite pour les collaborateurs (par ex. art. 20, 21, al. 3, et 23 LPers, art. 91 à 94*d* OPers).
- D'autres commentaires figurent dans le ***code de comportement de l'administration fédérale***[116] et dans les ***lignes directrices relatives aux activités accessoires et aux charges publiques*** (OFPER)[117].
- Brochure «Prévention de la corruption et ‹whistleblowing›»[118]

Mesures envisageables et meilleures pratiques

- Mise en place d'un service de *whistleblowing*[119] au sein du CDF et communication à ce sujet
- Code de comportement de l'administration fédérale et règles de conduite des départements et offices reposant sur l'art. 94*d* OPers (règles de récusation, acceptation de cadeaux, etc.)[120]
- Information régulière, mesures de sensibilisation (notamment du GTID Lutte contre la corruption) et formation des collaborateurs[121]
- Audits et contrôles aléatoires
- Contrôles internes, dont principe du double contrôle[122] (en l'espèce, une vérification tant formelle que matérielle est importante)
- Contrôles et mesures techniques des systèmes (par ex. restriction des accès et conditions de validation, signature électronique)
- Vérification matérielle des marchandises et des prestations (pour les paiements élevés)
- Séparation cohérente des fonctions
- Contrôles de sécurité relatifs aux personnes pour les postes exposés
- Obtention de références et vérification des registres officiels lors de nouvelles embauches
- Rôle de modèle des supérieurs hiérarchiques
- Renforcement de la loyauté des collaborateurs
- Mise en place d'une obligation de dénoncer et d'un droit de dénoncer pour les collaborateurs (art. 22*a* LPers)

Mesures spécifiques visant à réduire la corruption:

- Déclarations d'impartialité des personnes exposées
- Obligation de conclure des contrats écrits pour les acquisitions
- Procédure d'acquisition centralisée et transparente
- Clause d'intégrité dans les contrats conclus avec les fournisseurs
- Justification et documentation des procédures et des décisions d'adjudication
- Évaluation des risques lors de l'octroi de mandats
- Application cohérente des règles de récusation

[116] FF **2012** 7307

[117] Des règles de comportement plus spécifiques ont été définies dans plusieurs UA (par ex. AFF).

[118] Voir https://www.epa.admin.ch/epa/fr/home/documentation/publications.html et http://www.admin.ch/ch/f/rs/c172_220_1.html

[119] Voir http://www.efk.admin.ch/index.php?option=com_content&view=article&id=223&Itemid=238&lang=fr

[120] Voir https://www.epa.admin.ch/epa/fr/home/documentation/publications.html et http://www.admin.ch/ch/f/rs/c172_220_1.html

[121] Sur l'intégrité, par ex., à travers l'obligation de dénoncer et le droit de signaler selon la LPers

[122] En vertu de ce principe, les décisions importantes ne peuvent et ne doivent pas être prises par une seule personne et les activités critiques ne peuvent et ne doivent pas être exécutées par une seule personne afin de réduire le risque d'erreur ou d'abus.

Recommandations de l'AFF aux responsables de la gestion des risques des départements et des UA

1. ***Vérifier si une agrégation est nécessaire ou judicieuse*:**

- Différentes mesures sont déjà appliquées de manière centralisée (OFPER, CDF, OFCL, etc.). Il n'y a pas d'interactions touchant plusieurs départements ou UA. Une agrégation mettrait essentiellement en évidence l'importance globale du groupe de risques. La gestion des risques incombe toutefois aux UA. Le service de coordination de l'AFF ne recommande pas l'agrégation.

2. ***Vérifier si un pilotage centralisé existe déjà*:**

- Il existe plusieurs centres de compétence (voir ci-dessus). Ils ont une fonction consultative, mais ne prennent pas en considération le risque agrégé.

D) Risques liés au personnel, notamment pertes de savoir-faire

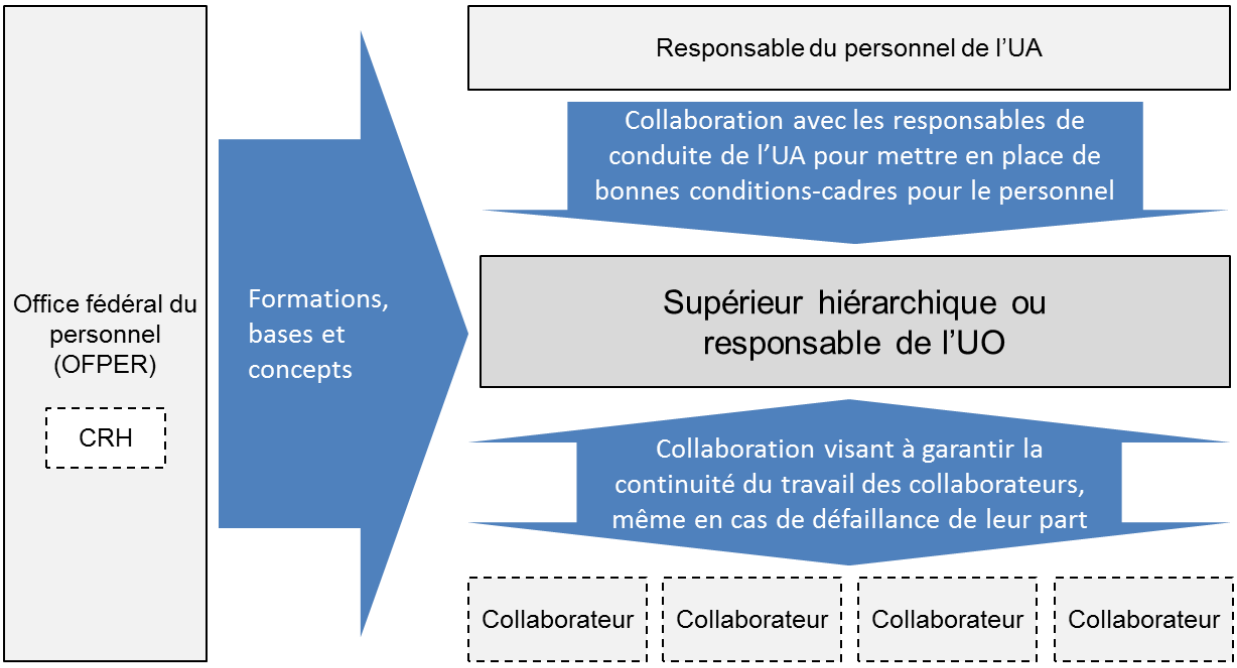
Analyse des risques
La ***défaillance de personnes-clés*** (par ex. pour cause de maladie, d'accident, de démission ou pour d'autres raisons) ayant un savoir-faire spécialisé peut perturber la marche des affaires de l'UA, provoquer une interruption des principaux processus et générer des coûts supplémentaires. En général, un ***manque de savoir-faire*** apparaît de façon insidieuse dans une UA lorsque les conditions-cadres ne sont pas intéressantes à moyen terme pour le personnel, que la formation continue des collaborateurs est déficiente, qu'il y a une pénurie de personnel qualifié sur le marché, etc. D'autres risques existent dans le domaine du personnel: connaissances spécialisées concentrées auprès d'un petit nombre de personnes, documentation lacunaire ou insuffisante des principaux processus, absence de gestion des connaissances, recours excessif aux conseillers externes, etc. La célérité d'une perte de savoir-faire (directement en cas de décès; temps équivalent au délai de congé lors d'une démission; planification en cas de départ à la retraite) détermine l'ampleur des conséquences négatives pour l'UA. *Interactions*: ▪ La défaillance d'un collaborateur peut se traduire, pour ses collègues, par des difficultés à gérer la charge de travail et, dans un scénario négatif, par d'autres départs à moyen terme.

Acteurs et tâches dans le cadre du processus de gestion des risques	
Collaborateur d'une UA	*Identification des risques:* identification des processus et du savoir-faire pour lesquels une documentation et une réglementation de la suppléance est nécessaire ou judicieuse[123] *Évaluation des risques: -* *Maîtrise des risques:* évaluation des mesures envisageables avec le supérieur hiérarchique et mise en œuvre *Surveillance: -*
Personnes chargées de la conduite / supérieur hiérarchique du collaborateur	*Identification des risques:* identification des processus et du savoir-faire pour lesquels une documentation et une réglementation de la suppléance est nécessaire ou judicieuse *Évaluation des risques:* oui; évaluer les conséquences de la défaillance du savoir-faire spécialisé pour l'UO *Maîtrise des risques:* évaluation des mesures envisageables (avec les collaborateurs) et décisions à ce sujet (y c. définition de la tolérance au risque) *Surveillance:* oui
Responsable du personnel de l'UA	*Identification des risques:* identification des lacunes dans le recrutement et la conduite de l'UA *Évaluation des risques: -* *Maîtrise des risques:* évaluation des mesures envisageables au sein de l'UA et mise en œuvre

[123] À cet égard, il faut tenir compte du fait que les collaborateurs concernés n'ont guère intérêt à partager ou à documenter leur savoir-faire spécialisé, qui fait partie intégrante de leur qualification et de leur valeur sur le marché. C'est la raison pour laquelle la gestion de ce risque incombe davantage aux personnes chargées de la conduite et au responsable du personnel de l'UO.

	Surveillance: de l'impact de ces mesures
Office fédéral du personnel (OFPER), y compris la Conférence des ressources humaines (CRH)[124]	*Identification des risques:* pour les risques de la Confédération concernant le recrutement et l'attachement des collaborateurs *Évaluation des risques:* - *Maîtrise des risques:* évaluation des mesures envisageables au niveau de la Confédération et mise en œuvre *Surveillance:* -

Collaboration entre les acteurs



CRH = Conférence des ressources humaines

Centre de compétence et informations complémentaires

Office fédéral du personnel (OFPER): élabore les bases et les concepts destinés à la Confédération (par ex. sur l'attachement des collaborateurs); intègre la perte de savoir-faire dans plusieurs formations (pour les cadres), etc.

- Documents de base: stratégie concernant le personnel de l'administration fédérale

[124] Composée des responsables du personnel des départements et de la ChF, la CRH joue un rôle essentiel dans la coordination et la mise en œuvre de la politique du personnel du Conseil fédéral.

Mesures envisageables et meilleures pratiques

- Suppléances pour les fonctions ou postes les plus importants (grâce à leur identification ou à celle des détenteurs de savoir)
- Mise en place d'une gestion des connaissances afin que le savoir-faire soit réparti auprès de plusieurs personnes
- Marketing du personnel pour le recrutement de collaborateurs qualifiés (centralisé auprès de l'OFPER)
- Mesures pour accroître l'attachement des collaborateurs (*retention management*): environnement de travail moderne, conditions de travail compétitives, modèles de développement de carrière, modèles de compétences, etc. (centralisées auprès de l'OFPER)
- Documentation compréhensible des processus opérationnels
- Promotion des échanges informels entre les collaborateurs
- Recours modéré aux conseillers externes
- Planification précoce de la succession lors de départs à la retraite des détenteurs du savoir

Recommandations de l'AFF aux responsables de la gestion des risques des départements et des UA

1. ***Vérifier si une agrégation est nécessaire ou judicieuse:***
   - Différentes mesures sont déjà appliquées de manière centralisée (OFPER, CRH). Il n'y a pas d'interactions touchant plusieurs UA. Une agrégation permettrait essentiellement de mettre en évidence l'importance globale du groupe de risques au niveau du département et de la Confédération. La gestion de ces risques incombe toutefois à chaque UA. Le service de coordination de l'AFF ne recommande pas l'agrégation.
2. ***Vérifier si un pilotage centralisé existe déjà:***
   - Un centre de compétence (OFPER) existe; il a une fonction purement consultative et n'exécute aucune agrégation des risques.
3. ***Échanger des informations:***
   - Un échange régulier entre les responsables du personnel des UA peut contribuer à la communication d'approches et d'idées visant à réduire ces risques ainsi qu'à la diffusion des meilleurs exemples au sein de l'administration fédérale.

8

E) SCI insuffisant pour garantir la régularité du compte d'État

Analyse des risques

La comptabilité de l'administration fédérale est organisée de manière décentralisée. Chaque UA saisit ses opérations comptables et est dès lors chargée de respecter les prescriptions légales sur la régularité du compte d'État. En revanche, le rapport financier (établissement du compte d'État) est réalisé centralement par l'AFF.

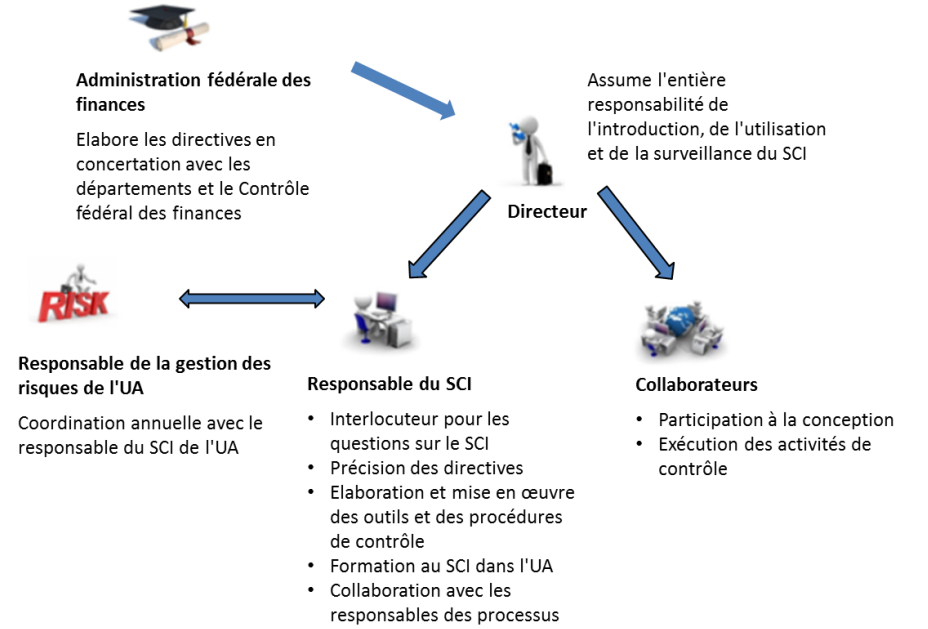
La régularité du compte d'État englobe les aspects suivants:

- Principes régissant la tenue des comptes (art. 38 LFC et 28 OFC):
  - universalité: toutes les opérations financières et tous les éléments comptables doivent être enregistrés intégralement et par période;
  - véracité: les écritures comptables doivent correspondre aux faits et doivent être effectuées selon les directives de l'AFF;
  - ponctualité: la comptabilité doit être tenue à jour et les mouvements de fonds doivent être enregistrés chaque jour. Les opérations doivent être consignées par ordre chronologique;
  - traçabilité: les opérations doivent être enregistrées de manière claire et compréhensible. Les corrections doivent être marquées comme telles et les écritures comptables doivent être attestées par des pièces justificatives.
- Principes régissant l'établissement des comptes (art. 47 LFC et 54 OFC):
  - importance: il convient de présenter toutes les informations nécessaires pour permettre une appréciation rapide et complète de l'état de la fortune, des finances et des revenus;
  - clarté: les informations doivent être claires et compréhensibles;
  - permanence des méthodes comptables: les principes régissant l'établissement du budget ainsi que la tenue et l'établissement des comptes doivent dans toute la mesure du possible rester inchangés sur une longue période;
  - produit brut: les charges sont inscrites au budget séparément des revenus et les dépenses d'investissement séparément des recettes d'investissement, sans aucune compensation, chacun d'entre eux y figurant pour son montant intégral.

Le système de contrôle interne (SCI) est un instrument central adéquat pour garantir la régularité de la tenue et de l'établissement des comptes dans les UA. S'il fait défaut ou si ses éléments principaux sont déficients, le rapport financier publié par l'administration fédérale, qui présente les comptes de la Confédération aux citoyens et sert de base de décision aux milieux politiques, aux investisseurs et aux agences de notation, risque de comporter des erreurs importantes. Celles-ci seraient non seulement préjudiciables à la réputation, mais fausseraient également cette base décisionnelle.

Acteurs et tâches dans le cadre du processus de gestion des risques	
Échelon de conduite supérieur (directrice / directeur)	*Identification des risques:* oui *Évaluation des risques:* oui *Maîtrise des risques:* oui; responsable du SCI dans son domaine de compétence *Surveillance:* oui
Responsable du SCI	*Identification des risques:* oui *Évaluation des risques:* oui; les matrices de contrôle des risques sont régulièrement vérifiées et renouvelées *Maîtrise des risques:* non; au plus pour son domaine de compétence en tant que supérieur hiérarchique *Surveillance:* oui; coordonne les activités de surveillance au sein de l'UA
Responsable d'un processus opérationnel ayant une incidence financière	*Identification des risques:* oui; en tant que supérieur hiérarchique, le responsable du processus connaît les risques inhérents à son processus *Évaluation des risques:* oui; les matrices de contrôle des risques sont régulièrement vérifiées et renouvelées *Maîtrise des risques:* oui; grâce à l'application des mesures SCI dans son domaine de compétence en tant que supérieur hiérarchique *Surveillance:* oui; surveille la gestion des risques dans son domaine de compétence
Collaborateurs des processus opérationnels ayant une incidence financière	*Identification des risques:* non *Évaluation des risques:* non *Maîtrise des risques:* oui; lors des contrôles du travail quotidien *Surveillance:* non
AFF	*Identification des risques:* non *Évaluation des risques:* non *Maîtrise des risques:* non *Surveillance:* non
CDF	*Identification des risques:* oui *Évaluation des risques:* oui *Maîtrise des risques:* non *Surveillance:* non

Collaboration entre les acteurs



Contrôle fédéral des finances:
Examine régulièrement le SCI dans les unités administratives, cet examen faisant partie intégrante de l'audit du compte d'Etat.

Centre de compétence et informations complémentaires

AFF: élabore les bases et les directives de la Confédération sur la tenue et l'établissement des comptes ainsi que sur le SCI; intègre ces thèmes aux cours et aux formations.

- Documents de base: manuel de gestion budgétaire et de tenue des comptes, chap. 4.8

Mesures envisageables et meilleures pratiques

- En vertu de l'art. 39 LFC, un système de contrôle interne efficace et approprié doit être mis en place dans les UA de l'administration fédérale centralisée pour garantir la régularité de la tenue et de l'établissement des comptes dans le compte d'État. Les mesures requises sont décrites dans le guide SCI de l'AFF, qui figure au chap. 4.8 du manuel de gestion budgétaire et de tenue des comptes.

Recommandations de l'AFF aux responsables de la gestion des risque des départements et des UA

L'AFF recommande d'évaluer régulièrement, dans le cadre de la gestion des risques de l'UA, le risque d'irrégularités dans la tenue et l'établissement des comptes ainsi que de vérifier l'existence et le fonctionnement durable du SCI dans l'UA.

Annexe 11: Modèle «Stratégie en matière de risques» pour les départements / la ChF et les UA

Généralités:

1. *Une stratégie en matière de risques doit être rédigée de manière claire et concise (max. deux pages A4). Elle précise comment la politique des risques du Conseil fédéral doit être mise en œuvre dans une UO et quels objectifs doivent être atteints.*
2. *Les directives du Conseil fédéral et de l'AFF concernant la gestion des risques ne doivent pas être reprises dans la stratégie en matière de risques. Cette dernière peut cependant y renvoyer.*
3. *Le présent modèle sert d'aide. Il doit être adapté aux besoins de l'UO concernée.*

1 Objet

La présente stratégie en matière de risques montre comment la direction entend mettre en œuvre les directives du Conseil fédéral du 24 septembre 2010 sur la politique de gestion des risques menée par la Confédération. La gestion des risques soutient la direction dans le cadre de l'exécution des tâches et de l'atteinte des objectifs.

2 Buts de la gestion des risques

Nos principaux buts sont:

– but n° 1:

– but n° 2:

– but n° x:

3 Principes de mise en œuvre

Nous appliquons les principes suivants lors de la mise en œuvre de la stratégie:

– Nous tenons compte des risques liés au travail de conduite à tous les échelons et intégrons la gestion des risques dans tous les processus relatifs à la stratégie et à la planification.

– La direction mène au moins deux fois par année, dans le cadre du rapport sur les risques, un dialogue structuré portant sur l'exposition aux risques; elle se concentre sur les principaux risques et examine la mise en œuvre et l'efficacité des mesures.

– La direction examine au moins tous les quatre ans sa gestion des risques. Elle vérifie de fond en comble le portefeuille des risques et des mesures, évalue les nouveaux groupes de risques qui pourraient apparaître à moyen terme et la collaboration avec la gestion des risques.

– Le responsable des risques de l'UA échange régulièrement avec les responsables des autres domaines d'aide à la conduite sur la situation en matière de risques.

4 Maîtrise des risques

Nous gérons nos risques de la manière suivante:

– Nous évaluons les mesures visant à réduire les risques qui ont été identifiés. La charge découlant de ces mesures ne doit pas être supérieure aux avantages que ces dernières peuvent apporter. Les décisions incombent à la hiérarchie et sont documentées.

– Le propriétaire du risque surveille la mise en œuvre et l'efficacité des mesures qui ont été prises.

– Pour chaque risque, nous définissons l’objectif de réduction à atteindre au moyen des mesures qui ont été prises.
– En ce qui concerne le contrôle de gestion des mesures, la direction est informée dans le cadre du rapport sur les risques.

5 Fonctions et responsabilités

La direction dispense des conseils en matière de gestion des risques et adopte deux fois par année un rapport sur les risques. Ce dernier est préparé par le responsable de la gestion des risques de l’UA en collaboration avec les propriétaires des risques et après consultation des responsables des mesures.

Conformément à son cahier des charges, le responsable de la gestion des risques de l’UA dispose de <xx> % pour remplir ses tâches. Dans cette fonction, il a un contact direct avec la direction de l’office et les chefs de division. Pour le reste, les tâches et responsabilités liées à la gestion des risques sont réglées au ch. 3 des directives de l’AFF sur la gestion des risques de la Confédération.

6 Dispositions finales

La présente stratégie en matière de risques entre en vigueur le <date>. Elle sera réexaminée au plus tard en <année> et présentée à la direction pour décision.

Lieu/date/signature du directeur / de la directrice d’office