Version du 15 février 2019

**▬▬▬▬▬▬▬▬▬▬▬**

# Conseil par rapport aux informations à transmettre par les entités sollicitant un agreement comme entreprise d’investissement en relation avec les systèmes d’information dans la section « Informations sur l’organisation de l’entreprise»

Conformément au règlement d’exécution (UE) [2017/1945](https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32017R1945&qid=1532531266570&from=FR) de la Commission du 19 juin 2017 la CSSF a émise un formulaire en ligne avec l’annexe I pour les entreprises d’investissement sollicitant un agrément à la CSSF.

Le présent document d'orientation a pour objet de préciser les informations à fournir dans la section "Informations sur l'organisation de l’entreprise", plus précisément en ce qui concerne les demandes d'informations référencées dans le règlement délégué (UE) [2017/1943](https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32017R1943&qid=1532531336838&from=FR) de la Commission du 14 juillet 2016, Article 6, en ce qui concerne les éléments liés aux Systèmes d’informations.

Nous tenons à souligner que ces orientations se concentrent uniquement sur les aspects informatiques à communiquer au titre de l'article 6, et plus précisément au titre de l'article :

* (c) (ii) la description des ressources (en particulier humaines et techniques) allouées aux différentes activités envisagées;
* (e) la liste des fonctions, services ou activités externalisés (ou destinés à l'être) et la liste des contrats passés ou envisagés avec des prestataires extérieurs ainsi que des ressources (notamment humaines et techniques, et le système de contrôle interne) affectées au contrôle des fonctions, services ou activités externalisés; si il s’agit d’un service informatique
* (g) une description des systèmes de contrôle des activités de l'entreprise, y compris, le cas échéant, des systèmes de sauvegarde, ainsi que des systèmes et contrôles des risques lorsque l'entreprise souhaite recourir au trading algorithmique et/ou fournir un accès électronique direct;
* (i) des précisions sur les systèmes permettant d'évaluer et de gérer les risques de blanchiment de capitaux et de financement du terrorisme;
* (j) les plans de continuité de l'activité, notamment en ce qui concerne les systèmes et les ressources humaines (personnel clé);

Afin de faciliter la fourniture des informations susmentionnées, nous vous fournissons le formulaire ci-dessous que nous vous encourageons vivement à remplir.

# Formulaire renseignant des informations à transmettre en relation avec les systèmes d’information dans le cadre d’une demande d’agrément comme entreprise d’investissement dans la section « Informations sur l’organisation de l’entreprise»

|  |  |
| --- | --- |
| Votre référence interne :*[insérer votre référence interne]* | *Référence de l’administration :* |
|  |

#### Cadre administratif :

1. Dénomination légale de l’entité :

|  |  |
| --- | --- |
|  | *Cadre réservé à l’administration* |
|  |

1. Nom du ou des directeur(s) / dirigeant(s) autorisé(s) ayant revu et approuvé ce document :

|  |  |
| --- | --- |
|  | *Cadre réservé à l’administration* |
|  |

1. Date de soumission à l’autorité compétente :

|  |  |
| --- | --- |
|  | *Cadre réservé à l’administration* |
|  |

#### Stratégie et organisation IT :

1. Veuillez fournir une description synthétique de l’organisation informatique (organigramme, nombre de personnes, rôles et responsabilités clé dans le domaine IT et de la sécurité de l’information) et de la stratégie informatique retenue (in-house ou sous-traitance informatique, complète ou partielle).

|  |  |
| --- | --- |
| *[insérer texte]* | *Cadre réservé à l’administration* |
|  |

1. En cas de sous-traitance, veuillez :
* spécifier les activités informatiques sous-traitées ainsi que les détails sur le(s) sous-traitant(s) (notamment: dénomination, appartenance au même groupe que l’entité à agréer, localisation, surveillance par une autorité de contrôle, prestataire agréé PSF de support).
* spécifier les systèmes et activités IT qui resteront à Luxembourg, sous votre responsabilité (i.e. non concernés par de la sous-traitance).
* confirmer qu’un contrat de sous-traitance et/ou SLA est signé entre les deux parties et est en ligne avec les meilleures pratiques professionnelles et prévoit notamment :
	+ description des services fournis par votre prestataire
	+ description de vos responsabilités et de celles de votre prestataire
	+ intégration de vos besoins dans les plans BCP/DRP et plans de backup de votre contractant
	+ conditions pour la révocation du contrat et dans ce cas des mesures prévues afin de garantir la continuité des services (i.e. transfert à un autre prestataire de service ou reprise par vos soins)
	+ gestion de la relation de sous-traitance (i.e. réunions/rapports réguliers entre votre contractant et vous, processus de gestion des incidents, KPI, etc.)
	+ conditions de sous-traitance en cascade pour votre contractant (i.e. nécessité de votre autorisation préalable)
	+ confidentialité et sécurité des données
	+ clause d’audit : possibilité pour les auditeurs internes et externes et pour votre superviseur (la CSSF) d’effectuer des audits sur site.
* préciser la personne de l’entité à agréer qui est responsable de la sous-traitance.
	+ indiquer les contrôles implémentés pour assurer la qualité des services fournis et leur conformité à réglementation applicable.

|  |  |
| --- | --- |
| *[insérer texte]* | *Cadre réservé à l’administration* |
|  |

1. Veuillez confirmer que l'entité à agréer sera en charge et activement impliquée dans la gestion des accès (par ex. validation des demandes d’accès et revue des profils d’accès, conformément aux principes du « need to know » et « least privilege ») ainsi que dans la gestion des changements sur ses systèmes informatiques (i.e. les changements pouvant impacter les données de l’entité à agréer doivent être approuvés par l’entité).

|  |  |
| --- | --- |
| *[insérer texte]* | *Cadre réservé à l’administration* |
|  |

1. Veuillez clarifier si le système comptable est localisé au Luxembourg ou à l’étranger. Dans le cas où ce système est situé à l’étranger, afin de réduire le risque pour l’entité à agréer de ne pas être capable d’établir le bilan et le compte de pertes et profits, veuillez préciser si une copie des documents comptables (y inclus le grand livre et le journal comptable) sera disponible au Luxembourg.

|  |  |
| --- | --- |
| *[insérer texte]* | *Cadre réservé à l’administration* |
|  |

#### Description des systèmes IT :

1. Veuillez préciser les systèmes informatiques « métiers » supportant les activités « métiers » prestées (par ex. logiciels d’administration de fonds, agent de transfert, comptabilité des sociétés domiciliées, réconciliation, gestion de portefeuille, de gestion de la relation client, Intranet, Site Web consultatif ou transactionnel,) et les systèmes informatiques « de support » utilisés pour l’organisation et l’administration de l’entité à agréer (par ex. système comptable , système de reporting CSSF, serveurs de messagerie, serveurs de fichiers internes et outils de gestion des ressources informatiques tel qu’Active Directory).

|  |  |
| --- | --- |
|  *[insérer texte]* | *Cadre réservé à l’administration* |
|  |

1. Veuillez fournir un tableau récapitulatif contenant les éléments suivants, pour chaque application listée au point A :
* description succincte de l’application,
* indication si l’application contient des données confidentielles (en précisant le type de données confidentielles),
* le vendeur de l’application (si elle n’est pas développée in-house),
* le site primaire (production) d’hébergement de l’application,
* le site secondaire (disaster recovery) d’hébergement de l’application,
* l’entité en charge de l’infrastructure IT,
* l’entité en charge de l’exploitation IT,
* l’entité en charge de la maintenance applicative,
* l’entité responsable de l’application (e.g. l’entité à agréer, une entité du groupe, un tiers),
	+ indication si l’application est dédiée ou partagée avec d’autres entités du groupe (merci de lister les autres entités avec lesquelles l’application est partagée)

|  |  |
| --- | --- |
| *Veuillez mettre le tableau en annexe de ce formulaire.* | *Cadre réservé à l’administration* |
|  |

1. Veuillez également fournir des informations sur l’intention de l’entité à agréer d’utiliser ou non des terminaux mobiles (e.g. smartphones, tablettes). En cas d’utilisation de terminaux mobiles, l'entité à agréer doit décrire les outils utilisés pour se connecter de manière sécurisée (e.g. Mobile/Enterprise Device Management tools) et pour contrôler les terminaux (y inclus remote wipe, passcode lock, etc.). L’entité doit également confirmer sa conformité aux rapports d’activités CSSF 2012 (chapitre XI, section 2.4), 2007 (chapitre VIII, section 2.1) et 2005, (chapitre VIII, section 2.2.1).

|  |  |
| --- | --- |
| *[insérer texte]* | *Cadre réservé à l’administration* |
|  |

1. Veuillez également préciser le type de ligne téléphonique que l’entité à agréer souhaite utiliser (i.e. PBAX classique ou VoIP). En cas d’utilisation de VoIP, l’entité à agréer doit confirmer sa conformité aux éléments du rapport d’activités CSSF 2013, chapitre XI, section 2.3.

|  |  |
| --- | --- |
| *[insérer texte]* | *Cadre réservé à l’administration* |
|  |

1. Veuillez décrire si l’entité à agréer assure elle-même l’hébergement de ses systèmes informatiques (de support et de métier) dans ses locaux et l’administration de ses systèmes informatiques. Si tel n’est pas le cas, merci de fournir des informations sur le type de service fourni (e.g. PaaS, SaaS, IaaS), la localisation du système (auprès d’un prestataire externe ou faisant partie du même groupe que l’entité à agréer, à Luxembourg ou à l’étranger), sur l’opérateur du système (notamment : dénomination sociale, siège social, appartenance au même groupe que l’entité à agréer, surveillance par une autorité de contrôle, PSF de support) et sur un éventuel partage du système avec d’autres entités (faisant partie du même groupe que l’entité à agréer ou non).

|  |  |
| --- | --- |
| *[insérer texte]* | *Cadre réservé à l’administration* |
|  |

1. Dans le cas d’une sous-traitance en cascade, l’établissement doit s’assurer que les principes énoncés dans la section précédente, relatifs à la sous-traitance, sont respectés par l’entité contractuellement responsable de la gestion des systèmes informatiques et que le processus de sous-traitance en cascade est maîtrisé. Veuillez fournir tous les éléments permettant de montrer que ce processus est maîtrisé.

|  |  |
| --- | --- |
| *[insérer texte]* | *Cadre réservé à l’administration* |
|  |

#### Description des systèmes IT :

1. Veuillez décrire les mesures et les mécanismes de sécurité logique relatifs aux connexions aux systèmes informatiques de l'entité à agréer. Ce point concerne les connexions internes et externes – les connexions externes étant celles qui ne passent pas par le réseau interne de l’entité à agréer. Dans ce contexte, merci de préciser :
* les mesures de redondance pour toutes ces connexions, afin d’assurer la continuité de service.
* les protocoles de sécurité utilisés (e.g. IPSec, SSL) ainsi que les algorithmes de chiffrement symétriques/asymétriques utilisés (e.g. RSA, AES) et les tailles de clés correspondantes utilisées.
* les contrôles en place afin d’assurer que l’implémentation de technologies de chiffrement n’est pas exposée à des vulnérabilités connues (e.g. vulnérabilités SSL comme le Heartbleed, Poodle, etc.).

|  |  |
| --- | --- |
| *[insérer texte]* | *Cadre réservé à l’administration* |
|  |

1. En cas d’accès distant, veuillez spécifier :
* les personnes qui utilisent les connexions externes (e.g. employés, support IT, groupe, prestataire externe). Dans le cas où il est prévu d’autoriser des employés de l’entité à agréer à accéder à distance sur les systèmes informatiques, l’entité à agréer doit préciser le nombre de personnes concernées, les systèmes accessibles à distance (en précisant si ces systèmes contiennent des données confidentielles ou non), la justification métier de cet accès et confirmer sa conformité aux exigences de la CSSF mentionnées dans les rapports d’activités 2013 (chapitre XI, section 2.7.) et 2007 (chapitre VIII, section 2.1.).
* les moyens techniques utilisés pour fournir cet accès distant (e.g. VPN, Citrix, etc.), les méthodes d’authentification utilisées (e.g. tokens) et les contrôles de sécurité en place pour éviter la fuite de données (e.g. chiffrement du disque dur, blocage des ports USB, blocage des fonctionnalités de copier/coller et d’impression, etc.).

|  |  |
| --- | --- |
| *[insérer texte]* | *Cadre réservé à l’administration* |
|  |

1. Veuillez également préciser les mesures de sécurité implémentées pour assurer la protection des données, ceci incluant la prévention de fuite de données et la ségrégation des environnements dans le cas où les ressources informatiques utilisées par l'entité à agréer sont partagées.

|  |  |
| --- | --- |
| *[insérer texte]* | *Cadre réservé à l’administration* |
|  |

1. Veuillez indiquer si les données stockées sont encryptées ou non. Dans l’affirmative, veuillez décrire les processus de cryptage qui ont été mis en place en précisant le protocole, l’algorithme de cryptage et la longueur des clés. Veuillez préciser la localisation des clés de cryptage de ces données ainsi que de leur copie éventuelle (sauvegardes) et les personnes pouvant y accéder.

|  |  |
| --- | --- |
| *[insérer texte]* | *Cadre réservé à l’administration* |
|  |

1. Veuillez décrire le niveau de contrôle que l’entité à agréer a sur les accès à ses systèmes (e.g. respect du principe du « need to know », revue régulière des accès, ouverture/fermeture des lignes de communication, authentification des utilisateurs, détection d'intrusion, antivirus, logs).

|  |  |
| --- | --- |
| *[insérer texte]* | *Cadre réservé à l’administration* |
|  |

1. Dans le cas où l’entité à agréer met à disposition de ses clients des applications accessibles depuis Internet (e.g. site Web, application mobile), merci de décrire les fonctionnalités offertes et les mesures de sécurité liées à l’infrastructure sous-jacente de ce(s) outil(s) ainsi que les mécanismes de sécurité pour les connexions clients.

|  |  |
| --- | --- |
| *[insérer texte]* | *Cadre réservé à l’administration* |
|  |

1. Veuillez décrire le processus implémenté dans le cadre de la gestion des patchs.

|  |  |
| --- | --- |
| *[insérer texte]* | *Cadre réservé à l’administration* |
|  |

#### Mesures de sécurité physique:

1. Veuillez préciser les mesures de sécurité physique relatives aux contrôles d’accès et à la sécurité environnementale pour :
* Les bureaux de l’entité à agréer,
* Les locaux informatiques (de l’entité et/ou de son sous-traitant).

|  |  |
| --- | --- |
| *[insérer texte]* | *Cadre réservé à l’administration* |
|  |

#### Continuité de l’activité :

1. Veuillez fournir une description des solutions de sauvegarde de l’entité à agréer (notamment: le type (i.e. full ou incrémental), la fréquence et les périodes de rétention, la localisation des sauvegardes, la restriction d'accès à ces sauvegardes). L’entité à agréer doit confirmer sa conformité avec le rapport d’activités CSSF 2012 (chapitre XI, section 2.7).

|  |  |
| --- | --- |
| *[insérer texte]* | *Cadre réservé à l’administration* |
|  |

1. Veuillez préciser où l'entité à agréer aura ses locaux de secours dans le cadre de l’activation d’un BCP (Business Continuity Plan). L’entité doit confirmer sa conformité, ou à défaut s’engager à devenir conforme, aux exigences CSSF décrites dans le rapport d’activités 2013 (chapitre XI, section 2.5.1). Merci de fournir également une description de la stratégie du DRP (Disaster Recovery Plan) (i.e. site secondaire prévu ou non), ainsi que des mesures de haute disponibilité.

|  |  |
| --- | --- |
| *[insérer texte]* | *Cadre réservé à l’administration* |
|  |

1. Veuillez confirmer que l'entité dispose d'un accès permanent, direct et inconditionnel (lecture et écriture) aux systèmes informatiques mis à disposition par des sous-traitants. L’entité doit à tout moment pouvoir reprendre ses activités en main.

|  |  |
| --- | --- |
| *[insérer texte]* | *Cadre réservé à l’administration* |
|  |

1. Veuillez confirmer que les solutions de sauvegarde, le BCP et le DRP seront en ligne avec les besoins de l’entité à agréer en termes de continuité.

|  |  |
| --- | --- |
| *[insérer texte]* | *Cadre réservé à l’administration* |
|  |