cssf

Commission de Surveillance
du Secteur Financier

Circulaire CSSF 24/847

sur le cadre de notification des incidents liés aux TIC

Circulaire CSSF 24/847

sur le cadre de notification des incidents liés aux TIC

À toutes les Entités Surveillées au sens des lois modifiées et des règlements suivants, tels que précisés au point 2 :

- la loi du 5 avril 1993 sur le secteur financier
- la loi du 15 décembre 2000 sur les services financiers postaux
- la loi du 10 novembre 2009 relative aux services de paiement
- la loi du 17 décembre 2010 concernant les organismes de placement collectif
- la loi du 12 juillet 2013 relative aux gestionnaires de fonds d'investissement alternatifs
- la loi du 15 mars 2016 relative aux produits dérivés de gré à gré, aux contreparties centrales et aux référentiels centraux
- la loi du 17 avril 2018 relative aux indices de référence
- la loi du 6 juin 2018 relative aux dépositaires centraux de titres
- la loi du 28 mai 2019 relative aux réseaux et aux systèmes d'information
- la loi du 16 juillet 2019 relative à l'opérationnalisation de règlements européens dans le domaine des services financiers

Luxembourg, le 5 janvier 2024

Mesdames, Messieurs,

La présente circulaire vise à introduire un nouveau cadre de notification des incidents liés aux TIC en vue d'obtenir une meilleure vue d'ensemble plus structurée de la nature, de la fréquence, de l'importance et des conséquences des incidents liés aux TIC, en prenant également en compte le risque croissant lié aux TIC et à la sécurité dans le contexte d'un système financier mondial fortement interconnecté.

Les dispositions de la présente circulaire se fondent sur l'article 53, paragraphe 1, de la loi modifiée du 5 avril 1993 relative au secteur financier (ci-après la « LSF »), l'article 31, paragraphe 4, de la loi modifiée du 10 novembre 2009 relative aux services de paiement (ci-après la « LSP »), l'article 2 de la loi modifiée du 15 décembre 2000 sur les services financiers postaux, l'article 147 de la loi modifiée du 17 décembre 2010 concernant les organismes de placement collectif (ci-après la « Loi OPCVM »), l'article 50 de la loi modifiée du 12 juillet 2013 relative aux gestionnaires de fonds d'investissement alternatifs (ci-après la « Loi GFIA »), l'article 2, paragraphe 1, de la loi modifiée du 15 mars 2016 relative aux produits dérivés de gré à gré, aux contreparties centrales et aux référentiels centraux (ci-après la « Loi EMIR »), l'article 2, paragraphe 1, de la loi du 17 avril 2018 relative aux indices de référence (ci-après la « Loi relative aux indices de référence »), l'article 2 de la loi du 6 juin 2018 relative aux dépositaires centraux de titres (ci-après la « Loi DCT »), et l'article 20-16 de la loi du 16 juillet 2019 relative à l'opérationnalisation de règlements européens dans le domaine des services financiers.

Conformément à l'article 3 de la loi du 28 mai 2019 relative aux réseaux et aux systèmes d'information (ci-après la « Loi SRI »), la CSSF est également l'autorité compétente en termes de sécurité des réseaux et de l'information pour les établissements de crédit et les infrastructures des marchés financiers qui ont été identifiés en tant qu'opérateurs de services essentiels (ci-après les

« OSE »), ainsi que pour les fournisseurs de services numériques (ci-après les « FSN ») qui sont déjà soumis à la surveillance de la CSSF (ci-après l'« autorité SRI »). L'objectif de la présente circulaire est de fixer les détails et modalités pratiques en matière d'obligations de notification prévues à l'article 8, paragraphes 4 et 5, à l'article 9, paragraphe 1, à l'article 11, paragraphes 3 et 4, et à l'article 12 de la Loi SRI et au règlement CSSF N° 24-01 relatif à la notification des incidents selon la loi du 28 mai 2019[1] (ci-après le « Règlement CSSF N° 24-01 ») notamment en ce qui concerne l'article 8, paragraphe 5, et l'article 11, paragraphe 3, de la Loi SRI.

La présente circulaire apporte les modifications suivantes au mécanisme actuel de notification des incidents :

- élargissement de la couverture des incidents qui est actuellement limitée à la fraude et aux incidents dus à des attaques informatiques externes conformément à la circulaire CSSF 11/504, en couvrant plus largement les incidents opérationnels et de sécurité liés aux TIC tout en évitant la double notification pour les incidents à notifier en vertu d'autres cadres de notification des incidents ;
- introduction de notifications reposant sur la classification. Les Entités Surveillées seront tenues de classifier les incidents liés aux TIC sur base des critères énoncés dans la présente circulaire et de notifier à la CSSF les cas d'incidents liés aux TIC qui sont classifiés en tant qu'incidents majeurs ou significatifs ;
- introduction d'un nouveau formulaire de notification d'incidents. Afin d'obtenir les données de manière structurée, les Entités Surveillées seront tenues de compléter et de soumettre un formulaire de notification d'incidents liés aux TIC au cas où l'incident lié aux TIC est classifié en tant qu'incident majeur ou significatif ;
- introduction d'un chapitre spécifique pour couvrir dans la même circulaire les exigences en matière de notification d'incidents (précédemment communiqué de manière bilatérale aux Entités Surveillées qui tombent sous le champ d'application de la Loi SRI) en vue d'appliquer le nouveau formulaire de notification d'incidents et les exigences pratiques aux notifications d'incidents évalués comme significatifs en vertu de la Loi SRI.

La présente circulaire est divisée en quatre chapitres :

- Le chapitre 1 (Définitions et champ d'application) fixe les définitions applicables aux fins de la présente circulaire et établit le champ d'application ;
- Le chapitre 2 (Exigences générales) établit les exigences pour la classification et les notifications d'incidents liés aux TIC ;
- Le chapitre 3 (Exigences spécifiques en vertu de la Loi SRI et du Règlement CSSF N° 24-01) est dédié aux exigences spécifiques pour les Entités Surveillées qui sont soumises à la Loi SRI et au Règlement CSSF N° 24-01 et qui sont définies comme OSE ou FSN ;
- Le chapitre 4 (Date d'application) prévoit l'entrée en vigueur de la présente circulaire.

[1] Règlement CSSF N° 24-01 du 5 janvier 2024 relatif à la notification des incidents selon la loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne.

TABLE DES MATIÈRES

Chapitre 1 : Définitions et champ d'application

Section 1.1 : Définitions

1. Aux fins de la présente circulaire, on entend par[2]:

   a) « Réseaux et systèmes d'information » :
      i. un réseau de communications électroniques au sens de l'article 2, point 1°, de la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques[3] ;
      ii. tout dispositif ou tout ensemble de dispositifs interconnectés ou apparentés, dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques ; ou
      iii. les données numériques stockées, traitées, récupérées ou transmises par les éléments visés aux points i. et ii. ci-dessus en vue de leur fonctionnement, utilisation, protection et maintenance.

   b) « Sécurité des réseaux et des systèmes d'information » : la capacité des réseaux et des systèmes d'information de résister, à un niveau de confiance donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées ou transmises ou faisant l'objet d'un traitement, ou des services que ces réseaux et systèmes d'information offrent ou rendent accessibles.

   c) « Incident lié aux TIC » : un événement unique ou une série d'événements liés entre eux que l'Entité Surveillée n'a pas prévu, qui compromet la sécurité des réseaux et des systèmes d'information, et a une incidence négative sur la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données ou sur les services fournis par l'Entité Surveillée.

   d) « Incident majeur lié aux TIC » : un incident lié aux TIC qui a une incidence négative élevée sur les réseaux et les systèmes d'information qui soutiennent les fonctions critiques ou importantes de l'Entité Surveillée.

   e) « Fonction critique ou importante » : une fonction dont la perturbation est susceptible de nuire sérieusement à la performance financière d'une Entité Surveillée, ou à la solidité ou à la continuité de ses services et activités, ou une interruption, une anomalie ou une défaillance de l'exécution de cette fonction qui est susceptible de nuire sérieusement à la capacité d'une Entité Surveillée de respecter en permanence les conditions et obligations de son agrément, ou ses autres obligations découlant des dispositions applicables des lois relatives aux services financiers.

[2] Les définitions aux points 1.f) à 1.i) sont spécifiques aux Entités Surveillées soumises aux exigences de la Loi SRI et du Règlement CSSF N° 24-01.

[3] Un « réseau de communications électroniques » : les systèmes de transmission, qu'ils soient ou non fondés sur une infrastructure permanente ou une capacité d'administration centralisée et, le cas échéant, les équipements de commutation ou de routage et les autres ressources, y compris les éléments de réseau qui ne sont pas actifs, qui permettent l'acheminement de signaux par câble, par la voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques, comprenant les réseaux satellitaires, les réseaux fixes (avec commutation de circuits ou de paquets, y compris l'internet) et mobiles, les systèmes utilisant le réseau électrique, pour autant qu'ils servent à la transmission de signaux, les réseaux utilisés pour la radiodiffusion sonore et télévisuelle et les réseaux câblés de télévision, quel que soit le type d'information transmise.

f) « Opérateur de services essentiels » (« OSE ») : conformément à l'article 2, point 3°, de la Loi SRI, une entité publique ou privée dont le type figure à l'annexe de la Loi SRI et qui répond aux critères énoncés à l'article 7, paragraphe 2, de la Loi SRI[4].

g) « Fournisseur de service numérique » (« FSN ») : conformément à l'article 2, point 5°, de la Loi SRI, une entité privée qui fournit un service numérique, tel que défini à l'article 2, point 4°, de la Loi SRI[5].

h) « Service essentiel » : un service qui est essentiel au maintien d'activités sociétales et/ou économiques critiques et qui est listé en tant que service essentiel à l'article 2 du règlement CSSF N° 20-04 du 15 juillet 2020[6].

i) « Incident significatif » : un incident qui a un impact significatif sur la continuité des services essentiels fournis par un OSE ou sur la prestation d'un service numérique par un FSN[7] au sein de l'Union européenne. Aux fins de la présente circulaire, un incident significatif est considéré par défaut comme « incident majeur lié aux TIC ».

2. Les entités suivantes sont à considérer comme Entités Surveillées dans le cadre de la présente circulaire :

a) les établissements de crédit et les professionnels du secteur financier au sens de la LSF ;

b) les dispositifs de publication agréés (« APA ») avec une dérogation et les mécanismes de déclaration agréés (« ARM ») avec une dérogation au sens de la LSF ;

c) les établissements de paiement et les établissements de monnaie électronique au sens de la LSP ;

d) POST Luxembourg régi par la loi du 15 décembre 2000 sur les services financiers postaux[8] ;

e) les sociétés de gestion de droit luxembourgeois soumises au chapitre 15 de la Loi OPCVM ;

f) les sociétés de gestion de droit luxembourgeois soumises aux articles 125-1 ou 125-2 du chapitre 16 de la Loi OPCVM ;

g) les succursales luxembourgeoises de gestionnaires de fonds d'investissement soumis au chapitre 17 de la Loi OPCVM ;

h) les sociétés d'investissement qui n'ont pas désigné une société de gestion au sens de l'article 27 de la Loi OPCVM ;

[4] En sa qualité d'autorité SRI, la CSSF a déjà notifié les Entités Surveillées concernées de leur identification en tant qu'OSE lorsque la Loi SRI est entrée en vigueur. La CSSF confirmera à nouveau le statut d'OSE aux Entités Surveillées concernées au plus tard le 1er mars 2024. Les Entités Surveillées qui n'ont pas reçu cette notification à la date prévue ne sont donc pas désignées comme OSE sans préjudice d'une possible désignation ultérieure.

[5] En sa qualité d'autorité SRI, la CSSF a déjà informé les Entités Surveillées concernées qu'elles sont considérées comme FSN lorsque la Loi SRI est entrée en vigueur. La CSSF confirmera à nouveau le statut de FSN aux Entités Surveillées concernées au plus tard le 1er mars 2024. Les Entités Surveillées qui n'ont pas reçu cette information à la date prévue ne sont donc pas considérées comme FSN sans préjudice d'une possible information ultérieure.

[6] Règlement CSSF N° 20-04 du 15 juillet 2020 relatif à la définition des services essentiels selon la loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne.

[7] Définition en ligne avec la Loi SRI.

[8] Par souci de clarté, le terme « services financiers postaux » a la même signification qu'à l'article 1 de la loi modifiée du 15 décembre 2000.

i) les gestionnaires de fonds d'investissement alternatifs agréés au titre du chapitre 2 de la Loi GFIA ;

j) les fonds d'investissement alternatifs à gestion interne au sens de l'article 4, paragraphe 1, point b), de la Loi GFIA ;

k) les contreparties centrales (« CCP ») au sens de l'article 2, paragraphe 1, du Règlement EMIR[9], y compris les contreparties centrales de pays tiers de catégorie 2 au sens de l'article 25, paragraphe 2*bis*, du Règlement EMIR, qui respectent les exigences applicables du Règlement EMIR conformément à l'article 25, paragraphe 2*ter*, point a), du Règlement EMIR ;

l) les dépositaires centraux de titres au sens de la Loi DCT ;

m) les administrateurs d'indices de référence d'importance critique au sens de l'article 20, paragraphe 1, point b), du Règlement sur les indices de référence[10] ;

n) les prestataires de services de financement participatif au sens de la loi du 16 juillet 2019 relative à l'opérationnalisation de règlements européens dans le domaine des services financiers ;

o) les établissements de crédit et les infrastructures des marchés financiers pour lesquels la CSSF est l'autorité compétente, en vertu de l'article 3 de la Loi SRI, en termes de sécurité des réseaux et de l'information et qui ont été identifiés en tant qu'OSE ;

p) les PSF de support agréés conformément à l'article 29-3 de la LSF pour lesquels la CSSF est l'autorité compétente, en vertu de l'article 3 de la Loi SRI, en termes de sécurité des réseaux et de l'information et qui ont été informés par la CSSF qu'ils sont considérés comme FSN conformément à la Loi SRI.

Section 1.2 : Champ d'application

3. La présente circulaire définit les attentes prudentielles à respecter dans le cas d'un incident lié aux TIC.

4. Les dispositions du chapitre 2 (Exigences générales) de la présente circulaire s'appliquent à toutes les Entités Surveillées, telles que définies au point 2.a) à n) ci-dessus, ci-après dénommées collectivement « **Entités Surveillées** » ou individuellement « **Entité Surveillée** », y compris leurs succursales telles que précisées dans les lois respectives. Les succursales au Luxembourg d'entités ayant leur siège social dans un pays tiers sont réputées être incluses dans la notion d'Entité Surveillée.

5. Les succursales au Luxembourg d'entités qui font partie d'une entité juridique dont le siège social est situé dans un État membre de l'Espace économique européen (EEE) différent (succursales EEE) sont soumises à la surveillance de l'autorité compétente de cet État membre (État membre d'origine). Cependant, la CSSF étant compétente pour veiller à ce que les succursales EEE respectent les exigences spécifiques prévues dans les cadres légaux

[9] Règlement (UE) n° 648/2012 du Parlement européen et du Conseil du 4 juillet 2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux.

[10] Règlement (UE) 2016/1011 du Parlement européen et du Conseil du 8 juin 2016 concernant les indices utilisés comme indices de référence dans le cadre d'instruments et de contrats financiers ou pour mesurer la performance de fonds d'investissement et modifiant les directives 2008/48/CE et 2014/17/UE et le règlement (UE) n° 596/2014.

et réglementaires sectoriels[11], la présente circulaire s'applique si un incident lié aux TIC a une incidence sur les domaines pour lesquels la CSSF conserve une responsabilité de contrôle.

6. Les dispositions du chapitre 3 (Exigences spécifiques en vertu de la Loi SRI et du Règlement CSSF N° 24-01) de la présente circulaire sont applicables uniquement aux Entités Surveillées qui sont également des OSE[4] ou des FSN[5].

7. Afin d'éviter la double notification, les Entités Surveillées tombant dans le champ d'application de la présente circulaire ne sont pas tenues de notifier, en vertu de la présente circulaire, les incidents qu'elles notifient conformément à :

   a) la circulaire CSSF 21/787 concernant l'application des Orientations de l'EBA (EBA/GL/2021/03) sur la notification des incidents majeurs en vertu de la directive DSP2 ; et/ou
   b) le cadre de notification des cyberincidents pour les Entités Surveillées définies en tant qu'établissements d'importance significative tombant sous la supervision directe de la BCE ; et/ou
   c) l'article 45, paragraphe 6, du règlement (UE) n° 909/2014 relatif à la notification d'incidents résultant de risques que les participants clés, les prestataires de services et les fournisseurs de services de réseau, les autres dépositaires centraux de titres (« DCT ») ou les autres infrastructures de marché sont susceptibles de représenter pour les activités de DCT ; et/ou
   d) l'article 71, paragraphe 4, point b), du règlement délégué (UE) 2017/392 de la Commission du 11 novembre 2016 complétant le règlement (UE) n° 909/2014 relatif à la notification d'incidents opérationnels importants à l'autorité compétente.

8. Par dérogation au point 7 ci-dessus, les Entités Surveillées tombant sous le point 7.b) et qui sont également des OSE sont tenues, conformément à la présente circulaire, de notifier à la CSSF les incidents qui ont un impact sur la continuité des services essentiels qu'elles fournissent, en sus de leurs autres obligations en matière de notification d'incidents.

Chapitre 2 : Exigences générales

Section 2.1 : Incidents à notifier

9. Les Entités Surveillées doivent notifier les incidents suivants conformément à la procédure définie à la section 2.3 :

   a) tout accès malveillant non autorisé réussi aux réseaux et systèmes d'information. Aux fins de la présente circulaire, ces accès malveillants non autorisés réussis sont à considérer comme incidents majeurs liés aux TIC ;
   b) tout incident autre que ceux visés au point a) ci-dessus, classifié conformément à la section 2.2 en tant qu'incident majeur lié aux TIC.

[11] Notamment dans le cadre de services d'investissement conformément à la loi modifiée du 30 mai 2018 relative aux marchés d'instruments financiers (ci-après la « Loi MiFID »), la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme (ci-après la « Loi LBC/FT »), la fourniture de services de gestion de portefeuille et l'exercice de tâches de dépositaire pour les organismes de placement collectif établis au Luxembourg.

Section 2.2 : Classification des incidents liés aux TIC

10. Les Entités Surveillées doivent classifier les incidents liés aux TIC et évaluer leur incidence sur base des critères suivants :

    a) le nombre et/ou la pertinence des clients[12] ou des contreparties financières affectés et, le cas échéant, le montant ou le nombre de transactions affectées par l'incident lié aux TIC et si cet incident a porté atteinte à la réputation ;
    b) la durée de l'incident lié aux TIC, y compris les interruptions de service ;
    c) la répartition géographique en ce qui concerne les zones touchées par l'incident lié aux TIC, en particulier si celui-ci touche plus de deux États membres ;
    d) les pertes de données occasionnées par l'incident lié aux TIC en ce qui concerne la disponibilité, l'authenticité, l'intégrité ou la confidentialité ;
    e) la criticité des services touchés, y compris les transactions et les opérations de l'Entité Surveillée ;
    f) les conséquences économiques, en particulier les coûts et pertes directs et indirects, en termes absolus et relatifs, de l'incident lié aux TIC.

11. Lorsque l'évaluation interne de l'Entité Surveillée fondée sur les critères énoncés au point 10 conduit l'Entité Surveillée à classifier un incident lié aux TIC en tant qu'incident majeur, l'incident lié aux TIC doit être considéré comme majeur en vertu de la présente circulaire.

12. Lorsque l'évaluation visée au point 11 ne permet pas de conclure clairement si un incident lié aux TIC est à classifier comme majeur, les Entités Surveillées doivent notifier l'incident lié aux TIC à la CSSF.

13. Les Entités Surveillées doivent classifier l'incident lié aux TIC rapidement après la détection de l'incident lié aux TIC et sans délai indu suivant la disponibilité de l'information requise pour la classification de l'incident lié aux TIC aux Entités Surveillées, mais pas plus tard que 24 heures suivant la détection de cet incident lié aux TIC. Si un délai plus long est nécessaire pour classifier l'incident lié aux TIC, les Entités Surveillées doivent en expliquer les raisons dans la notification initiale soumise à l'autorité compétente. Lorsque le délai pour la classification tombe un jour de fin de semaine ou un jour férié, les Entités Surveillées peuvent classifier l'incident le jour ouvrable suivant.

Section 2.3 : Notification d'incidents majeurs liés aux TIC

14. Les Entités Surveillées doivent soumettre à la CSSF, endéans les délais fixés à l'annexe I, les notifications suivantes relatives aux incidents majeurs liés aux TIC :

    a) Une notification initiale avec des « Informations initiales » lorsque l'incident lié aux TIC a été classifié comme majeur.
    b) Une notification intermédiaire avec « Causes, classification et incidence de l'incident » après la notification initiale visée au point 14.a), suivi, le cas échéant, de notifications actualisées chaque fois qu'une mise à jour pertinente est disponible, ainsi que sur demande spécifique de la CSSF.

[12] Les Entités Surveillées qui sont également des OSE doivent prendre en considération le nombre d'utilisateurs touchés par la perturbation du service essentiel. Les Entités Surveillées qui sont également des FSN doivent prendre en considération le nombre d'utilisateurs touchés par l'incident, en particulier ceux qui recourent au service numérique pour la fourniture de leurs propres services.

c) Une notification finale, lorsque l'analyse des causes originelles est terminée, que des mesures d'atténuation aient été mises en œuvre pleinement ou non, et lorsque les chiffres relatifs aux incidences réelles sont disponibles en lieu et place des estimations. Dans cette notification, les Entités Surveillées peuvent ajouter tout suivi ou informations complémentaires qu'elles jugent utiles pour l'incident lié aux TIC.

15. Lorsque l'incident lié aux TIC s'avère avoir ou pourrait avoir une grave incidence (par exemple, l'indisponibilité totale des systèmes), l'Entité Surveillée doit notifier la CSSF dès que possible endéans le délai fixé et, le cas échéant, avant la soumission formelle du formulaire de notification.

16. Les notifications concernant les incidents liés aux TIC visées au point 14 doivent être soumises à l'aide du formulaire correspondant disponible via la solution numérique de la CSSF, telle que précisée sur le site Internet de la CSSF.

17. Les Entités Surveillées doivent compléter la section pertinente du formulaire de notification, en fonction de la phase dans laquelle elles se trouvent (c.-à-d. la section « Informations initiales » (*Initial Information*) pour les notifications initiales, la section « Causes, classification et incidence de l'incident » (*Incident cause, classification and impact*) pour les notifications intermédiaires et la section « Causes originelles - suivi et informations complémentaires » (*Root cause – Follow-up and additional information*) pour les notifications finales). Le formulaire de notification contient des champs de données prévus à l'annexe II (uniquement disponible en anglais).

18. Les sections du formulaire de notification doivent être soumises dans l'ordre indiqué sous le point 14. Si l'Entité Surveillée dispose de toutes les informations requises au moment de la notification initiale, une seule soumission (contenant toutes les sections du formulaire de notification) doit être faite.

19. Les Entités Surveillées doivent également notifier à l'autorité compétente lorsque, en raison de l'évaluation continue de l'incident lié aux TIC, il a été déterminé qu'un incident lié aux TIC déjà notifié ne remplit plus les critères pour être considéré comme majeur et il est présumé que l'incident lié aux TIC ne les remplit pas avant sa résolution. Dans ce cas, les Entités Surveillées doivent reclassifier l'incident lié aux TIC dès que cette circonstance est identifiée et fournir une explication des raisons justifiant cette reclassification à la section « Informations initiales » du formulaire de notification.

20. Les Entités Surveillées peuvent externaliser les obligations de déclaration prévues par le présent chapitre à un prestataire tiers. Dans le cas d'une telle externalisation, l'Entité Surveillée reste pleinement responsable du respect des exigences en matière de déclaration des incidents liés aux TIC endéans les délais applicables et pour le contenu complet des déclarations des incidents.

Chapitre 3 : Exigences spécifiques en vertu de la Loi SRI et du Règlement CSSF N° 24-01

Section 3.1 : Notifications d'incidents par les Entités Surveillées qui sont également des OSE

21. Conformément à l'article 8, paragraphe 4, de la Loi SRI, les Entités Surveillées qui sont également des OSE doivent notifier à la CSSF, sans retard injustifié, les incidents qui ont un impact significatif sur la continuité des services essentiels qu'elles fournissent. On considère que la notion de « sans retard injustifié » est considérée comme respectée lorsque les Entités Surveillées soumettent leur notification d'incident conformément aux délais indiqués à la section 2.3 (Notification d'incidents majeurs liés aux TIC) et à l'annexe I.

22. À cet égard, conformément à l'article 8, paragraphe 5, de la Loi SRI et au Règlement CSSF N° 24-01, les Entités Surveillées qui sont également des OSE doivent évaluer si l'incident est à classifier en tant qu'incident significatif en appliquant mutatis mutandis les exigences énoncées à la section 2.2 (Classification des incidents liés aux TIC) et doivent notifier les incidents significatifs conformément aux exigences énoncées à la section 2.3 (Notification d'incidents majeurs liés aux TIC).

23. Les accès malveillants non autorisés réussis doivent être considérés par défaut comme des incidents significatifs et doivent être notifiés conformément aux exigences énoncées à la section 2.3 (Notification d'incidents majeurs liés aux TIC).

24. Lorsqu'un incident est classifié en tant qu'incident significatif et en tant qu'incident majeur lié aux TIC (par exemple, l'incident impacte aussi bien les services essentiels en vertu de la Loi SRI que les autres fonctions critiques ou importantes), les Entités Surveillées qui sont également des OSE doivent notifier l'incident une seule fois et indiquer dans leur notification que l'incident est également notifié en vertu de la Loi SRI.

Section 3.2 : Notifications d'incidents par les Entités Surveillées qui sont également des FSN

25. L'article 11, paragraphe 3, de la Loi SRI et le Règlement CSSF N° 24-01 indiquent que les FSN doivent notifier à l'autorité compétente, sans retard injustifié, les incidents ayant un impact significatif sur la fourniture d'un service numérique qu'ils offrent dans l'Union européenne. On considère que la notion de « sans retard injustifié » est considérée comme respectée lorsque les Entités Surveillées soumettent leur notification d'incident conformément aux délais indiqués à la section 2.3 (Notification d'incidents majeurs liés aux TIC) et à l'annexe I.

26. Les Entités Surveillées qui sont également des FSN doivent :

    a) évaluer si un incident (y compris des accès malveillants non autorisés réussis, tels que définis au point 9.a) de la section 2.1) est à classifier en tant qu'incident significatif conformément aux articles 3 et 4 du règlement d'exécution (UE) 2018/151 de la

Commission du 30 janvier 2018[13] portant précision de l'article 11, paragraphe 4, de la Loi SRI ;

b) appliquer mutatis mutandis les points 12 et 13 de la section 2.2 (Classification des incidents liés aux TIC) ;

c) notifier les incidents significatifs conformément aux exigences énoncées à la section 2.3 (Notification d'incidents majeurs liés aux TIC).

27. Lorsqu'un incident est classifié en tant qu'incident significatif et en tant qu'incident majeur lié aux TIC, les Entités Surveillées qui sont également des FSN doivent notifier l'incident une seule fois et indiquer dans leur notification que l'incident est également notifié en vertu de la Loi SRI.

Chapitre 4 : Date d'application

28. La présente circulaire entre en vigueur le 1er avril 2024 pour les Entités Surveillées telles que définies au point 2.a) à d) et k) à p) de la section 1.1, et le 1er juin 2024 pour les Entités Surveillées telles que définies au point 2.e) à j) de la section 1.1. La présente circulaire abrogera et remplacera la circulaire CSSF 11/504 concernant les fraudes et incidents dus à des attaques informatiques externes le 1er avril 2024 pour les Entités Surveillées telles que définies au point 2.a) à d) et k) à p) de la section 1.1, et le 1er juin 2024 pour les Entités Surveillées telles que définies au point 2.e) à j) de la section 1.1.

Claude WAMPACH
Directeur

Marco ZWICK
Directeur

Jean-Pierre FABER
Directeur

Françoise KAUTHEN
Directeur

Claude MARX
Directeur général

Annexes
I. Délais et explications concernant la soumission de notifications
II. Champs de données (uniquement en anglais)

[13] Règlement d'exécution (UE) 2018/151 de la Commission du 30 janvier 2018 portant modalités d'application de la directive (UE) 2016/1148 du Parlement européen et du Conseil précisant les éléments à prendre en considération par les fournisseurs de service numérique pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information ainsi que les paramètres permettant de déterminer si un incident a un impact significatif.

Annexe I : Délais et explications concernant la soumission de notifications

Section pertinente à remplir et à soumettre	Délais	Notes explicatives
N/A	*Classification de l'incident en tant que majeur* Endéans 24 heures après la détection de l'incident lié aux TIC Lorsque le délai pour la classification tombe un jour de fin de semaine ou un jour férié, les Entités Surveillées peuvent classifier l'incident le jour ouvrable suivant.	*Classification de l'incident en tant que majeur* Rappel du point 15 : Lorsque l'incident lié aux TIC s'avère avoir ou pourrait avoir une grave incidence (par exemple, l'indisponibilité totale des systèmes), l'Entité Surveillée doit notifier la CSSF dès que possible endéans le délai fixé et, le cas échéant, avant la soumission formelle du formulaire de notification.
INFORMATIONS INITIALES	Endéans 4 heures après la classification de l'incident en tant que majeur Lorsque le délai pour la notification tombe un jour de fin de semaine ou un jour férié, les Entités Surveillées peuvent notifier l'incident le jour ouvrable suivant.	La section « INFORMATIONS INITIALES » comprend les informations générales concernant l'incident qui doivent être incluses dans la notification lors de la première soumission.
CAUSES, CLASSIFICATION ET INCIDENCE DE L'INCIDENT	Endéans 3 jours ouvrables après la soumission des INFORMATIONS INITIALES à la CSSF	La section « CAUSES, CLASSIFICATION ET INCIDENCE DE L'INCIDENT » fournit une description plus détaillée de l'incident, de ses conséquences et des mesures correctives prises pour la résolution. Si l'Entité Surveillée peut mettre à jour des rapports antérieurs (concernant le même incident), une version actualisée de la section du formulaire peut être soumise.

CAUSES ORIGINELLES - SUIVI ET INFORMATIONS COMPLÉMENTAIRES	Endéans 20 jours ouvrables après la soumission à la CSSF des CAUSES ORIGINELLES - SUIVI ET INFORMATIONS COMPLÉMENTAIRES	La section « CAUSES ORIGINELLES - SUIVI ET INFORMATIONS COMPLÉMENTAIRES » fournit les informations concernant l'analyse des causes originelles, les enseignements tirés et toute autre information pertinente. Lors de la soumission de ces informations, l'Entité Surveillée doit examiner les autres sections du formulaire et les mettre à jour, le cas échéant.

Annexe II : Champs de données (uniquement en anglais)

Section – Initial Information

Data Field description / Question	Field type	Proposed options
1. Contact person within the supervised entity for updates: Name and surname	Alphanumeric	
1. Contact person within the supervised entity for updates: Email	Alphanumeric (email format)	
1. Contact person within the supervised entity for updates: Phone	Number (telephone format)	
2. Second contact person within the supervised entity for updates: Name and surname	Alphanumeric	
2. Second contact person within the supervised entity for updates: Email	Alphanumeric (email format)	
2. Second contact person within the supervised entity for updates: Phone	Number (telephone format)	
3. Country(ies) affected by the incident	Choice (multiple) - Select all that apply	List of world countries
4. Date and time of detection of the incident	yyyy-mm-dd hh:mm	
5. Date and time of classification of the incident as major	yyyy-mm-dd hh:mm	
6. Criteria triggering the major ICT-related incident report	Choice (multiple) - Select all that apply	• Clients or financial counterparts affected • Transactions affected • Reputational impact • Service downtime • Geographical spread • Data losses entailed in relation to availability, authenticity, integrity or confidentiality • Criticality of the services affected • Economic impact

Data Field description / Question	Field type	Proposed options
7. The incident was detected by	Choice (multiple) – Select one option	• IT security • Staff member • Internal audit • Consumer / payment service user • External auditor • Third party provider • Attacker / warning • Other
7.1. If "Other", specify	Alphanumeric	
8. General description of the incident Provide a general description of the incident, its immediate impact and including the measures that have been taken so far	Alphanumeric	
9. Short description of impact in other EU member states	Alphanumeric	
10. Has the incident been reported to other authorities?	Boolean (Checkbox)	
10.1. If checkbox was ticked, specify	Alphanumeric	
11. If the incident caused a service interruption, is the service restored (even in degraded mode) at the time of this notification?	Alphanumeric	
12. Is the incident notified under NIS (Network Information System) framework?	Boolean (Checkbox)	

Section – Incident cause, classification and impact

Data Field description / Question	Field type	Proposed options
1. Detailed description of the incident, Provide a detailed description of the incident, including (if known and/or applicable): - How the incident started - Background and incident detection, who was involved, what happened, how did it evolve? - Cause of the incident	Alphanumeric	
2. What are the main areas/systems/channels that were affected as the incident evolved?	Alphanumeric	
3. Was it related to a previous incident(s)?	Boolean (Checkbox)	
3.1. If checkbox was ticked, specify	Alphanumeric	
4. Date and time of beginning of the incident - if known	yyyy-mm-dd hh:mm	
5. Who is leading the investigation of the incident?	Choice (multiple) – Select one option	• Group • Supervised entity • Service provider • Security company • Other
6. Cause and type		
6.1. Details regarding incident cause and type (Select all that apply). Select at least one of the main options. Then, as applicable, select the subcategories	Choice (multiple) - Select all that apply	• Under investigation • Malware • Social engineering • Insider/Third Party Provider Threat • Intrusion/Unauthorised access

Data Field description / Question	Field type	Proposed options
		• Denial of service • System/Process failure • Human error • Other
6.1.1. If "Other", specify	Alphanumeric	
6.2. As applicable, select the subcategories	Choice (multiple) - Select all that apply	• Malware o Ransomware o Trojan horse o Virus/Worm/Spyware o Other (Malware) • Social engineering o Phishing/*ishing o Other (Social engineering) • Insider/Third Party Provider Threat o Accidental data leakage/corruption o Intentional misuse of access rights by insider o Intentional misuse of access rights by service provider o Other (Insider/Third Party Provider Threat) • Intrusion/Unauthorised access o Brute force attack o Malicious script injection and/or OS commanding o Unauthorized use of resources, copyright o Account/application compromise o Other exploited vulnerability o Other (Intrusion/Unauthorised access) • Denial of service • System/Process failure o Hardware failure o Software/application failure o Network failure o Database/Storage failure o Physical damage o Other (System/Process failure)

Data Field description / Question	Field type	Proposed options
		• Human error • Other
7. If this incident is related to a cyber-attack, provide information regarding the attacker(s) (select all that apply)	Choice (multiple) - Select all that apply	• Terrorists • Hacktivists • Foreign agencies • Inside job/Unaware employee • Unknown • Other
7.1. If "Other", specify	Alphanumeric	
8. Users impacted		
8.1. Number of internal users impacted	Numeric	
Actual or estimated	Choice (multiple) – Select one option	• Actual figure • Estimation • Not yet available
8.1.1. As a % total internal users (values allowed from 0 to 100, rounded, no decimals, percentage sign not allowed)	Numeric	
Actual or estimated	Choice (multiple) – Select one option	• Actual figure • Estimation • Not yet available
8.2. Number of customers impacted	Numeric	
Actual or estimated	Choice (multiple) – Select one option	• Actual figure • Estimation • Not yet available
8.2.1. As a % total customers (values allowed from 0 to 100, rounded, no decimals, percentage sign not allowed)	Numeric	
Actual or estimated	Choice (multiple) – Select one option	• Actual figure • Estimation • Not yet available

Data Field description / Question	Field type	Proposed options
9. Service downtime?	Boolean (Checkbox)	
9.1. If checkbox was ticked, provide the total service downtime (DD:HH:MM)	Alphanumeric (DD:HH:MM)	
Actual or estimated	Choice (multiple) – Select one option	• Actual figure • Estimation • Not yet available
10. Economic impact		
10.1. Direct financial loss in EUR	Numeric	
Actual or estimated	Choice (multiple) – Select one option	• Actual figure • Estimation • Not yet available
10.2. Indirect financial loss in EUR	Numeric	
Actual or estimated	Choice (multiple) – Select one option	• Actual figure • Estimation • Not yet available
11. Were crisis management (or equivalent) procedures activated or is it likely to be activated?	Boolean (Checkbox)	
11.1. If checkbox was ticked, specify the actions taken	Alphanumeric	
12. Were any legal or regulatory requirements breached?	Boolean (Checkbox)	
12.1. If checkbox was ticked, specify	Alphanumeric	
13. Was there any media coverage?	Boolean (Checkbox)	
13.1. If checkbox was ticked, specify the media/newspapers/blogs that covered the topic	Alphanumeric	

Data Field description / Question	Field type	Proposed options
14. Overall impact (select all that apply)	Choice (multiple) - Select all that apply	• Integrity • Availability • Confidentiality • Reputational
15. Was the incident affecting you directly, or indirectly through a service provider?	Choice (multiple) – Select one option	• Directly • Indirectly
15.1. If "Indirectly", specify the service provider's name	Alphanumeric	
16. Other impacts	Alphanumeric	
17. Corrective actions/measures that have been taken so far or are planned to recover from the incident	Alphanumeric	
18. Was a business continuity plan activated? If yes, when and how?	Boolean (Checkbox)	
18.1. Date and time	yyyy-mm-dd hh:mm	
18.2. Describe	Alphanumeric	
19. Was a disaster recovery plan activated? If yes, when and how?	Boolean (Checkbox)	
19.1. Date and time	yyyy-mm-dd hh:mm	
19.2. Describe	Alphanumeric	
20. Is the incident in any way related to remote access (e.g., teleworking, remote connectivity, etc.)?	Boolean (Checkbox)	
20.1. If checkbox was ticked, specify	Alphanumeric	

Section - Root cause, follow-up and additional information

Data Field description / Question	Field type	Proposed options
1. Additional information Provide details regarding the following: Lessons learned (including main actions/measures taken/planned to prevent the incident from happening again in the future)	Alphanumeric	
2. Root cause and/or Vulnerabilities/weaknesses identified (select all that apply)	Choice (multiple) – Select all that apply	• Inadequate Change Management • Migration failure • Inadequacy of internal procedures and documentation • Improper operations • Latency issues • Recovery issues • Lack of staff awareness and/or compliance • Unauthorised software/wrong version • Inadequate privileged account management • Inadequate email/web browser protection • Inadequate malware defences • Inadequate identity access management • Inadequate security configurations for secure hardware and software on devices, laptops, workstations, servers • Inadequate boundary defences • Inadequate control of network ports, protocols and services • Inadequate resilience and/or back-up of systems or files • Unsecured network devices (firewalls, routers, switches) • Inadequate maintenance and monitoring of logs • Inadequate DDoS defences • Inadequate penetration and security testing • Inadequate patch management • Inadequate application software security controls (web-based and other applications) • Other

Data Field description / Question	Field type	Proposed options
2.1. If "Other", specify	Alphanumeric	
3. Other relevant information on the root cause (e.g., What went wrong with the change, New technical vulnerability exploited, etc.)	Alphanumeric	
4. If this incident is related to a cyber-attack, what was the entry vector of the incident? (select all that apply)	Choice (multiple) – Select all that apply	• Website • Instant messaging • Phone • Insider attack (privileged user) • E-mail • Third party network • Unauthorised devices • Insider attack (regular / business users) • Lost / stolen devices • Chat rooms / social media • Other
4.1. If "Other", specify	Alphanumeric	
5. Who is leading the remediation actions?	Choice (multiple) – Select one option	• Group • Supervised entity • Service provider • Security company • Other
5.1. If "Other", specify	Alphanumeric	
6. Are Police/other security agencies involved in the investigation?	Choice (multiple) – Select one option	• Police • Other • None
6.1. If "Other", specify	Alphanumeric	
7. If the incident is related to ICT security, was the incident reported to the national CERT (e.g., CIRCL, GOVCERT)?	Boolean (Checkbox)	
8. Has any legal action been taken (e.g., complaint with prosecutor against provider or perpetrator)?	Boolean (Checkbox)	

Data Field description / Question	Field type	Proposed options
8.1. If checkbox was ticked, specify	Alphanumeric	
9. Assessment of the effectiveness of the action taken	Choice (multiple) – Select one option	• Highly effective • Moderately effective • Not effective • Not yet available
9.1. Details	Alphanumeric	
10. What is the current status of the incident?	Choice (multiple) – Select one option	• Resolved • Contained • Ongoing • Unknown
10.1. Provide the date and time when then incident was closed or is expected to be closed if known	yyyy-mm-dd hh:mm	