

FiMiS - User Guide for DORA_INCIDENT- and DORA_CYBERTHREAT-Surveys

Table des matières

I.	APERÇU GÉNÉRAL	2
II.	ACCES A FiMiS	3
III.	PREMIÈRE UTILISATION DE FiMiS	4
1.	Accéder à FiMiS	4
2.	Choix d'un certificat	4
3.	Premiers écrans lors de l'enregistrement sur la plateforme FiMiS	4
4.	La page de log-on	6
IV.	ACCES AUX SURVEYS	8
1.	Via l'onglet « My eDossier »	8
2.	Via l'onglet « Dossiers »	8
3.	Via l'onglet « Surveys »	10
4.	Création d'une nouvelle survey	10
V.	LIGNES DIRECTRICES POUR REMPLIR LES SURVEYS DORA_INCIDENT ET DORA_CYBERTHREAT	11
1.	Préalable	11
2.	Création d'une nouvelle survey DORA_INCIDENT- ou DORA_CYBERTHREAT	12
3.	Compléter la survey DORA_INCIDENT	13
a.	Généralités	13
b.	Section "General information about the financial entity"	14
c.	Section notification	15
d.	Reclassification d'un incident majeur lié aux TIC en un incident non majeur lié aux TIC	17
4.	Compléter la survey DORA_CYBERTHREATS	18
5.	Soumettre les surveys DORA_INCIDENT et DORA_CYBERTHREAT	18
6.	Validation report: errors et warnings	19
	Annexe 1 : liste des champs à remplir dans la survey DORA_INCIDENT	21
	Annexe 2 : liste des champs à remplir dans la survey DORA_CYBERTHREAT	44

I. APERÇU GÉNÉRAL

Ce document est un guide d'utilisation des surveys FiMiS "DORA_INCIDENT" et "DORA_CYBERTHREAT". Ces surveys vous permettent, conformément aux attentes du Règlement sur la résilience opérationnelle numérique (ci-après DORA), de signaler à la FSMA les incidents majeurs liés aux TIC ou les cybermenaces importantes dont votre entité a été victime. La FSMA notifiera ces incidents à son tour aux autorités européennes de surveillance (AES).

Tout d'abord, le guide explique comment accéder à l'environnement sécurisé FiMiS et comment utiliser cette application.

Dans un second temps, le guide abordera le fonctionnement des surveys DORA_INCIDENT et DORA_CYBERTHREAT, qui ont été établies conformément aux exigences du règlement DORA. Dans les annexes de ce document, vous trouverez les exigences précises relatives aux différents champs à remplir.

La déclaration d'un incident se compose de trois phases successives : la notification initiale, le rapport intermédiaire et le rapport final. Selon la phase, le niveau d'informations requis varie. Le cas échéant, une reclassification de l'incident majeur en non majeur est également prévue. En revanche, la notification des cybermenaces majeures se déroule en une seule étape.

La FSMA transmet sans délai aux AES les surveys correspondant à une phase spécifique de la notification. À partir de ce moment, aucune modification ultérieure de la survey soumise n'est autorisée. Il est donc essentiel de faire preuve de rigueur lors du remplissage de ces enquêtes

Toutefois, en ce qui concerne spécifiquement les déclarations d'incidents, des modifications peuvent encore être apportées à des stades ultérieurs du processus de notification. Ainsi, si une valeur incorrecte a été saisie lors de la soumission d'une survey pour une notification intermédiaire, cette valeur peut être corrigée lorsque la survey est soumise pour une notification finale.

Si vous êtes dans l'impossibilité de vous connecter suite à un incident majeur lié aux TIC à la plateforme FiMiS et à la survey concernée, vous pouvez exceptionnellement contacter la FSMA (voir aussi : [Précisions sur la collecte du registre d'informations sur les prestataires tiers et sur les déclarations d'incidents majeurs liés aux TIC | FSMA](#)) par :

- e-mail: dora@fsma.be ;
- ou par téléphone : +32(0)2 220 52 11.

Les instructions ci-dessous clarifient le fonctionnement des surveys "DORA_INCIDENT" et "DORA_CYBERTHREAT". Toutefois, en cas de difficulté, nous vous invitons à contacter la FSMA :

- à l'adresse dora@fsma.be pour toute question concernant le contenu des surveys respectives ;
- à l'adresse Servicedesk@fsma.be pour des problèmes techniques liés à FiMiS.

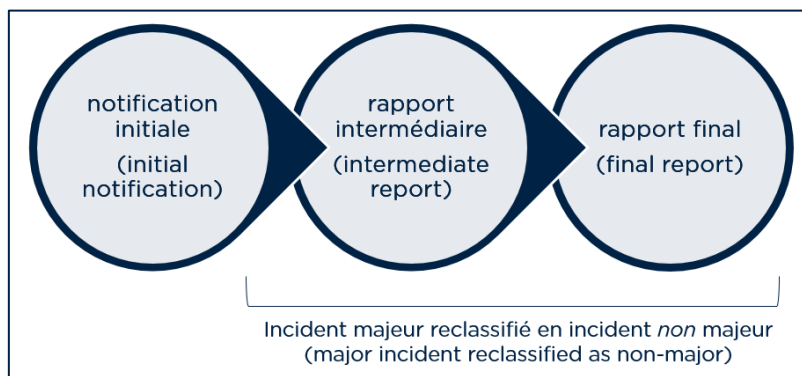


Figure 1: Processus de notification des incidents liés aux TIC

II. ACCES A FiMiS

Pour accéder à FiMiS, chaque utilisateur doit disposer d'un certificat personnel. L'utilisateur a le choix parmi les options suivantes :

- Globalsign Personal 3 (<http://www.globalsign.be>) ;
- Isabel (<http://www.isabel.be>) ;
- Votre carte d'identité électronique (eID) (<http://eid.belgium.be>).

Remarques :

- Les cartes Isabel et les cartes d'identité électroniques nécessitent un lecteur de cartes.
- L'utilisation de l'eID nécessite le téléchargement du logiciel eID (<http://eid.belgium.be>).

Un certificat vous est délivré par une tierce partie autorisée. Après acquisition, le certificat doit être installé sur le PC qui sera utilisé pour accéder à FiMiS conformément aux recommandations du fournisseur.

Pour plus d'informations, nous vous invitons à prendre contact avec le fournisseur de votre certificat.

Le certificat est strictement personnel. Chaque utilisateur doit donc avoir son propre certificat.

III. PREMIÈRE UTILISATION DE FiMiS

1. Accéder à FiMiS

Accédez à FiMiS via le « [Guichet digital](#) » du site web de la FSMA. Cliquez ensuite sur le bouton « **FiMiS Survey** ».

2. Choix d'un certificat

Si plusieurs certificats sont installés sur votre PC, le système vous demande de choisir celui que vous souhaitez utiliser.

- Pour l'eID : Cliquez sur le certificat "Citizen CA xxxx" puis sur OK.
- Pour un autre certificat : cliquez sur le certificat puis sur OK.



Si vous utilisez une carte Isabel ou une carte d'identité électronique, il vous sera demandé d'introduire votre code.



Introduisez-le et cliquez sur OK.

Attention: il s'agit de votre code PIN ou de votre code Isabel, pas du code d'activation.

3. Premiers écrans lors de l'enregistrement sur la plateforme FiMiS

Vous êtes désormais identifié comme possédant un certificat valide. Si l'écran ci-dessous n'apparaît pas, cela signifie que l'installation du certificat s'est mal déroulée. Prenez dans ce cas contact avec le Service Desk de la

FSMA (Servicedesk@fsma.be).

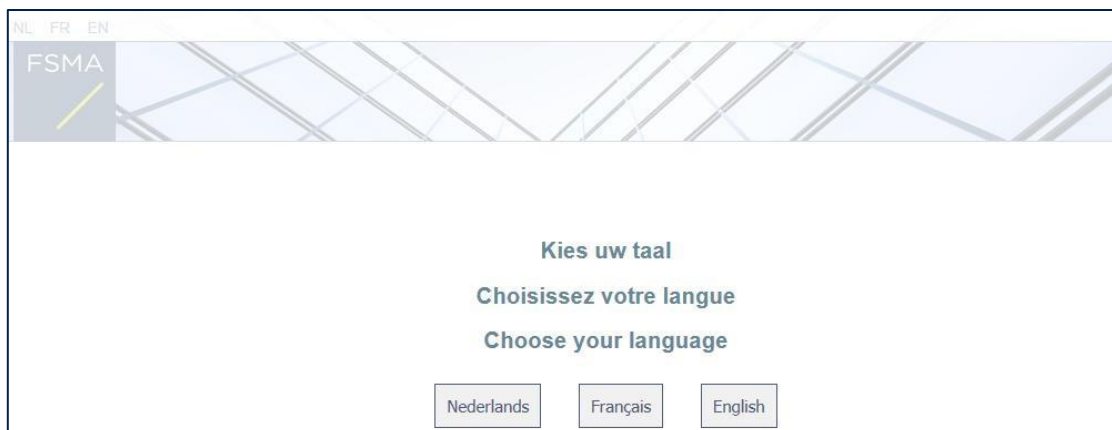


Figure 2: écran de sélection de la langue dans FiMiS

Le choix de la langue détermine la langue dans laquelle vous souhaitez travailler. Celle-ci peut encore être modifiée ultérieurement. Les surveys DORA_INCIDENT et DORA_CYTBERTHREAT seront disponibles dans trois langues (néerlandais, français, anglais).

ATTENTION !

Etant donné que les normes techniques réglementaires (RTS et ITS) concernées n'ont pas encore été publiées, la FSMA n'a pour l'instant développé la survey qu'en anglais, sur la base des instructions communiquées à la FSMA par les AES. Dès que les textes réglementaires concernés seront publiés, la FSMA proposera également les surveys en néerlandais et en français.

Pour utiliser FiMiS, vous devez également accepter la clause relative au traitement des données personnelles (voir la figure 3 : clause relative à l'utilisation des données personnelles).

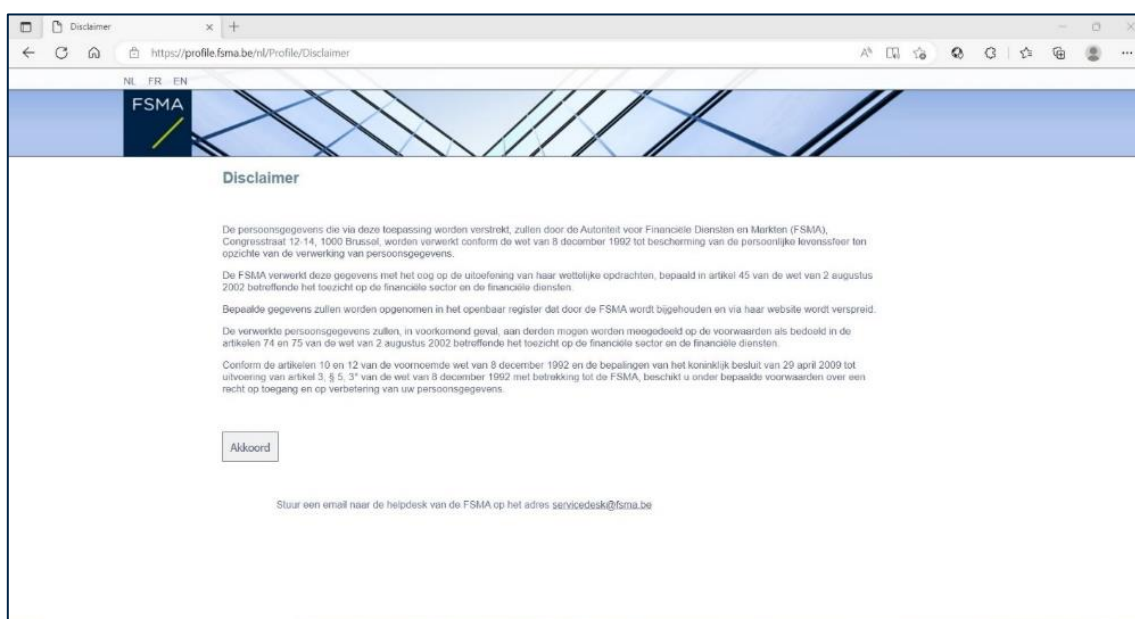


Figure 3: clause relative à l'utilisation des données personnelles

Enfin, l'application vous demande de saisir vos données d'identification (voir la figure 4 : écran d'enregistrement de votre profil d'utilisateur). Vous ne devez le faire qu'une seule fois. Une fois que vous avez terminé, cliquez sur « Register » et l'application FiMiS sera lancée.

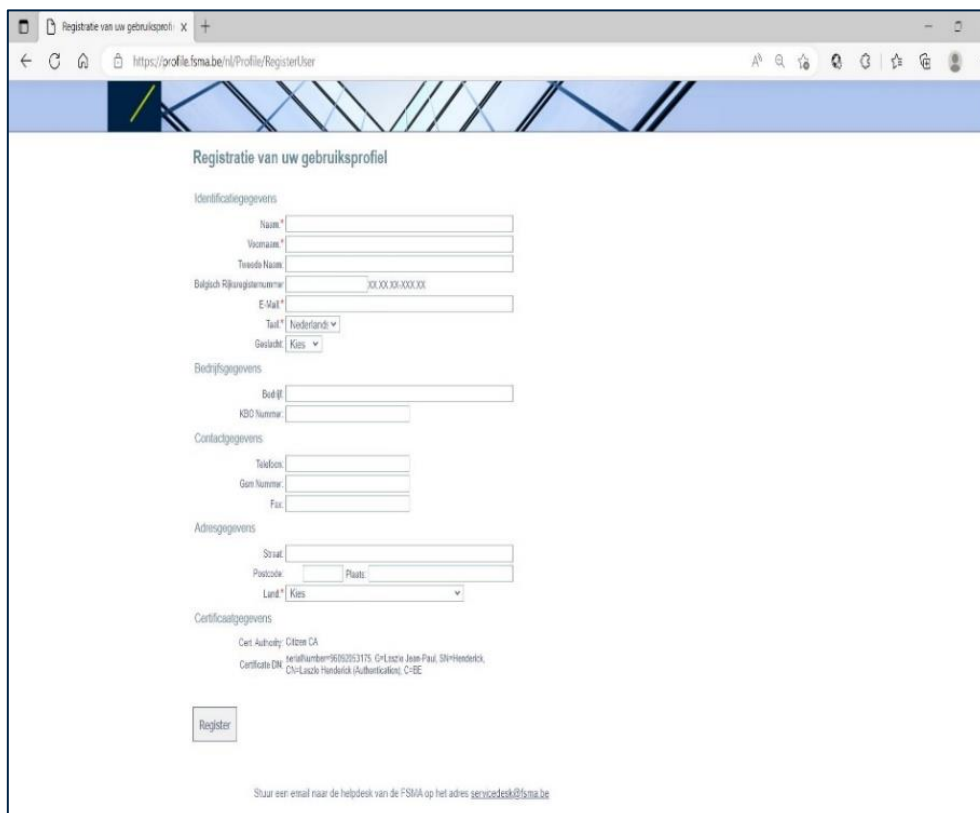


Figure 4: écran d'enregistrement de votre profil d'utilisateur

4. La page de log-on

Lors de la première connexion à FiMiS, l'utilisateur doit introduire le code d'activation que la FSMA lui a transmis.



Cette identification est alors couplée automatiquement par nos soins au certificat que vous utilisez de manière à ce qu'à la prochaine utilisation, l'identification par code d'activation soit superflue. Vous obtenez alors la page d'accueil de FiMiS.

IV. ACCES AUX SURVEYS

Il y a trois façons d'accéder à des surveys spécifiques :

- Via l'onglet « Mon eDossier »
- Via l'onglet « Dossiers »
- Via l'onglet « Surveys »

1. Via l'onglet « My eDossier »

L'onglet “**My eDossier**” (voir la figure 6: écran My eDossier) vous donne un aperçu des dossiers et des surveys auxquels vous avez accès et quelques informations clés sur ces dossiers.

Cet écran est organisé en 4 volets :

- Surveys : tous les reportings des entités qui vous concernent ;
- Dossiers : toutes les entités pour lesquelles vous avez été désigné(e) comme personne de contact;
- I Want To : les actions disponibles - dans cette section, vous pouvez lancer une nouvelle survey en cliquant sur « New Survey »;
- Links : les liens vers d'autres sites.

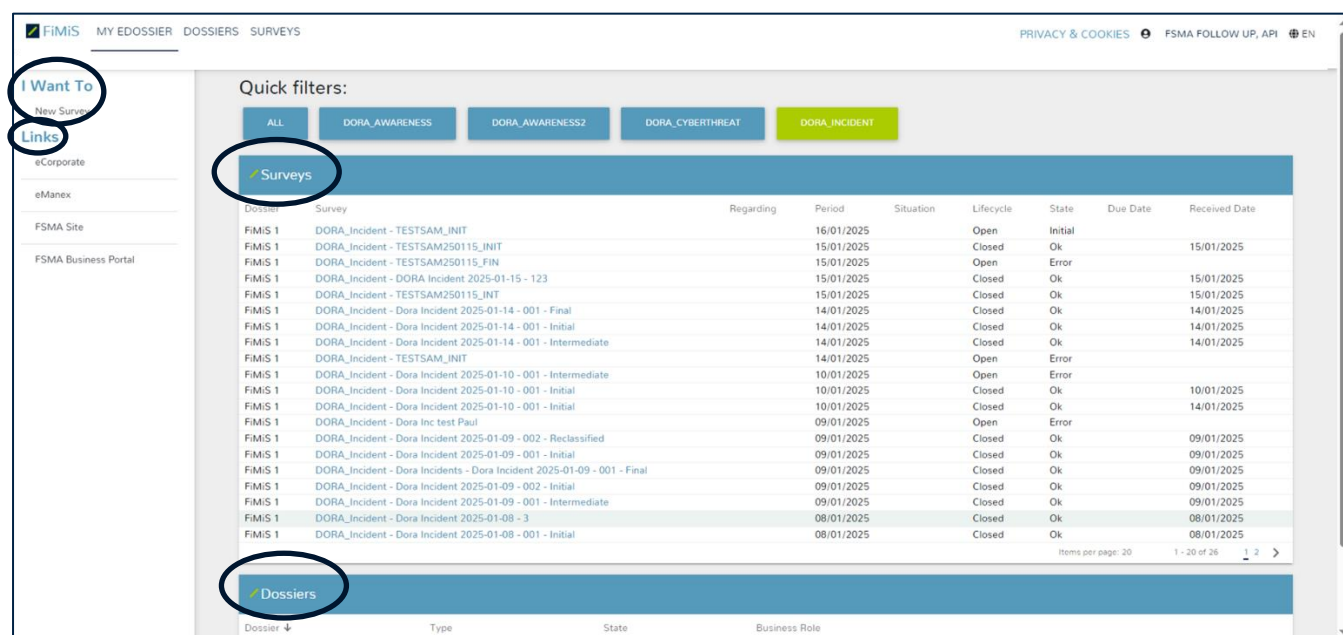


Figure 6: écran My eDossier

Cliquer sur une Survey vous amène à l'onglet Surveys pour celle-ci.

Cliquer sur un Dossier vous amène à l'onglet Dossiers pour celui-ci (c'est-à-dire l'entreprise concernée par le reporting).

2. Via l'onglet « Dossiers »

Cet onglet (voir la figure 7: écran Dossiers) vous permet soit de visualiser l'ensemble des dossiers auxquels

vous avez accès, soit de limiter la visualisation aux dossiers qui répondent aux filtres introduits, soit de visualiser les informations d'un dossier sélectionné depuis un autre onglet.

Cliquer sur un dossier vous amène à un écran qui fournit des informations complémentaires sur ce dossier et sur sa liste de surveys. Cliquer sur une de ces surveys vous amène ensuite à l'onglet Surveys pour celle-ci.

https://fimis-test.fsma.be/nl/Do... x

https://fimis-test.fsma.be/nl/Dossier/Detail?dossierId=1853dd55-b579-41ce-a110-eb88274b0943

FIMIS MY EDOSSIER DOSSIERS SURVEYS

PRIVACY & COOKIES FSMA FOLLOW UP, POL NL

FIMIS 1

Info

Surveys

Parameters

Info

Officiële naam FIMIS 1

Type Company

Status Open

Main domain IORP - Prudentieel toezicht op de Instellingen voor bedrijfspensioenvoorziening

Surveys

Survey	Betreft	Periode	Situation	Lifecycle	Status	Deadline	Ontvangen
InsFamily -		18/01/2023		Open	Error		
InsFamily -		18/01/2023		Open	Initial		
InsFamily -		12/01/2023		Open	Ok		
InsFamily -		19/12/2022		Closed	Ok	20/12/2022	
InsFamily -		09/12/2022		Open	Error		
InsFamily -		22/11/2022		Open	Error		
InsFamily -		21/11/2022		Open	Error		
InsFamily -		18/11/2022		Open	Error		
InsFamily -		18/11/2022		Open	Error		
InsFamily -		18/11/2022		Closed	Ok	18/11/2022	

Items per page: 20 1 - 10 of 10

Figure 7: écran Dossiers

3. Via l'onglet « Surveys »

Cet onglet (voir la figure 8: écran Surveys) vous permet soit de visualiser l'ensemble des surveys pour lesquelles vous avez été désigné(e) comme personne de contact, soit de limiter la visualisation aux surveys qui répondent aux filtres introduits, soit de visualiser les informations d'une survey sélectionnée depuis un autre onglet. Cliquer sur une survey permet ensuite de voir ses différentes sections et de rentrer dans celles-ci.

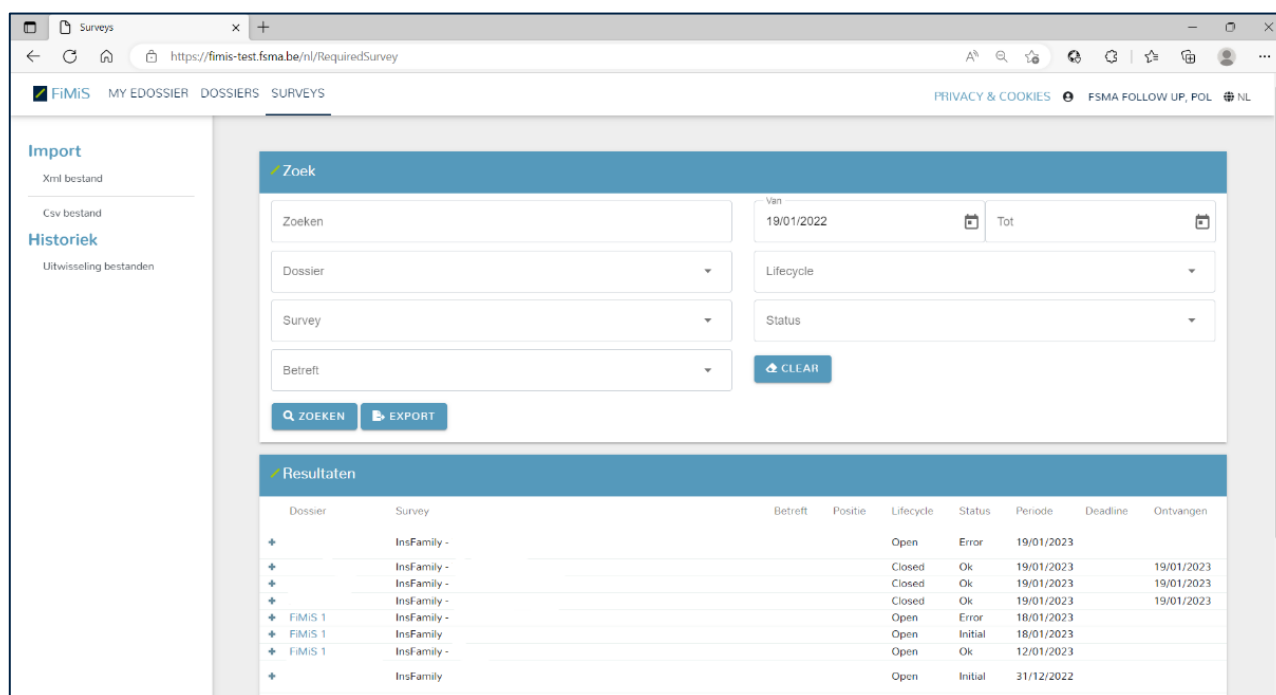


Figure 8: écran Surveys

4. Création d'une nouvelle survey

Pour créer une nouvelle survey, naviguez sur l'écran « My eDossiers » (voir Figure 6 : écran My eDossiers) ; dans la section « I want to » cliquez ensuite sur « New Survey. » L'écran « New Survey » s'ouvre (voir ci-après la figure 9 : écran New Survey).

Pour chaque notification d'un incident majeur lié aux TIC, pour chaque modification dans une nouvelle phase du processus de notification d'un incident déjà notifié, ou pour chaque notification d'une cybermenace importante, une nouvelle survey doit être créée de cette façon.

V. LIGNES DIRECTRICES POUR REMPLIR LES SURVEYS DORA_INCIDENT ET DORA_CYBERTHREAT

1. Préalable

Concernant la notification d'un **incident majeur lié aux TIC** (DORA_INCIDENT-survey):

- Le processus de notification d'un incident majeur lié aux TIC comprend **trois phases** (voir également la figure 1 : processus de notification d'un incident TIC) : la notification initiale, le rapport intermédiaire et le rapport final. Pour chaque phase de la notification (initiale, intermédiaire, finale), une nouvelle survey doit être créée dans FiMiS. Les informations saisies dans les surveys dans le contexte des notifications précédentes peuvent être rechargées en sélectionnant la survey précédemment soumise dans « previous survey » (voir **1** dans la figure 9 : écran New Survey).
- Une fois qu'une survey DORA_INCIDENT (qu'il s'agisse d'une notification initiale, d'un rapport intermédiaire ou final) est soumise, elle est **automatiquement et immédiatement envoyée** aux AES. **Par conséquent, aucun ajustement de la survey n'est possible après qu'elle a été soumise.** Une notification initiale ne peut être ajustée que lors de la soumission du rapport intermédiaire (voir ci-avant). La notification initiale et le rapport intermédiaire peuvent être ajustés lors de la saisie du rapport final (voir ci-avant). Toutefois, une fois le rapport final soumis, il n'est plus possible de procéder à des ajustements.
- Un seul champ de la survey DORA_INCIDENT est définitif après la soumission de la notification initiale. Il s'agit du **code de référence de l'incident attribué par l'entité financière** (« Incident reference code assigned by the financial entity »), qui doit être saisi au moment de la notification initiale. La valeur introduite dans ce champ est définitive car elle est utilisée comme référence unique tout au long du processus de notification d'incident pour identifier l'incident (tant par la FSMA que par les AES).
- **Il est donc fortement recommandé de remplir la survey à chaque phase du processus de notification d'incident avec prudence, de la manière la plus correcte et la plus complète possible.**

Concernant la notification volontaire d'une **cybermenace** (DORA_CYBERTHREAT-survey):

- La notification volontaire d'une cybermenace ne nécessite qu'une seule survey. Cette notification est également transmise automatiquement et immédiatement aux AES. Par conséquent, une fois que vous avez soumis cette notification, aucune modification n'est possible.
- Il est donc fortement recommandé de remplir la survey pour la notification d'une cybermenace avec prudence, de la manière la plus correcte et la plus complète possible.

2. Création d'une nouvelle survey DORA_INCIDENT- ou DORA_CYBERTHREAT

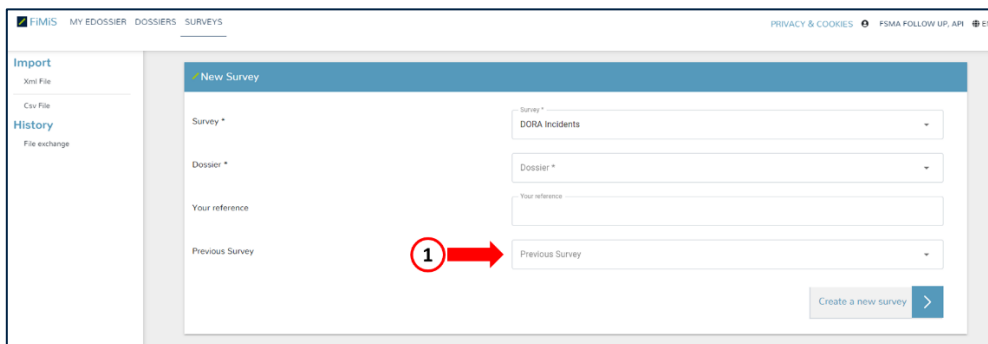


Figure 9: écran "New Survey"

Si vous devez notifier à la FSMA un nouvel incident majeur lié aux TIC¹ ou si vous souhaitez compléter les informations relatives à un incident existant (pour le rapport intermédiaire ou final), vous devez créer une nouvelle survey.

Dans l'écran « New Survey » (voir la figure 9), vous devez remplir au moins les champs suivants :

- Dans le champ « Survey », vous devez choisir le type de survey (dans ce cas, DORA INCIDENTS).
- Dans le champ « Dossier », vous devez indiquer pour quelle entité vous souhaitez créer une survey.
- Dans le champ « Your reference », vous pouvez ajouter votre propre référence à la survey afin de la retrouver plus facilement par la suite.
- Si la survey ne concerne pas une notification initiale mais un rapport intermédiaire ou final, vous pouvez sélectionner une survey précédemment soumise dans le champ « Previous Survey » (voir ¹ dans la figure 9). De cette manière, tous les champs déjà remplis de la survey précédente seront rechargés dans la nouvelle survey.
- Cliquez après sur « Create a new survey » pour passer à l'écran suivant.

¹ Pour les critères de classification des incidents majeurs liés aux TIC et des cybermenaces importantes, voir le *regulatory technical standard* (RTS) « for the classification of ICT-related incidents and cyber threats » ([Delegated regulation - EU - 2024/1772 - EN - EUR-Lex](#)) ou la documentation pédagogique relative à DORA sur le site web de la FSMA ([Règlement DORA | FSMA](#)).

3. Compléter la survey DORA_INCIDENT

Le remplissage de la survey DORA_INCIDENT, qui a été entièrement conçue selon les attentes des AES, est en principe très intuitif. Cependant, il y a quelques points à prendre en compte.

Figure 10: écran 'General information about the financial entity'

a. Généralités

- La survey se compose de deux sections (voir ① dans la figure 10 : écran 'General information about the financial entity'), à savoir une section « General information about the financial entity » et une section « Notification ». Vous pouvez passer d'une section à l'autre en cliquant sur « Next » ou sur le nom correspondant dans la partie « Sections ». Lorsque la section « General information about the financial entity » est correctement remplie, vous pouvez naviguer à la section « Notification ».
- Dans la partie « Actions », vous avez la possibilité d'exporter la survey au format PDF ou Excel. L'option de charger la dernière survey disponible apparaît également ; toutefois, étant donné que dans le cas de la notification d'incidents majeurs liés aux TIC ou de cybermenaces importantes, une survey est définitive dès qu'elle a été soumise, cette option ne sera pas disponible. La modification d'une notification d'un incident majeur lié au TIC est seulement possible en créant une nouvelle survey dans une phase ultérieure (intermédiaire ou finale – voir ci-avant). La modification d'une notification d'une cybermenace importante n'est pas possible du tout dès qu'elle a été soumise (voir ci-avant).
- En outre, il existe un autre bouton « Submit the survey », qui s'allume en bleu une fois que toutes les données saisies ont été validées.
- En dessous de ce bouton se trouve un autre bouton qui vous permet de revenir à l'aperçu général de toutes les surveys (« back to dashboard »).

INFORMATIONS IMPORTANTES

La valeur attendue pour chaque champ à remplir sera précisée par les AES dans un *implementing technical standard* (ITS). Ce document n'est pas encore publié au Journal Officiel de l'UE. Dans l'attente de cette publication, un fichier Excel a été mis à la disposition de la FSMA par les AES, clarifiant les valeurs attendues par champ. Pour votre commodité, nous avons copié le tableau correspondant dans

l'annexe 1 : liste des champs à remplir dans la survey DORA_INCIDENT. La numérotation des champs utilisée dans le fichier Excel (et repris dans l'annexe 1) correspond à la numérotation telle qu'elle figure dans la survey DORA_INCIDENT dans FiMiS. Cela devrait vous permettre de retrouver facilement les informations requises pour chaque champ.



- Selon le type de notification que vous sélectionnez (initial, intermédiaire, final ou reclassification ; voir 2 dans la figure 10: écran 'General information about the financial entity'), les règles de validation pour la section « Notification » seront affectées, de même que le nombre de champs à remplir pour soumettre la survey relative à la notification d'un incident majeur lié aux TIC.
- Il est possible de soumettre un rapport intermédiaire ou final sans soumettre une notification initiale ou un rapport intermédiaire au préalable. Pour cela, dans le champ « Type of report », sélectionnez la phase de la notification que vous souhaitez soumettre (voir 2 dans la figure 10: écran 'General information about the financial entity'). Toutefois, veuillez noter que le fait d'omettre une phase du processus de notification ne vous dispense pas de remplir tous les champs demandés dans les phases de notification précédentes.
- Tout au long de la survey, vous verrez régulièrement le symbole plus (+). En cliquant sur ce symbole, vous pouvez ajouter une ligne avec une option de réponse supplémentaire. Par exemple, dans le cas des champs 1.4, 1.5 et 1.6 (voir 3 dans la figure 10: écran 'General information about the financial entity'), vous pouvez ajouter des lignes supplémentaires si votre entité a plusieurs statuts (par exemple un « Management Company » et un « Manager of alternative investment fund »).

b. Section “General information about the financial entity”

- En cas de problème de format de la valeur saisie (« pattern check ») pour le code LEI (mais aussi pour les indications de date et d'heure, et également pour les autres valeurs comme les pourcentages), le message d'erreur s'affichera dans le champ lui-même et non dans le rapport de validation (voir la figure 11 : code LEI incorrect (« pattern check »)). Le format doit être corrigé avant de pouvoir poursuivre la survey. Si la validité du code LEI (« check digits ») pose problème, elle sera incluse dans les « errors » (voir V.6. Validation report: errors et warnings).



Figure 11: code LEI incorrecte (« pattern check »)

- Aucun contrôle spécifique n'est prévu pour l'EU ID. Compte tenu de l'absence de ce contrôle pour l'EU ID et du fait que les autres champs demandent principalement le code LEI, nous recommandons vivement d'opter pour le code LEI si vous avez le choix entre les deux
- Lorsque toutes les données ont été correctement introduites, il sera possible de les valider et de les sauvegarder () et ainsi de passer () à la notification effective de l'incident majeur lié aux TIC (section « Notification »).

L'introduction de données dans la section « General information about the financial entity » ne doit se faire qu'au moment de la notification initiale d'un incident majeur lié aux TIC, ou, si vous décidez d'omettre la

notification initiale ou le rapport intermédiaire, respectivement dans le rapport intermédiaire ou final. Par la suite, ces données seront automatiquement reprises dès que vous ferez référence à une survey précédente lors de la création d'une nouvelle survey pour un rapport intermédiaire ou final en complétant le champ « Previous Survey » (voir ① dans la figure 9 : écran « New survey »).

c. Section notification

Les informations requises dans chaque champ sont décrites dans l'**annexe 1 : liste des champs à remplir dans la survey DORA_INCIDENT** du présent guide. La numérotation de chaque champ dans cette annexe correspond à la numérotation des champs dans la survey, ce qui vous permet de trouver facilement les informations requises.

The screenshot displays the 'Notification' section of the FIMI S system. The sidebar on the left contains navigation links for 'FIMI S', 'MY EDOSSIER', 'DOSSIERS', and 'SURVEYS'. Below these, there are sections for 'Sections' (General information about the f..., Notification) and 'Actions' (Load Last Submitted Survey, Export Survey to PDF, Export Survey to Excel, Submit the Survey, Back to Dashboard). The main form area is titled 'Notification' and includes tabs for 'Initial', 'Intermediate', and 'Final'. The form contains several fields and sections: 'Incident response code assigned by the financial entity' (2.1), 'Date and time of detection of the ICT-related incident' (2.2), 'Date and time of classification of the incident as major' (2.3), 'Description of the ICT-related incident' (2.4), 'Classification criteria that triggered the incident report' (2.5), 'Materiality thresholds for the classification criterion "Geographical spread"' (2.6), 'Discovery of the major ICT-related incident' (2.7), 'Indication whether the incident originates from a third party provider or another financial entity' (2.8), 'Activation of business continuity plan, if activated' (2.9), and 'Other relevant information' (2.10). Red circles and arrows highlight specific elements: 1 points to the 'Initial' tab, 2 points to the incident response code field, 3 points to the 'Submit the Survey' button, 4 points to the 'Validate & Save' button, and 5 points to the 'Description of the ICT-related incident' field.

Figure 12: écran section "Notification" – partie 1

Figure 13: écran section "Notification" – partie 2

Cependant, dans la section « Notification », il y a aussi quelques points qui méritent une explication :

- Il est possible de déjà ajouter des informations demandées dans les phases ultérieures du processus de notification, et d'ajuster des informations déjà complétées. Pour passer d'une phase à l'autre de la notification, il suffit de cliquer sur « initiale », « intermédiaire » ou « finale » au numéro ① dans la figure 12 : section d'écran « Notification » - partie 1, ou sur « next » au numéro ④ dans la même figure.
- Certains champs nécessitent une **indication de la date et de l'heure** (voir par exemple ② dans la figure 12 : section d'écran « Notification » - partie 1). Les AES utilisent la norme ISO8601 à cette fin. La FSMA a adopté cette norme dans cette survey. Par conséquent, la date et l'heure doivent être notées dans le format suivant : YYYY-MM-DDThh:mm:ss, où
 - YYYY représente l'année en 4 chiffres
 - MM représente le mois en 2 chiffres
 - DD représente le jour en 2 chiffres
 - T indique que ce qui suit est l'indication de l'heure
 - hh est l'heure en 2 chiffres
 - mm représente les minutes en 2 chiffres
 - ss indique les secondes en 2 chiffres
 - Par exemple :
 - Si l'incident a été découvert le **17 janvier 2025 à 12h23**, il doit être noté comme suit : **2025-01-17T12:23:00**.
 - Si vous n'avez pas saisi la date et l'heure dans le bon format, un message d'erreur (voir la figure 14) apparaîtra dans le champ. Vous ne pourrez pas poursuivre la survey (i.e. cliquer sur « Suivant » ni passer à une autre étape du processus de notification, ni cliquer sur « Valider et enregistrer ») tant que la date et l'heure n'auront pas été saisies dans le bon format.

Figure 14: message d'erreur pour un format incorrect de l'indication de la date et de l'heure (« pattern check »)

- Dans certains champs, vous devrez spécifier **une durée** (par exemple dans le champ relatif au « Service

downtime » - voir ⁶ dans la figure 13 : écran section « Notification » - partie 2). La durée doit être exprimée au format **DDD:HH:MM**, où DDD est le nombre de jours, HH est le nombre d'heures (qui ne peut pas dépasser 23) et MM est le nombre de minutes (qui ne peut pas dépasser 59).

- Par exemple : un incident d'une durée de **74 heures et 32 minutes** doit donc être noté **003:02:32**.
- Si le format dans lequel la durée a été introduite est incorrect, un message d'erreur apparaît dans le champ. Vous devez corriger le champ avant de pouvoir continuer (cf. indication de la date et de l'heure ci-dessus).

d. Reclassification d'un incident majeur lié aux TIC en un incident non majeur lié aux TIC

- Si l'incident majeur lié aux TIC précédemment notifié doit être reclassifié en incident *non* majeur sur base d'une réévaluation des critères qui avaient causé la classification de l'incident comme majeur au moment de la découverte de l'incident², vous pouvez le faire en sélectionnant « Major incident reclassified as non-major » dans la section « General information about the financial entity » dans le champ « Type of report » (voir ² dans la figure 10 : écran « General information about the financial entity »).
- Quand vous décidez de reclassifier l'incident en *non* majeur, vous devez préciser les raisons de la reclassification dans le champ 2.10 « Autres informations pertinentes » de la section « Notification » de la notification initiale (voir ³ dans la figure 12 : écran section « notification » - partie 1).
- La pertinence et l'exhaustivité des raisons de la reclassification peuvent être évaluées par la FSMA après que vous avez soumis la survey.

² Voir pour les critères de classification le RTS « for the classification of ICT-related incidents and cyber threats » ([Delegated regulation - EU - 2024/1772 - EN - EUR-Lex](#)) ou la documentation pédagogique relative à DORA dossier thématique DORA sur le site web de la FSMA ([Règlement DORA | FSMA](#)).

4. Compléter la survey DORA_CYBERTHREATS



Figure 15: écran Significant Cyber Threats

Pour la survey DORA_CYBERTHREAT, une seule section doit être remplie (« Significant Cyber Threats »). Pour connaître les exigences relatives à chaque champ à remplir, vous trouverez les informations nécessaires dans **l'annexe 2 : liste des champs à remplir dans la survey DORA_CYBERTHREAT**. Les numéros accompagnant les champs de la survey DORA_CYBERTHREAT correspondent aux numéros utilisés dans l'annexe 2, ce qui devrait vous permettre de trouver facilement les informations nécessaires sur les exigences par champ.



En général, les mêmes directives que celles expliquées pour la survey DORA_INCIDENT (voir chapitre précédent) sont valables pour remplir la survey DORA_CYBERTHREAT.

Ainsi, certaines exigences en matière de format doivent également être prises en compte, notamment pour le code LEI et pour l'indication de la date et l'heure (conformément à la norme ISO8601 – voir ① dans la figure 15 : écran Significant Cyber Threats). Ces exigences de format sont les mêmes que celles déjà expliquées dans la partie précédente de ce document (voir également ② dans la figure 12 : écran section « Notification » - partie 1). Si le format n'est pas respecté, un message d'erreur apparaît dans le champ lui-même. Vous devez le corriger avant de pouvoir continuer à valider et à soumettre la survey. Pour plus d'explications, voir également ci-dessus.

5. Soumettre les surveys DORA_INCIDENT et DORA_CYBERTHREAT

- Une fois toutes les données correctement saisies, il sera possible de les valider et de les enregistrer () et de passer ainsi () à la section suivante (voir ④ dans la figure 12 : écran section « Notification » - partie 1 ou ② dans la figure 15 : écran « Significant Cyber Threats »).
- En cas d'erreurs de saisie, celles-ci apparaîtront dans le « validation report ». Vous devez d'abord les

corriger (voir le chapitre V.6. Validation report : errors et warnings).

- Les champs à remplir obligatoirement dans le cadre d'une notification d'un incident majeur lié aux TIC dépendent de la phase de notification pour laquelle vous souhaitez soumettre la survey. Les champs obligatoires du rapport intermédiaire ou final ne provoqueront pas d'erreurs lors de la soumission d'une survey pour une notification initiale.
- Une fois que vous avez pu valider () définitivement la survey après avoir corrigé les erreurs (« errors ») indiquées, vous pouvez soumettre la survey. Pour ce faire, cliquez sur  sur le côté gauche de l'écran.
- Une fenêtre pop-up apparaît expliquant que la survey devient désormais « read only » et qu'aucune modification ne peut plus être apportée.

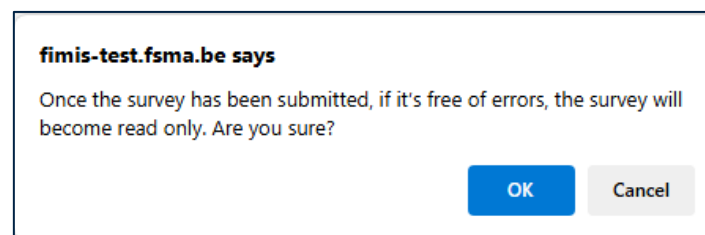


Figure 16: message au moment de la soumission de la survey

6. Validation report: errors et warnings

Si vous n'avez pas, ou incorrectement, rempli certains champs, FiMiS vous l'indiquera dans le rapport de validation. Celui-ci apparaît dans le coin supérieur gauche de l'écran de la survey lorsque vous essayez de valider et d'enregistrer les informations saisies (voir la figure 17 : validation report).



Figure 17: Validation report

Vous pouvez consulter ce rapport en cliquant sur la flèche bleue à côté de « Validation report » (voir cercle rouge dans la figure 17 : validation report). Deux types de problèmes liés aux données introduites peuvent se présenter :

- **Errors** : il s'agit de champs obligatoires qui n'ont pas été remplis ou qui l'ont été de manière incorrecte. Les erreurs empêchent la soumission de la notification et doivent donc être corrigées.
- **Warnings** : il s'agit de champs qui n'ont pas été remplis ou qui l'ont été de manière incorrecte mais qui ne bloquent pas la soumission effective de la notification.

Dans la survey DORA_INCIDENT, les deux types de problèmes diffèrent en fonction de la phase de la notification pour laquelle vous soumettez la survey. Par exemple, le rapport final nécessite beaucoup plus de données que la notification initiale.

Les *errors* et les *warnings* indiqués sont conformes aux règles de validation définies par les AES. Vous pouvez également consulter ces règles dans l'annexe 1 : liste des champs à remplir dans la survey DORA_INCIDENT » dans les trois dernières colonnes :

- Mandatory for initial report
- Mandatory for intermediate report
- Mandatory for final report

Pour la notification d'une cybermenace, les *errors* et les *warnings* inclus dans la survey sont conformes aux règles de validation définies par les AES. Vous pouvez les consulter dans la dernière colonne (« Mandatory field ») de l'annexe 2 : liste des champs à remplir dans la survey DORA_CYBERTHREAT.

Annexe 1 : liste des champs à remplir dans la survey DORA_INCIDENT



Source: DORA Incident reporting Template

En attendant la publication au Journal Officiel de l'UE de l'ITS concerné, la présente liste n'est disponible qu'en anglais.

Field Code	Field Name	Description	Field Type	Mandatory for initial report	Mandatory for intermediate report	Mandatory for final report
General information about the financial entity (initial notification tab)						
1.1	Type of submission	Indicate the type of incident notification or report being submitted to the competent authority.	Choice: - initial notification - intermediate report - final report - major incident reclassified as non-major	Yes	Yes	Yes
1.2	Name of the entity submitting the report	Full legal name of the entity submitting the report.	Alphanumeric	Yes	Yes	Yes
1.3a	Identification code of the entity submitting the report (LEI)	Identification code of the entity submitting the report. Where financial entities submit the notification/report, the identification code shall be a Legal Entity Identifier (LEI), which is a unique 20 alphanumeric character code, based on ISO 17442-1:2020.	Alphanumeric	Yes. if field 1.3b is empty	Yes. if field 1.3b is empty	Yes. if field 1.3b is empty
1.3b	Identification code of the entity submitting the report (EU ID)	Identification code of the entity submitting the report. A third-party provider that submits a report for a financial entity can use an identification code as specified in the implementing technical standards adopted pursuant to Article 28(9) of Regulation (EU) 2022/2554.	Alphanumeric	Yes. if field 1.3a is empty	Yes. if field 1.3a is empty	Yes. if field 1.3a is empty

1.4	Type of the affected financial entity	<p>Type of the entity as referred to in Article 2(1). points (a) to (t). of Regulation (EU) 2022/2554 for whom the report is submitted.</p> <p>In case of aggregated reporting as referred to in Article 7 of this Regulation. the different types of financial entities covered in the aggregated report to be selected.</p>	<p>Choice (multiselect):</p> <ul style="list-style-type: none"> - investment firm - trading venue - manager of alternative investment fund - management company - insurance intermediary. - reinsurance intermediary and ancillary insurance intermediary - institution for occupational retirement provision - crowdfunding service provider 	Yes	Yes	Yes
1.5	Name of the financial entity affected	<p>Full legal name of the financial entity affected by the major ICT-related incident and required to report the major incident to its competent authority under Article 19 of Regulation (EU) 2022/2554.</p> <p>In case of aggregated reporting:</p> <p>(a) list of all names of the financial entities affected by the major ICT-related incident. separated by a semicolon.</p> <p>(b) the third-party provider submitting a major incident notification or report in an aggregated manner as referred to in Article 7 of this Regulation. to list the names of all financial entities impacted by the incident. separated by a semicolon.</p>	Alphanumeric	Yes. if the financial entity affected by the incident is different from the entity submitting the report and in case of aggregated reporting.	Yes. if the financial entity affected by the incident is different from the entity submitting the report and in case of aggregated reporting.	Yes. if the financial entity affected by the incident is different from the entity submitting the report and in case of aggregated reporting.
1.6	LEI code of the financial entity affected	<p>Legal Entity Identifier (LEI) of the financial entity affected by the major ICT-related incident assigned in accordance with the International Organisation for Standardisation.</p> <p>In case of aggregated reporting:</p> <p>(a) a list of all LEI codes of the financial entities affected by the major ICT-related incident. separated by a semicolon.</p> <p>(b) the third-party provider submitting a major incident notification or report in an aggregated manner as referred to in Article 7 of this Regulation to list the LEI codes of all financial entities impacted by the incident. separated by a semicolon.</p> <p>The order of appearance of LEI codes and financial entities names shall be identical.</p>	Unique 20 alphanumeric character code. based on ISO 17442-1:2020	Yes. if the financial entity affected by the major ICT-related incident is different from the entity submitting the report and in case of aggregated reporting.	Yes. if the financial entity affected by the major ICT-related incident is different from the entity submitting the report and in case of aggregated reporting.	Yes. if the financial entity affected by the major ICT-related incident is different from the entity submitting the report and in case of aggregated reporting.
1.7	Primary contact person name	<p>Name and surname of the primary contact person of the financial entity.</p> <p>In case of aggregated reporting as referred to in Article 7 of this Regulation. the name of the primary contact person in the entity submitting the aggregated report.</p>	Alphanumeric	Yes	Yes	Yes

1.8	Primary contact person email	Email address of the primary contact person that can be used by the competent authority for follow-up communication. In case of aggregated reporting as referred to in Article 7 of this Regulation, the email of the primary contact person in the entity submitting the aggregated report.	Alphanumeric	Yes	Yes	Yes
1.9	Primary contact person telephone	Telephone number of the primary contact person that can be used by the competent authority for follow-up communication In case of aggregated reporting as referred to in Article 7 of this Regulation, the telephone number of the primary contact person in the entity submitting the aggregated report. Telephone number shall be reported with all international prefixes (e.g. +33XXXXXXXXX)	Alphanumeric	Yes	Yes	Yes
1.10	Second contact person name	Name and surname of the second contact person or the name of the responsible team of the financial entity or an entity submitting the report on behalf of the financial entity	Alphanumeric	Yes	Yes	Yes
1.11	Second contact person email	Email address of the second contact person or a functional email address of the team that can be used by the competent authority for follow-up communication.	Alphanumeric	Yes	Yes	Yes
1.12	Second contact person telephone	The telephone number of the second contact person, or of a team, that can be used by the competent authority for follow-up communication. Telephone number shall be reported with all international prefixes (e.g. +33XXXXXXXXX)	Alphanumeric	Yes	Yes	Yes
1.13	Name of the ultimate parent undertaking	Name of the ultimate parent undertaking of the group to which the affected financial entity belongs, where applicable.	Alphanumeric	Yes, if the FE belongs to a group.	Yes, if the FE belongs to a group.	Yes, if the FE belongs to a group.
1.14	LEI code of the ultimate parent undertaking	LEI of the ultimate parent undertaking of the group to which the affected financial entity belongs, where applicable. Assigned in accordance with the International Organisation for Standardisation.	Unique 20 alphanumeric character code, based on ISO 17442-1:2020.	Yes, if the FE belongs to a group.	Yes, if the FE belongs to a group.	Yes, if the FE belongs to a group.
1.15	Reporting currency	Currency used for the incident reporting	Choice populated by using ISO 4217 currency codes	Yes	Yes	Yes
Content of the initial notification (Initial notification tab)						
2.1	Incident reference code assigned by the financial entity	Unique reference code issued by the financial entity unequivocally identifying the major ICT-related incident. In case of aggregated reporting as referred to in Article 7 of this Regulation, the incident reference code assigned by the third-party provider.	Alphanumeric	Yes	Yes	Yes
2.2	Date and time of detection of the ICT-related incident	Date and time at which the financial entity has become aware of the ICT-related incident. For recurring incidents, the date and the time at which the last ICT-related incident was detected.	ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss)	Yes	Yes	Yes
2.3	Date and time of classification of the incident as major	Date and time when the ICT-related incident was classified as major according to the classification criteria established in Regulation (EU) 2024/1772.	ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss)	Yes	Yes	Yes

2.4	Description of the ICT-related incident	<p>Description of the most relevant aspects of the major ICT-related incident.</p> <p>Financial entities shall provide a high-level overview of the following information such as possible causes, immediate impacts, systems affected, and others. Financial entities, shall include, where known or reasonably expected, whether the incident impacts third-party providers or other financial entities, the type of provider or financial entity, their name, their respective identification codes and type of the identification code (e.g. LEI or EUID).</p> <p>In subsequent reports, the field content can evolve over time to reflect the ongoing understanding of the ICT-related incident and describe any other relevant information about the ICT-related incident not captured by the data fields, including the internal severity assessment by the financial entity (e.g. very low, low, medium, high, very high) and an indication of the level and name of most senior decision structures that has been involved in response to the ICT-related incident.</p>	Alphanumeric	Yes	Yes	Yes
2.5	Classification criteria that triggered the incident report	<p>Classification criteria under Delegated Regulation (EU) 2024/1772 that have triggered determination of the ICT-related incident as major and subsequent notification and reporting.</p> <p>In the case of aggregated reporting as referred to in Article 7 of this Regulation, the classification criteria that have triggered determination of the ICT-related incident as major for at least one or more financial entities.</p>	<p>Choice (multiple):</p> <ul style="list-style-type: none"> - Clients, financial counterparts and transactions affected - Reputational impact - Duration and service downtime - Geographical spread - Data losses - Critical services affected - Economic impact 	Yes	Yes	Yes
2.6	Materiality thresholds for the classification criterion 'Geographical spread'	<p>EEA Member States impacted by the ICT-related incident</p> <p>When assessing the impact of the major ICT-related incident in other Member States, financial entities shall take into account Articles 4 and 12 of Delegated Regulation 2024/1772.</p>	<p>Choice (multiple) populated by using ISO 3166 ALPHA-2 of the affected countries</p>	Yes, if 'Geographical spread' threshold is met.	Yes, if 'Geographical spread' threshold is met.	Yes, if 'Geographical spread' threshold is met.
2.7	Discovery of the major ICT-related incident	<p>Indication of how the major ICT-related incident has been discovered.</p>	<p>Choice:</p> <ul style="list-style-type: none"> - IT Security - Staff - Internal audit - External audit - Clients - Financial counterparts - Third-party provider - Attacker - Monitoring systems - Authority / agency / law enforcement body - Other 	Yes	Yes	Yes

2.8	Indication whether the incident originates from a third-party provider or another financial entity	<p>Indication whether the major ICT-related incident originates from a third-party provider or another financial entity.</p> <p>Financial entities shall indicate whether the major ICT-related incident originates from a third-party provider or another financial entity (including financial entities belonging to the same group as the reporting entity) and the name, identification code of the third-party provider or financial entity and type of the identification code (e.g. LEI or EUID).</p>	Alphanumeric	Yes, if the incident originates from a third-party provider or another financial entity	Yes, if the incident originates from a third-party provider or another financial entity	Yes, if the incident originates from a third-party provider or another financial entity
2.9	Activation of business continuity plan, if activated	Indication of whether there has been a formal activation of the business continuity response measures of the financial entity.	Boolean (Yes or No)	Yes	Yes	Yes
2.10	Other relevant information	<p>Any further information not covered in the template.</p> <p>Financial entities that have reclassified a major ICT-related incident as non-major shall describe the reasons why the ICT-related incident does not fulfil, and is not expected to fulfil, the criteria to be considered as a major ICT-related incident</p>	Alphanumeric	Yes, if there is other information not covered in the template or if the major ICT-related incident has been reclassified as non-major.	Yes, if there is other information not covered in the template or if the major ICT-related incident has been reclassified as non-major	Yes, if there is other information not covered in the template or if the major ICT-related incident has been reclassified as non-major
Content of the intermediate report (Intermediate report tab)						
3.1	Incident reference code provided by the competent authority	Unique reference code assigned by the competent authority at the time of receipt of the initial notification to unequivocally identify the major ICT-related incident.	Alphanumeric	No	Yes, if applicable	Yes, if applicable
3.2	Date and time of occurrence of the incident	<p>Date and time at which the major ICT-related incident has occurred, if different from the time the financial entity has become aware of the major ICT-related incident.</p> <p>For recurring major ICT-related incidents, the date and the time at which the last major ICT-related incident has occurred.</p>	ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss)	No	Yes	Yes
3.3	Date and time when services, activities or operations have been recovered	Information on the date and time of the recovery of the services, activities or operations affected by the major ICT-related incident.	ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss)	No	Yes, if data field 3.16, 'Service downtime' has been populated	Yes, if data field 3.16, 'Service downtime' has been populated

3.4	Number of clients affected	<p>Number of clients affected by the major ICT-related incident that use the service provided by the financial entity.</p> <p>When assessing the number of clients affected, financial entities shall take into account Articles 1(1) and 9(1), point (b), of Delegated Regulation 2024/1772 in their assessment. A financial entity that cannot determine the actual number of clients impacted shall use estimates based on available data from comparable reference periods.</p> <p>In the case of aggregated reporting as referred to in Article 7 of this Regulation, the total number of clients affected across all financial entities.</p>	Numerical integer	No	Yes	Yes
3.5	Percentage of clients affected	<p>Percentage of clients affected by the major ICT-related incident in relation to the total number of clients that make use of the affected service provided by the financial entity. In case of more than one service affected, the services shall be provided in an aggregated manner.</p> <p>Financial entities shall take into account Article 1(1) and Article 9(1), point (a), of Delegated Regulation 2024/1772 in their assessment.</p> <p>A financial entity that cannot determine the actual percentage of clients impacted shall use estimates based on available data from comparable reference periods.</p> <p>In the case of aggregated reporting as referred to in Article 7 of this Regulation, a financial entity shall divide the sum of all affected clients by the total number of clients of all impacted financial entities.</p>	Expressed as percentage - any value up to 5 numeric characters including up to 1 decimal place expressed as percentage (e.g. 2.4 instead of 2.4%). If the value has more than 1 digit after the decimal, reporting counterparties shall round half-up	No	Yes	Yes
3.6	Number of financial counterparts affected	<p>Number of financial counterparts affected by the major ICT-related incident that have concluded a contract with the financial entity.</p> <p>When assessing the number of financial counterparts affected, financial entities shall take into account Article 1(2) of Delegated Regulation 2024/1772 in their assessment. A financial entity that cannot determine the actual number of financial counterparts impacted shall use estimates based on available data from comparable reference periods.</p> <p>In the case of aggregated reporting as referred to in Article 7 of this Regulation, the total number of financial counterparts affected across all financial entities.</p>	Numerical integer	No	Yes	Yes
3.7	Percentage of financial counterparts affected	<p>Percentage of financial counterparts affected by the major ICT-related incident in relation to the total number of financial counterparts that have concluded a contract with the financial entity.</p> <p>When assessing the percentage of financial counterparts affected, financial entities shall take into account Articles 1(1) and 9(1), point (c) of Delegated Regulation 2024/1772 in their assessment. A financial entity that cannot determine the actual percentage of financial counterparts impacted shall use estimates based on available data from comparable reference periods.</p> <p>In the case of aggregated reporting as referred to in Article 7 of this Regulation, indicate the sum of all affected financial counterparts divided by the total number of financial counterparts of all impacted financial entities.</p>	Expressed as percentage - any value up to 5 numeric characters including up to 1 decimal place expressed as percentage (e.g. 2.4 instead of 2.4%). If the value has more than 1 digit after the decimal, reporting counterparties shall round half-up	No	Yes	Yes

3.8	Impact on relevant clients or financial counterparts	Any identified impact on relevant clients or financial counterpart as referred to in Article 1(3) and Article 9(1). point (f). of Delegated Regulation (EU) 2024/1772.	Boolean (Yes or No)	No	Yes. if 'Relevance of clients and financial counterparts' threshold is met	Yes. if 'Relevance of clients and financial counterparts' threshold is met
3.9	Number of affected transactions	<p>Number of transactions affected by the major ICT-related incident.</p> <p>When assessing the impact on transactions, financial entities shall take into account Article 1(4) of Delegated Regulation 2024/1772. including all affected domestic and cross-border transactions containing a monetary amount that have at least one part of the transaction carried out in the Union.</p> <p>A financial entity that cannot determine the actual number of transactions impacted shall use estimates based on available data from comparable reference periods.</p> <p>In the case of aggregated reporting as referred to in Article 7 of this Regulation, indicate the total number of transactions affected across all financial entities.</p>	Numerical integer	No	Yes. if any transaction has been affected by the incident	Yes. if any transaction has been affected by the incident
3.10	Percentage of affected transactions	<p>Percentage of affected transactions in relation to the daily average number of domestic and cross-border transactions carried out by the financial entity related to the affected service.</p> <p>Financial entities shall take into account Article 1(4) and Article 9(1). point (d). of Delegated Regulation 2024/1772.</p> <p>A financial entity that cannot determine the actual percentage of transactions impacted shall use estimates.</p> <p>In the case of aggregated reporting as referred to in Article 7 of this Regulation, a financial entity shall sum the number of all affected transactions and divide the sum by the total number of transactions of all impacted financial entities.</p>	Expressed as percentage - any value up to 5 numeric characters including up to 1 decimal place expressed as percentage (e.g. 2.4 instead of 2.4%). If the value has more than 1 digit after the decimal, reporting counterparties shall round half-up	No	Yes. if any transaction has been affected by the incident	Yes. if any transaction has been affected by the incident
3.11	Value of affected transactions	<p>Total value of the transactions affected by the major ICT-related incident shall be assessed in accordance with Article 1(4) and Article 9(1). point (e) of Delegated Regulation 2024/1772.</p> <p>A financial entity that cannot determine the actual value of transactions impacted shall use estimates based on available data from comparable reference periods.</p> <p>A financial entity shall report the monetary amount as a positive value.</p> <p>In the case of aggregated reporting as referred to in Article 7 of this Regulation, the total value of the transactions affected across all financial entities.</p>	<p>Monetary</p> <p>Financial entities shall report the data point in units using a minimum precision equivalent to thousands of units (e.g. 2.5 instead of EUR 2500).</p>	No	Yes. if any transactions have been affected by the incident	Yes. if any transaction has been affected by the incident

3.12	Information on whether the numbers are actual or estimates, or whether there has not been any impact	Information on whether the values reported in the data fields 3.4. to 3.11. are actual or estimates, or whether there has not been any impact.	Choice (multiple): <ul style="list-style-type: none"> - Actual figures for clients affected - Actual figures for financial counterparts affected - Actual figures for transactions affected - Estimates for clients affected - Estimates for financial counterparts affected - Estimates for transactions affected - No impact on clients - No impact on financial counterparts - No impact on transactions 	No	Yes	Yes
3.13	Reputational impact	<p>Information about the reputational impact resulting from the major ICT-related incident as referred to in Articles 2 and 10 of Delegated Regulation 2024/1772.</p> <p>In the case of aggregated reporting as referred to in Article 7 of this Regulation, the reputational impact categories that apply to at least one financial entity.</p>	Choice (multiple): <ul style="list-style-type: none"> - the major ICT-related incident has been reflected in the media; - the major ICT-related incident has resulted in repetitive complaints from different clients or financial counterparts on client-facing services or critical business relationships - the financial entity will not be able to or is likely not to be able to meet regulatory requirements as a result of the major ICT-related incident; - the financial entity will or is likely to lose clients or financial counterparts with a material impact on its business as a result of the major ICT-related incident. 	No	Yes, if 'Reputational impact' criterion met	Yes, if 'Reputational impact' criterion met

3.14	Contextual information about the reputational impact	<p>Information describing how the major ICT-related incident has affected or could affect the reputation of the financial entity, including infringements of law, regulatory requirements not met, number of client complaints, and other.</p> <p>The contextual information shall include the type of media (e.g. traditional and digital media, blogs, streaming platforms) and media coverage, including reach of the media (local, national, international). Media coverage in this context shall not mean a few negative comments by followers or users of social networks.</p> <p>The financial entity shall also indicate whether the media coverage highlighted significant risks for its clients in relation to the major ICT-related incident, including the risk of the financial entity's insolvency or the risk of losing funds.</p> <p>Financial entities shall also indicate whether they have provided information to the media that served to reliably inform the public about the major ICT-related incident and its consequences.</p> <p>Financial entities may also indicate whether there was false information in the media in relation to the ICT-related incident, including information based on deliberate misinformation spread by threat actors, or information relating to or illustrating defacement of the financial entity's website.</p>	Alphanumeric	No	Yes, if 'Reputational impact' criterion met.	Yes, if 'Reputational impact' criterion met.
3.15	Duration of the major ICT-related incident	<p>Financial entities shall measure the duration of the major ICT-related incident from the moment the major ICT-related incident occurred until the moment the incident was resolved.</p> <p>Financial entities that are unable to determine the moment when the major ICT-related incident has occurred shall measure the duration of the major ICT-related incident from the earlier between the moment the financial entity detected the incident and the moment when the financial entity recorded the incident in network or system logs or other data sources. Financial entities that do not yet know the moment when the major ICT-related incident will be resolved shall apply estimates. The value shall be expressed in days, hours, and minutes.</p> <p>In the case of aggregated reporting as referred to in Article 7 of this Regulation, financial entities shall measure the longest duration of the major ICT-related incident in case of differences between financial entities.</p>	DD:HH:MM	No	Yes	Yes

3.16	Service downtime	<p>Service downtime measured from the moment the service is fully or partially unavailable to clients, financial counterparts or other internal or external users, until the moment when regular activities or operations have been restored to the level of service that was provided prior to the major ICT-related incident.</p> <p>Where the service downtime causes a delay in the provision of service after regular activities or operations have been restored, financial entities shall measure the downtime from the start of the major ICT-related incident until the moment when that delayed service is provided. Financial entities that are unable to determine the moment when the service downtime has started, shall measure the service downtime from the earlier between the moment the incident was detected and the moment when it has been recorded.</p> <p>In the case of aggregated reporting as referred to in Article 7 of this Regulation, financial entities shall measure the longest duration of the service downtime in case of differences between financial entities.</p>	DD:HH:MM	No	Yes, if the incident has caused a service downtime	Yes, if the incident has caused a service downtime
3.17	Information whether the numbers for duration and service downtime are actual or estimates.	Information on whether the values reported in data fields 3.15 and 3.16, are actual or estimates.	Choice: - Actual figures - Estimates - Actual figures and estimates - No information available	No	Yes, if 'Duration and service downtime' criterion met	Yes, if 'Duration and service downtime' criterion met
3.18	Types of impact in the Member States	<p>Type of impact in the respective EEA Member States.</p> <p>Indication of whether the major ICT-related incident has had an impact in other EEA Member States (other than the Member State of the competent authority to which the incident is directly reported), in accordance with Article 4 of Delegated Regulation (EU) 2024/1772, and in particular with regard to the significance of the impact in relation to:</p> <p>a) clients and financial counterparts affected in other Member States; or b) branches or other financial entities within the group carrying out activities in other Member States; or c) financial market infrastructures or third-party providers, which may affect financial entities in other Member States to which they provide services.</p>	Choice (multiple): - clients - financial counterparts - branch of the financial entity - financial entities within the group carrying out activities in the respective Member State - financial market infrastructure - third-party providers that may be common to other financial entities	No	Yes, if 'Geographical spread' threshold is met	Yes, if 'Geographical spread' threshold is met
3.19	Description of how the major ICT-related incident has an impact in other Member States	<p>Description of the impact and severity of the major ICT-related incident in each affected Member State, including an assessment of the impact and severity on:</p> <p>(a) clients; (b) financial counterparts; (c) branches of the financial entity; (d) other financial entities within the group carrying out activities in the respective Member State; (e) financial market infrastructures; (f) third-party providers that may be common to other financial entities as applicable in other member state(s).</p>	Alphanumeric	No	Yes, if 'Geographical spread' threshold is met	Yes, if 'Geographical spread' threshold is met

3.20	Materiality thresholds for the classification criterion 'Data losses'	<p>Type of data losses that the major ICT-related incident entails in relation to availability, authenticity, integrity, and confidentiality of data.</p> <p>Financial entities shall take into account Articles 5 and 13 of Delegated Regulation 2024/1772 in their assessment.</p> <p>In case of aggregated reporting as referred to in Article 7 of this Regulation, the data losses affecting at least one financial entity.</p>	<p>Choice (multiple):</p> <ul style="list-style-type: none"> - availability - authenticity - integrity - confidentiality 	No	Yes, if 'Data losses' criterion is met	Yes, if 'Data losses' criterion is met
3.21	Description of the data losses	<p>Description of the impact of the major ICT-related incident on availability, authenticity, integrity, and confidentiality of critical data in accordance with Articles 5 and 13 of Delegated Regulation 2024/1772.</p> <p>Information about the impact on the implementation of the business objectives of the financial entity or on meeting regulatory requirements.</p> <p>As part of the information provided, financial entities shall indicate whether the data affected are client data, other entities' data (e.g. financial counterparts), or data of the financial entity itself.</p> <p>The financial entity may also indicate the type of data involved in the incident - in particular, whether the data is confidential and what type of confidentiality was involved (e.g. commercial/business confidentiality, personal data, professional secrecy, banking secrecy, insurance secrecy, payment services secrecy, etc.).</p> <p>The information may also include possible risks associated with the data losses, such as whether the data affected by the incident can be used to identify individuals and could be used by the threat actor to obtain credit or loans without their consent, to conduct spear phishing attacks, to disclose information publicly.</p> <p>In the case of aggregated reporting as referred to in Article 7 of this Regulation, a general description of the impact of the incident on the affected financial entities. Where there are differences of the impact, the description of the impact shall clearly indicate the specific impact on the different financial entities.</p>	Alphanumeric	No	Yes, if 'Data losses' criterion is met	Yes, if 'Data losses' criterion is met
3.22	Classification criterion 'Critical services affected'	<p>Information related to the criterion 'Critical services affected'.</p> <p>Financial entities shall take into account Articles 6 of Delegated Regulation (EU) 2024/1772 in their assessment, including information about:</p> <ul style="list-style-type: none"> - the affected services or activities that require authorisation, registration or that are supervised by competent authorities; or - the ICT services or network and information systems that support critical or important functions of the financial entity; and - the nature of the malicious and unauthorised access to the network and information systems of the financial entity. <p>In the case of aggregated reporting as referred to in Article 7 of this Regulation, the impact on critical services that apply to at least one financial entity.</p>	Alphanumeric	No	Yes	Yes

3.23	Type of the major ICT-related incident	Classification of incidents by type.	Choice (multiple): - Cybersecurity-related - Process failure - System failure - External event - Payment-related - Other (please specify)	No	Yes	Yes
3.24	Other types of incidents	Other types of ICT-related incidents: financial entities that have selected 'other' type of incidents in the data field 3.23. shall specify the type of ICT-related incident.	Alphanumeric	No	Yes. if 'other' type of incidents is selected in data field 3.23	Yes. if 'other' type of incidents is selected in data field 3.23
3.25	Threats and techniques used by the threat actor	Indicate the threats and techniques used by the threat actor. including: (a) social engineering. including phishing; (b) (D)DoS; (c) identity theft; (d) data encryption for impact. including ransomware; (e) resource hijacking; (f) data exfiltration and manipulation. excluding identity theft; (g) data destruction; (h) defacement; (i) supply-chain attack; (j) other (please specify).	Choice (multiple): - Social engineering (including phishing) - (D)DoS - Identity theft - Data encryption for impact. including ransomware - Resource hijacking - Data exfiltration and manipulation. including identity theft - Data destruction - Defacement - Supply-chain attack - Other (please specify)	No	Yes. if the type of the ICT-related incident is 'cybersecurity-related' in field 3.23	Yes. if the type of the ICT-related incident is 'cybersecurity-related' in field 3.23
3.26	Other types of techniques	Other types of techniques Financial entities that have selected 'other' type of techniques in data field 3.25 shall specify the type of technique.	Alphanumeric	No	Yes. if other' type of techniques is selected in data field 3.25	Yes. if other' type of techniques is selected in data field 3.25

3.27	<p>Information about affected functional areas and business processes</p>	<p>Indication of the functional areas and business processes that are affected by the incident. including products and services.</p> <p>The functional areas shall include but are not limited to:</p> <p>(a) marketing and business development; (b) customer service; (c) product management; (d) regulatory compliance; (e) risk management; (f) finance and accounting; (g) HR and general services; (h) information Technology;</p> <p>The business processes shall include but are not limited to:</p> <ul style="list-style-type: none"> • account information; • actuarial services; • acquiring of payment transactions; • authentication/authorization; • authority • client on-boarding; • benefit administration; • benefit payment management; • buying and selling packaged insurances policies between insurances; • card payments; • cash management; • cash placement or withdrawals; • insurance claim management; • claim process insurance; • clearing; • corporate loans conglomerates; • collective insurances; • credit transfers; • custody and asset safekeeping; • customer onboarding; • data ingestion; • data processing; • direct debits; • export insurances; • finalizing trades/deals; • financial instruments placing; • fund accounting; • FX money; • investment advice; • investment management; • issuing of payment instruments; 	Alphanumeric	No	Yes	Yes
------	---	---	--------------	----	-----	-----

		<ul style="list-style-type: none"> • lending management; • life insurance payments process; • money remittance; • net asset calculation; • order; • payment initiation; • insurance underwriting; • portfolio management; • premium collection; • reception/transmission/execution; • reinsurance; • settlement; • transaction monitoring; <p>In the case of aggregated reporting as referred to in Article 7 of this Regulation, the affected functional areas and business processes in at least one financial entity.</p>				
3.28	Affected infrastructure components supporting business processes	Information on whether infrastructure components (servers, operating systems, software, application servers, middleware, network components, others) supporting business processes have been affected by the major ICT-related incident.	Choice: - Yes - No - Information not available	No	Yes	Yes
3.29	Information about affected infrastructure components supporting business processes	<p>Description on the impact of the major ICT-related incident on infrastructure components supporting business processes including hardware and software.</p> <p>Hardware includes servers, computers, data centres, switches, routers, hubs. Software includes operating systems, applications, databases, security tools, network components, others please specify. The descriptions shall describe or name affected infrastructure components or systems, and, where available:</p> <p>(a) version information; (b) internal infrastructure/partially outsourced/fully outsourced – third-party provider name; (c) whether the infrastructure is used or shared across multiple business functions; (d) relevant resilience/continuity/recovery/ substitutability arrangements in place.</p>	Alphanumeric	No	Yes, if the incident has affected infrastructure components supporting business processes	Yes, if the incident has affected infrastructure components supporting business processes
3.30	Impact on the financial interest of clients	Information on whether the major ICT-related incident has impacted the financial interest of clients.	Choice: - Yes - No - Information not available	No	Yes	Yes
3.31	Reporting to other authorities	<p>Specification of which authorities were informed about the major ICT-related incident.</p> <p>Taking into account the differences resulting from the national legislation of the Member States, the concept of law enforcement authorities shall be understood by financial entities broadly to include public authorities empowered to prosecute cybercrime, including police, law enforcement agencies, and public prosecutors.</p>	Choice (multiple): - Police/Law Enforcement - CSIRT - Data Protection Authority - National Cybersecurity Agency - None - Other (please specify)	No	Yes	Yes

3.32	Specification of 'other' authorities	<p>Specification of 'other' types of authorities informed about the major ICT-related incident.</p> <p>If selected in Data field 3.31. 'Other', the description shall include more detailed information about the authority to which the financial entity has submitted information about the major ICT-related incident.</p>	Alphanumeric	No	Yes, if 'other' type of authorities have been informed by the financial entity about the major ICT-related incident.	Yes, if 'other' type of authorities have been informed by the financial entity about the major ICT-related incident.
3.33	Temporary actions/measures taken or planned to be taken to recover from the incident	<p>Indication of whether financial entity has implemented (or plan to implement) any temporary actions that have been taken (or planned to be taken) to recover from the major ICT-related incident.</p>	Boolean (Yes or No)	No	Yes	Yes
3.34	Description of any temporary actions and measures taken or planned to be taken to recover from the incident	<p>The information shall describe the immediate actions taken, including the isolation of the incident at the network level, workaround procedures activated, USB ports blocked, Disaster Recovery site activated, any other additional security controls temporarily put in place.</p> <p>Financial entities shall indicate the date and the time of the implementation of the temporary actions and the expected date of return to the primary site. For any temporary actions that have not been implemented but are still planned, indication of the date by when their implementation is expected.</p> <p>If no temporary actions/measures have been taken, please indicate the reason.</p>	Alphanumeric	No	Yes, if temporary actions/measures have been taken or are planned to be taken (data field 3.33)	Yes, if temporary actions/measures have been taken or are planned to be taken (data field 3.33)

3.35	Indicators of compromise	<p>Information related to the major ICT-related incident that may help identify malicious activity within a network or information system (Indicators of Compromise, or IoC), where applicable.</p> <p>The field applies only to those financial entities that fall within the scope of Directive (EU) 2022/2555 of the European Parliament and of the Council and those financial entities identified as essential or important entities pursuant to national rules transposing Article 3 of Directive (EU) 2022/2555, where relevant.</p> <p>The IoC provided by the financial entity shall include the following categories of data:</p> <ul style="list-style-type: none"> (a) IP addresses; (b) URL addresses; (c) domains; (d) file hashes; (e) malware data (malware name, file names and their locations, specific registry keys associated with malware activity); (f) network activity data (ports, protocols, addresses, referrers, user agents, headers, specific logs or distinctive patterns in network traffic); (g) e-mail message data (sender, recipient, subject, header, content); (h) DNS requests and registry configurations; (i) user account activities (logins, privileged user account activity, privilege escalation); (j) database traffic (read/write), requests to the same file. <p>In practice, this type of information may include data relating to, inter alia, indicators describing patterns in network traffic corresponding to known attacks/botnet communications, IP addresses of machines infected with malware (bots), data relating to “command and control” servers used by malware (usually domains or IP addresses), and URLs relating to phishing sites or websites observed hosting malware or exploit kits.</p>	Alphanumeric	No	Yes, if cybersecurity-related is selected as a type of incident in data field 3.23	Yes, if cybersecurity-related is selected as a type of incident in data field 3.23
Content of the final report (Final report tab)						
4.1	High-level classification of root causes of the incident	<p>High-level classification of root cause of the major ICT-related incident under the incident types, including the following high-level categories:</p> <ul style="list-style-type: none"> (a) malicious actions; (b) process failure; (c) system failure/malfunction; (d) human error; (e) external event. 	<p>Choice (multiple):</p> <ul style="list-style-type: none"> - Malicious actions - Process failure - System failure / malfunction - Human error - External event 	No	No	Yes

4.2	<p>Detailed classification of root causes of the incident</p>	<p>Detailed classification of root causes of the major ICT-related incident under the incident types, including the following detailed categories linked to the high-level categories that are reported in data field 4.1:</p> <p>1. Malicious actions (if selected, choose one or more the following): (a) deliberate internal actions; (b) deliberate physical damage/manipulation/theft; (c) fraudulent actions.</p> <p>2. Process failure (if selected, choose one or more the following): (a) insufficient monitoring or failure of monitoring and control; (b) insufficient/unclear roles and responsibilities; (c) ICT risk management process failure; (d) insufficient or failure of ICT operations and ICT security operations; (e) insufficient or failure of ICT project management; (f) inadequate internal policies, procedures and documentation; (g) inadequate ICT systems acquisition, development, or maintenance; (h) other (please specify).</p> <p>3. System failure/malfunction (if selected, choose one or more the following): (a) hardware capacity and performance: major ICT-related incidents caused by hardware resources which prove inadequate in terms of capacity or performance to fulfil the applicable legislative requirements; (b) hardware maintenance: major ICT-related incidents resulting from inadequate or insufficient maintenance of hardware components, other than "Hardware obsolescence/ageing" ; (c) hardware obsolescence/ageing: this root cause type involves major ICT-related incidents resulting from outdated or aging hardware components; (d) software compatibility/configuration: major ICT-related incidents caused by software components that are incompatible with other software or system configurations, including major ICT-related incidents resulting from software conflicts, incorrect settings, or misconfigured parameters that impact the overall system functionality; (e) software performance: major ICT-related incidents resulting from software components that exhibit poor performance or inefficiencies, for reasons other than those specified under "Software compatibility/configuration", including major ICT-related incidents caused by slow response times, excessive resource consumption, or inefficient query execution impacting the performance of the software or system; (f) network configuration: major ICT-related incidents resulting from incorrect or misconfigured network settings or infrastructure, including major ICT-related incidents caused by network configuration errors, routing issues, firewall misconfigurations, or other network-related problems affecting connectivity or communication; (g) physical damage: major ICT-related incidents caused by physical damage to ICT infrastructure which lead to system failures; (h) other (please specify).</p> <p>4. Human error (if selected, choose one or more the following): (a) omission (unintentional);</p>	<p>Choice (multiple):</p> <ul style="list-style-type: none"> - malicious actions: deliberate internal actions - malicious actions: deliberate physical damage/manipulation/theft - malicious actions: fraudulent actions - process failure: insufficient monitoring or failure of monitoring and control - process failure: insufficient/unclear roles and responsibilities - process failure: ICT risk management process failure - process failure: insufficient or failure of ICT operations and ICT security operations; - process failure: insufficient or failure of ICT project management - process failure: inadequacy of internal policies, procedures and documentation - Process failure: inadequate ICT systems acquisition, development, and maintenance - process failure: other (please specify) - system failure: hardware capacity and performance - system failure: hardware maintenance - system failure: hardware obsolescence/ageing - system failure: software compatibility/configuration - system failure: software performance - system failure: network configuration - system failure: physical damage - system failure: other (please specify) - human error: omission - human error: mistake 	No	No	Yes
-----	--	---	---	----	----	-----

		<p>(b) mistake;</p> <p>(c) skills & knowledge: major ICT-related incidents resulting from a lack of expertise or proficiency in handling ICT systems or processes that may be caused by inadequate training, insufficient knowledge, or gaps in skills required to perform specific tasks or address technical challenges;</p> <p>(d) inadequate human resources: major ICT-related incidents caused by a lack of necessary resources, including hardware, software, infrastructure, or personnel, and including situations where insufficient resources lead to operational inefficiencies, system failures, or an inability to meet business demands;</p> <p>(e) miscommunication;</p> <p>(f) other (please specify).</p> <p>5. External event (if selected, choose one or more the following)</p> <p>(a) natural disasters/force majeure;</p> <p>(b) third-party failures;</p> <p>(c) other (please specify).</p> <p>Financial entities shall consider that for recurring major ICT-related incidents, the specific apparent root cause of the incident is taken into account and not the broad categories included in this field.</p>	<p>- human error: skills & knowledge</p> <p>- human error: inadequate human resources</p> <p>- human error: miscommunication</p> <p>- human error: other (please specify)</p> <p>- external event: natural disasters/force majeure</p> <p>- external event: third-party failures</p> <p>- external event: other (please specify)</p>			
--	--	---	--	--	--	--

4.3	Additional classification of root causes of the incident	<p>Additional classification of root causes of the major ICT-related incident under the incident type, including the following additional classification categories linked to the detailed categories that are to be reported in data field 4.2.</p> <p>The field is mandatory for the final report if specific categories that require further granularity are reported in data field 4.2.</p> <p>2(a) Insufficient or failure of monitoring and control: (a) monitoring of policy adherence; (b) monitoring of third-party service providers; (c) monitoring and verification of remediation of vulnerabilities; (d) identity and access management; (e) encryption and cryptography; (f) logging.</p> <p>2(c) ICT risk management process failure: (a) failure in specifying accurate risk tolerance levels; (b) insufficient vulnerability and threat assessments; (c) inadequate risk treatment measures; (d) poor management of residual ICT risks.</p> <p>2(d) Insufficient or failure of ICT operations and ICT security operations: (a) vulnerability and patch management; (b) change management; (c) capacity and performance management; (d) ICT asset management and information classification; (e) backup and restore; (f) error handling.</p> <p>2(g) Inadequate ICT Systems acquisition, development, and maintenance: (a) inadequate ICT Systems acquisition, development, and maintenance; (b) insufficient software testing or failure of software testing.</p>	<p>Choice (multiple):</p> <ul style="list-style-type: none"> - monitoring of policy adherence - monitoring of third-party service providers - monitoring and verification of remediation of vulnerabilities - identity and access management - encryption and cryptography - logging - failure in specifying accurate risk tolerance levels - insufficient vulnerability and threat assessments - inadequate risk treatment measures - poor management of residual ICT risks - vulnerability and patch management - change management - capacity and performance management - ICT asset management and information classification - backup and restore - error handling - inadequate ICT systems acquisition, development, and maintenance - insufficient or failure of software testing 	No	No	Yes
4.4	Other types of root cause types	Financial entities that have selected 'other' type of root cause in data field 4.2, shall specify other types of root cause types	Alphanumeric	No	No	Yes, if 'other' type of root causes is selected in data field 4.2.
4.5	Information about the root causes of the incident	<p>Description of the sequence of events that led to the major ICT-related incident and description of how the major ICT-related incident has a similar apparent root cause if that incident is classified as a recurring incident, including a concise description of all underlying reasons and primary factors that contributed to the occurrence of the major ICT-related incident.</p> <p>Where there were malicious actions, description of the modus operandi of the malicious action, including the tactics, techniques and procedures used, as well as the entry vector of the major ICT-related incident, including a description of the investigations and analysis that led to the identification of the root causes, if applicable.</p>	Alphanumeric	No	No	Yes

4.6	Incident resolution	<p>Additional information regarding the actions/measures taken/planned to permanently resolve the major ICT-related incident and to prevent that incident from happening again.</p> <p>Lessons learnt from the major ICT-related incident.</p> <p>The description shall contain the following points:</p> <p>1. Resolution actions description (a) actions taken to permanently resolve the major ICT-related incident (excluding any temporary actions); (b) for each action taken, indicate the potential involvement of a third-party provider and of the financial entity; (c) indicate whether procedures have been adapted following the major ICT-related incident; (d) indicate any additional controls that were put in place or that are planned with related implementation timeline.</p> <p>Potential issues identified regarding the robustness of the IT systems impacted /or in terms of the procedures or controls in place, if applicable.</p> <p>Financial entities shall clearly indicate how the envisaged remediation actions will address the identified root causes and when the major ICT-related incident is expected to be resolved permanently.</p> <p>2. Lessons learnt</p> <p>Financial entities shall describe findings from the post-incident review.</p>	Alphanumeric	No	No	Yes
4.7	Date and time when the incident root cause was addressed	Date and time when the incident root cause was addressed.	ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss)	No	No	Yes
4.8	Date and time when the incident was resolved	Date and time when the incident was resolved.	ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss)	No	No	Yes
4.9	Information if the permanent resolution date of the incidents differs from the initially planned implementation date	Descriptions of the reason why the permanent resolution date of the major ICT-related incidents is different from the initially planned implementation date, where applicable.	Alphanumeric	No	No	Yes

4.10	Assessment of risk to critical functions for resolution purposes	<p>Assessment of whether the major ICT-related incident poses a risk to critical functions within the meaning of Article 2(1), point (35), of Directive 2014/59/EU of the European Parliament and of the Council .</p> <p>Entities as referred to in Article 1(1) of Directive 2014/59/EU shall indicate whether the incident poses a risk to the critical functions within the meaning of Article 2(1), point (35), of Directive 2014/59/EU, and as reported in Template Z07.01 of Commission Implementing Regulation (EU) 2018/1624 and mapped to the specific entity in Template Z07.02.</p>	Alphanumeric	No	No	Yes, if the incident poses a risk to critical functions of financial entities under Article 2(1), point 35, of Directive 2014/59/EU
4.11	Information relevant for resolution authorities	<p>Description of whether and, if so, how the major ICT-related incident has affected the resolvability of the entity or the group.</p> <p>Entities as referred to in Article 1(1) of Directive 2014/59/EU shall provide information on whether and, if so, how the major ICT-related incident has affected the resolvability of the entity or the group.</p> <p>Those entities shall also indicate whether the major ICT-related incident affects the solvency or liquidity of the financial entity and the potential quantification of the impact.</p> <p>Those entities shall also provide information on the impact on operational continuity, impact on resolvability of the entity, any additional impact on the costs and losses from the major ICT-related incident, including on the financial entity's capital position, and whether the contractual arrangements on the use of ICT services are still robust and fully enforceable in the event of resolution of the entity.</p>	Alphanumeric	No	No	Yes, if the incident has affected the resolvability of the entity or the group.
4.12	Materiality threshold for the classification criterion 'Economic impact'	Detailed information about thresholds eventually reached by the major ICT-related incident in relation to the criterion 'Economic impact' referred to in Articles 7 and 14 of the Delegated Regulation 2024/1772.	Alphanumeric	No	No	Yes

4.13	Amount of gross direct and indirect costs and losses	<p>Total amount of gross direct and indirect costs and losses incurred by the financial entity stemming from the major ICT-related incident, including:</p> <p>(a) the amount of expropriated funds or financial assets for which the financial entity is liable;</p> <p>(b) the amount of replacement or relocation costs of software, hardware or infrastructure;</p> <p>(c) the amount of staff costs, including costs associated to replacing or relocating staff, hiring extra staff, remuneration of overtime and recovering lost or impaired skills of staff;</p> <p>(d) the amount of fees due to non-compliance with contractual obligations;</p> <p>(e) the amount of customer redress and compensation costs;</p> <p>(f) the amount of losses due to forgone revenues;</p> <p>(g) the amount of costs associated with internal and external communication;</p> <p>(h) the amount of advisory costs, including costs associated with legal counselling, forensic and remediation services;</p> <p>(i) the amount other costs and losses, including:</p> <p>(i) direct charges, including impairments and settlement charges, to the profit and loss account and write-downs due to the major ICT-related incident;</p> <p>(ii) provisions or reserves accounted for in the profit and loss account against probable losses related to the major ICT-related incident;</p> <p>(iii) pending losses, in the form of losses stemming from the major ICT-related incident, which are temporarily booked in transitory or suspense accounts and are not yet reflected in the profit and loss which are planned to be included within a time period commensurate to the size and age of the pending item;</p> <p>(iv) material uncollected revenues, related to contractual obligations with third parties, including the decision to compensate a client following the major ICT-related incident, rather than by a reimbursement or direct payment, through a revenue adjustment waiving or reducing contractual fees for a specific future period of time;</p> <p>(v) timing losses, where they span more than one financial accounting year and give rise to legal risk.</p> <p>Financial entities shall take into account in their assessment Article 7(1) and (2) of Delegated Regulation 2024/1772. Financial entities shall not include in this figure financial recoveries of any type.</p> <p>Financial entities shall report the monetary amount as a positive value.</p> <p>In the case of aggregated reporting as referred to in Article 7 of this Regulation, financial entities shall take into account the total amount of costs and losses across all financial entities.</p> <p>Financial entities shall report the data point in units using a minimum precision equivalent to thousands of units.</p>	Monetary	No	No	Yes
------	--	---	----------	----	----	-----

4.14	Amount of financial recoveries	<p>Total amount of financial recoveries.</p> <p>Financial recoveries shall relate to the original loss caused by the incident, independently from the time when the financial recoveries in the form of funds or inflows of economic benefits are received.</p> <p>Financial entities shall report the monetary amount as a positive value.</p> <p>In the case of aggregated reporting as referred to in Article 7 of this Regulation, financial entities shall take into account the total amount of financial recoveries across all financial entities.</p>	<p>Monetary</p> <p>The data point shall be reported in units using a minimum precision equivalent to thousands of units</p>	No	No	Yes
4.15	Information on whether the non-major incidents have been recurring	<p>Information on whether more than one non-major ICT-related incident have been recurring and are together considered to be a major incident within the meaning of Article 8(2) of Delegated Regulation 2024/1772.</p> <p>Financial entities shall indicate whether the non-major ICT-related incidents have been recurring and are together considered as one major ICT-related incident.</p> <p>Financial entities shall also indicate the number of occurrences of these non-major ICT-related incidents.</p>	Alphanumeric	No	No	Yes, if the major incident comprises more than one non-major recurring incidents.
4.16	Date and time of occurrence of recurring incidents	<p>Where financial entities report recurring ICT-related incidents, date and time at which the first ICT-related incident has occurred.</p>	ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss)	No	No	Yes, for recurring incidents

Annexe 2 : liste des champs à remplir dans la survey DORA_CYBERTHREAT



Source : DORA significant
cyber threats Template

En attendant la publication de l'ITS concerné au Journal Officiel de l'UE, la présente liste n'existe qu'en anglais.

Column Code	Column Name	Description	Field Type	Mandatory field
1	Name of the entity submitting the notification	Full legal name of the entity submitting the notification.	Alphanumeric	Yes
2a	Identification code of the entity submitting the notification (LEI)	Identification code of the entity submitting the notification. Where financial entities submit the notification/report, the identification code shall be a Legal Entity Identifier (LEI), which is a unique 20 alphanumeric character code, based on ISO 17442-1:2020.	Alphanumeric	Yes, if field 2b is empty
2b	Identification code of the entity submitting the notification (EU ID)	Identification code of the entity submitting the notification. Where a third-party provider submits a report for a financial entity, it may use an identification code as specified in the implementing technical standards adopted pursuant to Article 28(9) of Regulation (EU) 2022/2554.	Alphanumeric	Yes, if field 2a is empty
3	Type of financial entity submitting the report	Type of the entity referred to in Article 2(1), points (a) to (t) of Regulation (EU) 2022/2554 submitting the report.	Choice (multiselect): - investment firm; - trading venue; - manager of alternative investment fund; - management company; - insurance intermediary, reinsurance intermediary and ancillary insurance intermediary; - institution for occupational retirement provision; - crowdfunding service provider	Yes, if the report is not provided by the affected financial entity directly.
4	Name of the financial entity	Full legal name of the financial entity notifying the significant cyber threat.	Alphanumeric	Yes, if the financial entity is different from the entity submitting the notification.
5	LEI code of the financial entity	Legal Entity Identifier (LEI) of the financial entity notifying the significant cyber threat, assigned in accordance with the International Organisation for Standardisation.	Unique alphanumeric 20 character code, based on ISO 17442-1:2020	Yes, if the financial entity notifying the significant

				cyber threat is different from the entity submitting the report
6	Primary contact person name	Name and surname of the primary contact person of the financial entity.	Alphanumeric	Yes
7	Primary contact person email	Email address of the primary contact person that can be used by the competent authority for follow-up communication.	Alphanumeric	Yes
8	Primary contact person telephone	The telephone number of the primary contact person that can be used by the competent authority for follow-up communication. The telephone number shall be reported with all international prefixes (e.g. +33XXXXXXXXXX)	Alphanumeric	Yes
9	Second contact person name	Name and surname of the second contact person of the financial entity or an entity submitting the notification on behalf of the financial entity, where available.	Alphanumeric	Yes, if name and surname of the second contact person of the financial entity or an entity submitting the notification for the financial entity is available.
10	Second contact person email	Email address of the second contact person or a functional email address of the team that can be used by the competent authority for follow-up communication, where available.	Alphanumeric	Yes, if email address of the second contact person or a functional email address of the team that can be used by the competent authority for follow-up communication is available.
11	Second contact person telephone	The telephone number of the second contact person that can be used by the competent authority for follow-up communication, where available. The telephone number shall be reported with all international prefixes (e.g. +33XXXXXXXXXX).	Alphanumeric	Yes, if the telephone number of the second contact person that can be used by the competent authority for follow-up communication is available.
12	Date and time of detection of the cyber threat	Date and time at which the financial entity has become aware of the significant cyber threat.	ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss)	Yes
13	Description of the significant cyber threat	Description of the most relevant aspects of the significant cyber threat. Financial entities shall provide: (a) a high-level overview of the most relevant aspects of the significant cyber threat; (b) the related risks arising from it, including potential vulnerabilities of the systems of the financial entity that can be exploited; (c) information about the probability of materialisation of the significant cyber threat; and (d) information about the source of information about the cyber threat.	Alphanumeric	Yes
14	Information about potential impact	Information about the potential impact of the cyber threat on the financial entity, its clients or financial counterparts if the cyber threat has materialised	Alphanumeric	Yes

15	Potential incident classification criteria	The classification criteria that could have triggered a major incident report if the cyber threat had materialised.	Choice (multiple): - clients, financial counterparts and transactions affected; - reputational impact; - duration and service downtime; - geographical spread; - data losses; - critical services affected; - economic impact.	Yes
16	Status of the cyber threat	Information about the status of the cyber threat for the financial entity and whether there have been any changes in the threat activity. Where the cyber threat has stopped communicating with the financial entity's information systems, the status can be marked as inactive. If the financial entity has information that the threat remains active against other parties or the financial system as a whole, the status shall be marked as active.	Choice: - active - inactive	Yes
17	Actions taken to prevent materialisation	High-level information about the actions taken by the financial entity to prevent the materialisation of the significant cyber threats, if applicable	Alphanumeric	Yes
18	Notification to other stakeholders	Information about notification of the cyber threat to other financial entities or authorities.	Alphanumeric	Yes, if other financial entities or authorities have been informed about the cyber threat).
19	Indicators of compromise	Information related to the significant threat that may help identify malicious activity within a network or information system (Indicators of Compromise, or IoC), where applicable. The IoC provided by the financial entity may include, but is not to be limited to, the following categories of data: (a) IP addresses; (b) URL addresses; (c) domains; (d) file hashes; (e) malware data (malware name, file names and their locations, specific registry keys associated with malware activity); (f) network activity data (ports, protocols, addresses, referrers, user agents, headers, specific logs or distinctive patterns in network traffic); (g) e-mail message data (sender, recipient, subject, header, content); (h) DNS requests and registry configurations; (i) user account activities (logins, privileged user account activity, privilege escalation); (j) database traffic (read/write), requests to the same file. This type of information may include data relating to indicators describing patterns in network traffic corresponding to known attacks/botnet communications, IP addresses of machines infected with malware (bots), data relating to "command and control" servers used by malware (usually domains or IP addresses), and URLs relating to phishing sites or websites observed hosting malware or exploit kits.	Alphanumeric	Yes, if information about indicators of compromise connected with the cyber threat are available.)
20	Other relevant information	Any other relevant information about the significant cyber threat	Alphanumeric	Yes, if applicable and if there is other information available, not covered in the template.