

FiMiS - User Guide for DORA_INCIDENT- and DORA_CYBERTHREAT-Surveys

Inhoudstafel

I.	OVERZICHT	2
II.	TOEGANG TOT FiMiS	3
III.	EERSTE GEBRUIK VAN FiMiS	4
1.	FiMiS starten.....	4
2.	Een certificaat selecteren	4
3.	Eerste schermen bij aanmelding op het FiMiS-platform.....	4
4.	De loginpagina	6
IV.	TOEGANG TOT DE SURVEYS.....	8
1.	Via het tabblad “My eDossier”	8
2.	Via het tabblad “Dossiers”	8
3.	Via het tabblad “Surveys”	10
4.	Creatie nieuwe survey	10
V.	RICHTLIJNEN VOOR HET INVULLEN VAN DE DORA_INCIDENT- EN DORA_CYBERTHREAT-SURVEYS.....	11
1.	Voorafgaand	11
2.	Nieuwe DORA_INCIDENT- of DORA_CYBERTHREAT-survey creëren	12
3.	De DORA_INCIDENT-survey invullen	13
a.	Algemeen	13
b.	Sectie “General information about the financial entity”	14
c.	Sectie Notification	15
d.	Herclassificatie van een ernstig ICT-incident naar een niet-ernstig ICT-incident.....	17
4.	De DORA_CYBERTHREAT-survey invullen	18
5.	De DORA_INCIDENT- en DORA_CYBERTHREAT surveys indienen	18
6.	Validation report: errors en warnings	19
	Bijlage 1: lijst van in te vullen velden DORA_INCIDENT-survey	21
	Bijlage 2: lijst van in te vullen velden DORA_CYBERTHREAT-survey.....	44

I. OVERZICHT

Dit document betreft een handleiding voor het gebruik van de DORA_INCIDENT- en DORA_CYBERTHREAT-surveys in FiMiS. Deze surveys stellen u in staat om, conform de verwachtingen van de Digital Operational Resilience Act (hierna 'DORA-verordening'), ernstige ICT-incidenten of significante cyberdreigingen waarvan uw entiteit slachtoffer is geworden te melden aan de FSMA. De FSMA zal deze op haar beurt doorsturen naar de Europese Toezichthoudende Autoriteiten (hierna 'ESAs').

Het document bespreekt eerst algemeen de toegang tot de beveiligde omgeving van FiMiS, en hoe deze applicatie gebruikt dient te worden.

Hierna gaan we in op de werking van de specifieke DORA_INCIDENT en DORA_CYBERTHREAT-surveys die werden opgesteld conform aan de vereisten van de DORA-verordening. In de bijlagen bij dit document vindt u de exacte vereisten met betrekking tot de in te vullen velden terug.

De incident rapportering dient te gebeuren in drie opeenvolgende fases (zie figuur 1: ICT-Incident kennisgevingsproces), namelijk (1) de eerste kennisgeving, (2) het tussentijdse verslag en (3) het eindverslag. Hoe verder in het kennisgevingsproces, hoe meer informatie gevraagd zal worden. Desgevallend werd er ook een herclassificatie van het ernstige incident als niet-ernstig voorzien. Voor de rapportering van significante cyberdreigingen is er daarentegen slechts één enkele fase.

De FSMA stuurt een survey met betrekking tot een bepaalde fase van kennisgeving onmiddellijk door naar de ESAs. Wijzigingen aan de ingediende survey zijn vanaf dan niet meer mogelijk. Omzichtigheid is dus geboden bij het invullen van de surveys.

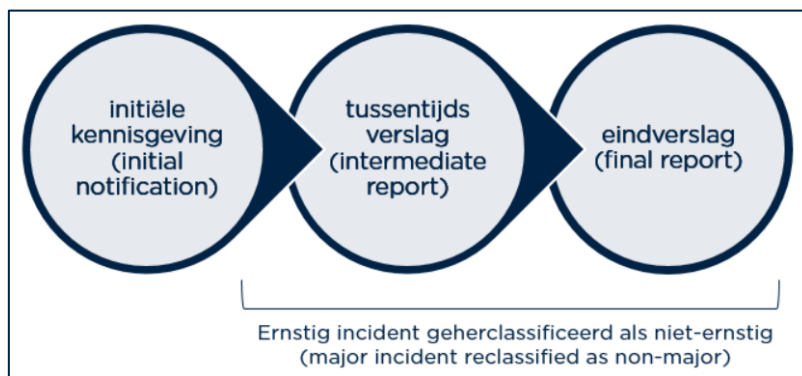
Specifiek met betrekking tot de incident rapportering kunnen evenwel nog wijzigingen aangebracht worden in latere fases van het kennisgevingsproces. Indien een verkeerde waarde werd ingegeven bij een survey voor een tussentijds verslag, kan deze waarde dus verbeterd worden bij het indienen van de survey voor een eindverslag.

Indien het ICT-incident u verhindert om zich te connecteren op het FiMiS-platform en de desbetreffende survey, kan u om het incident te melden uitzonderlijk contact opnemen met de FSMA (zie ook: [Nadere toelichting bij het opvragen van het informatieregister over derde dienstverleners en over meldingen van ernstige ICT-incidenten | FSMA](#)) via

- Mail: dora@fsma.be; of
- Telefoon: +32(0)2 220 52 11.

Bijgevoegde instructies bieden klaarheid bij het gebruik van de DORA_INCIDENT- en DORA_CYBERTHREAT-surveys. Aarzel niet om contact op te nemen met de FSMA indien u problemen ondervindt met betrekking tot

- De inhoud van de respectieve surveys via dora@fsma.be;
- Technische problemen met betrekking tot FiMiS: Servicedesk@fsma.be.



Figuur 1: ICT-incident kennisgevingsproces

II. TOEGANG TOT FiMiS

Om toegang te krijgen tot FiMiS, heeft elke gebruiker een persoonlijk certificaat nodig. U kan hierbij kiezen uit de volgende certificaten:

- Globalsign Personal 3 (<http://www.globalsign.be>);
- Isabel (<http://www.isabel.be>);
- Uw elektronische identiteitskaart (eID) (<http://eid.belgium.be>).

Opmerkingen:

- Gebruikt u een Isabel-kaart of een eID, dan heeft u een kaartlezer nodig.
- Gebruikt u een eID, dan moet u de eID-software downloaden (<http://eid.belgium.be>).

Een persoonlijk certificaat wordt u door een erkende derde partij toegekend. Na aankoop van een certificaat moet u het, conform de richtlijnen van de verstrekker, installeren op de pc die u zal gebruiken om toegang te krijgen tot FiMiS.

Voor meer informatie kunt u bij de verstrekker van uw certificaat terecht.

Het certificaat is strikt persoonlijk. Elke gebruiker moet dus zijn eigen certificaat hebben.

III. EERSTE GEBRUIK VAN FiMiS

1. FiMiS starten

Start FiMiS via het “[Digitaal loket](#)” op de FSMA-website. Klik daarna op de knop “**FiMiS Survey**”.

2. Een certificaat selecteren

Zijn er verschillende certificaten op uw pc geïnstalleerd, dan vraagt het systeem u het certificaat te kiezen dat u wilt gebruiken.

- Voor een eID: klik op het certificaat “Citizen CA xxxx” en dan op OK.
- Voor een ander certificaat: klik op het certificaat en dan op OK.



Gebruikt u een Isabel-kaart of een eID, dan wordt u gevraagd uw code in te geven.



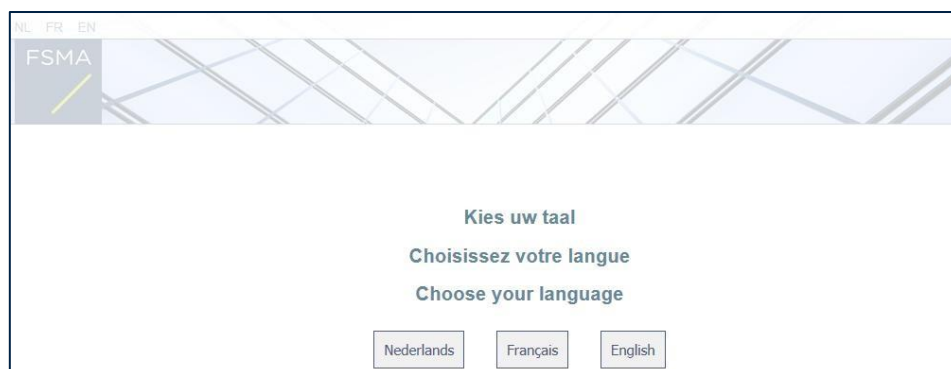
Geef uw code in en klik op OK.

Opgelet: het gaat hier om uw pin- of Isabel-code, niet om uw activeringscode van FiMiS.

3. Eerste schermen bij aanmelding op het FiMiS-platform

U bent nu geïdentificeerd als gebruiker met een geldig certificaat. Als onderstaand scherm niet verschijnt, is er iets fout gelopen bij de installatie van het certificaat. Contacteer in dit geval de Servicedesk van de

FSMA (Servicedesk@fsma.be).



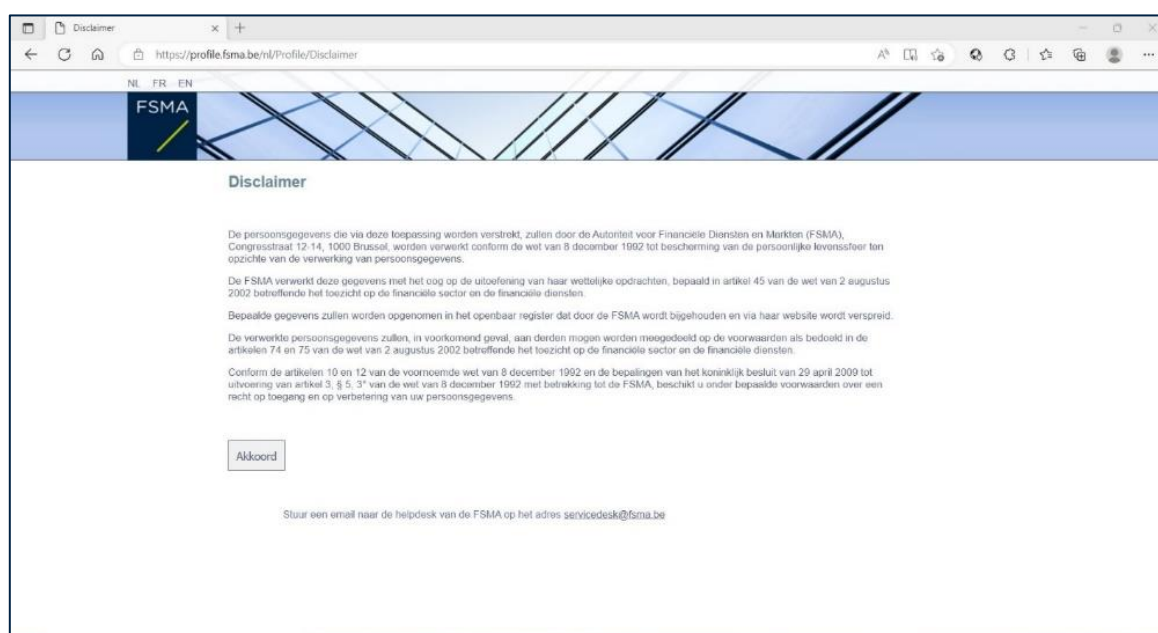
Figuur 2: keuzescherf taal in FiMiS

U kiest nu de taal waarin u wil werken. Later kan u uw taalkeuze nog aanpassen. De DORA_INCIDENT- en DORA_CYTBERTHREAT-surveys zullen in drie talen (Nederlands, Frans, Engels) beschikbaar worden gesteld.

OPGELET!

Gegeven het feit dat de betrokken regelgevende teksten (RTS en ITS) nog niet officieel gepubliceerd werden, heeft de FSMA momenteel de survey enkel in het Engels ontwikkeld, op basis van de instructies die met de FSMA gedeeld werden door de ESAs. Zodra de desbetreffende regelgevende teksten worden gepubliceerd, zal de FSMA de surveys eveneens in het Nederlands en het Frans aanbieden.

Om gebruik te maken van FiMiS dient u ook akkoord te gaan met de disclaimer omtrent de verwerking van persoonlijke gegevens (zie Figuur 3: disclaimer omtrent gebruik persoonlijke gegevens).



Figuur 3: disclaimer omtrent gebruik persoonlijke gegevens

Tot slot vraagt de applicatie u nog om uw identificatiegegevens in te geven (zie Figuur 4: scherm registratie van uw gebruikersprofiel). Dit hoeft u maar één keer te doen. Zodra u dit gedaan heeft klikt u op “Register” en de FiMiS-applicatie wordt opgestart.

Registratie van uw gebruikersprofiel

Identificatiegegevens

Naam *

Voorname *

Tweede Naam

Belgisch Registratienummer *

E-Mail *

Taal *

Gender *

Bedrijfsgegevens

Bedrijf *

KBO Nummer

Contactgegevens

Telefoon

Gen Nummer

Fax

Adresgegevens

Straat *

Postcode *

Plaats *

Land *

Certificatiegegevens

Cert Authority: Citizen CA

Serial Number: 9605253175

Certificate DN: O=Luzac Hendrick (Authenticatie), C=BE

Register

Stuur een e-mail naar de helpdesk van de FSMA op het adres servicedesk@fsma.be

Figuur 4: scherm registratie van uw gebruikersprofiel

4. De loginpagina

Bij uw eerste aanmelding op FiMiS moet u de activeringscode gebruiken die de FSMA u heeft bezorgd.

NL FR EN

FSMA FiMiS

LOG ON

Activation Code :

Log On

Bij deze identificatie koppelen we deze activeringscode automatisch aan het certificaat dat u gebruikt. Bij uw volgend gebruik van FiMiS moet u zichzelf dan niet opnieuw met uw activeringscode identificeren. U komt nu op de FiMiS-homepage terecht.

FIMIS

MY EDOSSIER

DOSSIERS

SURVEYS

PRIVACY & COOKIES

FSMA FOLLOW UP, API

EN

I Want To

New Survey

Links

eCorporate

eManex

FSMA Site

FSMA Business Portal

Quick filters:

ALL

DORA_AWARENESS

DORA_AWARENESS2

DORA_CYBERTHREAT

DORA_INCIDENT

Surveys

Dossier	Survey	Regarding	Period	Situation	Lifecycle	State	Due Date	Received Date
FIMIS 1	DORA_Incident - TESTSAM_INIT		16/01/2025		Open	Initial		
FIMIS 1	DORA_Incident - TESTSAM250115_INIT		15/01/2025		Closed	Ok		15/01/2025
FIMIS 1	DORA_Incident - TESTSAM250115_FIN		15/01/2025		Open	Error		
FIMIS 1	DORA_Incident - DORA Incident 2025-01-15 - 123		15/01/2025		Closed	Ok		15/01/2025
FIMIS 1	DORA_Incident - TESTSAM250115_INIT		15/01/2025		Closed	Ok		15/01/2025
FIMIS 1	DORA_Incident - Dora Incident 2025-01-14 - 001 - Final		14/01/2025		Closed	Ok		14/01/2025
FIMIS 1	DORA_Incident - Dora Incident 2025-01-14 - 001 - Initial		14/01/2025		Closed	Ok		14/01/2025
FIMIS 1	DORA_Incident - Dora Incident 2025-01-14 - 001 - Intermediate		14/01/2025		Closed	Ok		14/01/2025
FIMIS 1	DORA_Incident - TESTSAM_INIT		14/01/2025		Open	Error		
FIMIS 1	DORA_Incident - Dora Incident 2025-01-10 - 001 - Intermediate		10/01/2025		Open	Error		
FIMIS 1	DORA_Incident - Dora Incident 2025-01-10 - 001 - Initial		10/01/2025		Closed	Ok		10/01/2025
FIMIS 1	DORA_Incident - Dora Incident 2025-01-10 - 001 - Initial		10/01/2025		Closed	Ok		14/01/2025
FIMIS 1	DORA_Incident - Dora Inc test Paul		09/01/2025		Open	Error		
FIMIS 1	DORA_Incident - Dora Incident 2025-01-09 - 002 - Reclassified		09/01/2025		Closed	Ok		09/01/2025
FIMIS 1	DORA_Incident - Dora Incident 2025-01-09 - 001 - Initial		09/01/2025		Closed	Ok		09/01/2025
FIMIS 1	DORA_Incident - Dora Incidents - Dora Incident 2025-01-09 - 001 - Final		09/01/2025		Closed	Ok		09/01/2025
FIMIS 1	DORA_Incident - Dora Incident 2025-01-09 - 002 - Initial		09/01/2025		Closed	Ok		09/01/2025
FIMIS 1	DORA_Incident - Dora Incident 2025-01-09 - 001 - Intermediate		09/01/2025		Closed	Ok		09/01/2025
FIMIS 1	DORA_Incident - Dora Incident 2025-01-08 - 3		08/01/2025		Closed	Ok		08/01/2025
FIMIS 1	DORA_Incident - Dora Incident 2025-01-08 - 001 - Initial		08/01/2025		Closed	Ok		08/01/2025

Items per page: 201 - 20 of 2612

Dossiers

Dossier	Type	State	Business Role
---------	------	-------	---------------

Figuur 5: FiMiS-homepage

In de tabel hieronder werden enkele definities opgenomen met betrekking tot de terminologie die gebruikt wordt in de applicatie en die u kunnen helpen bij een beter begrip van de FiMiS-applicatie.

Concept	Definitie
Dossier	De onderneming(en) waarvoor u kan rapporteren.
Survey	Een naam die u aan de survey heeft gegeven die u in staat stelt de survey naderhand makkelijk terug te vinden. In geval van een DORA_INCIDENT-survey kan het bv. nuttig zijn het type van de kennisgeving mee op te nemen (initiële kennisgeving, tussentijds verslag of eindverslag).
Period	De datum waarop de survey is aangemaakt (bv. 17/01/2025).
Lifecycle	Dit begrip geeft aan of de rapportering geopend of afgesloten is. Er zijn twee mogelijkheden: <ul style="list-style-type: none"> Open: de survey is geopend en kan worden ingevuld; Closed: de survey is afgesloten en kan niet meer worden gewijzigd.
State	Dit begrip geeft aan hoever de rapportering is gevorderd. De mogelijke waarden zijn: <ul style="list-style-type: none"> Initial: de survey is leeg, er is nog geen enkel gegeven ingebracht; Error: er zitten nog steeds (kritieke) fouten ("errors" – zie V.6. Report validation: errors en warnings) in de gegevens die in een of meer secties van de survey zijn ingebracht. Zolang die fouten niet zijn gecorrigeerd, kan de survey niet worden ingediend ("Submit the Survey"). Warning: er zitten nog steeds fouten ("warnings" – zie V.6. Report validation: errors en warnings) in de gegevens die in een of meer secties van de survey zijn ingebracht. Deze beletten u echter niet om de survey in te dienen ("Submit the Survey"). Ok: alle gegevens die in alle secties zijn ingevoerd, voldoen (zonder verdere aandachtspunten) aan de validatieregels.

IV. TOEGANG TOT DE SURVEYS

Er zijn drie manieren om toegang te verkrijgen tot specifieke surveys:

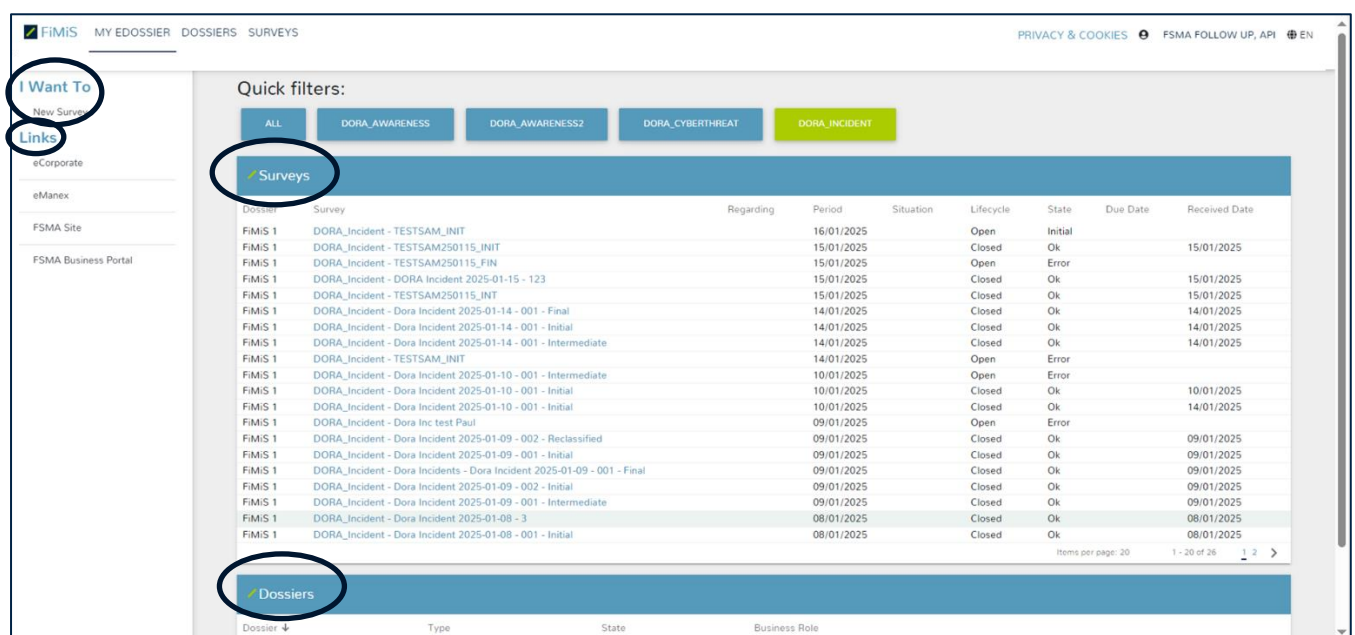
- Via het tabblad “My eDossier”
- Via het tabblad “Dossiers”
- Via het tabblad “Surveys”

1. Via het tabblad “My eDossier”

Via het tabblad “**My eDossier**” (zie Figuur 6: scherm My eDossier) krijgt u een overzicht van de dossiers en de surveys waartoe u toegang heeft, alsook enkele kerngegevens over deze dossiers en surveys.

Dit scherm bestaat uit 4 luiken:

- Surveys: alle rapporteringen van de entiteiten die u aanbelangen;
- Dossiers: alle entiteiten waarvoor u als contactpersoon bent aangesteld;
- I Want To: de beschikbare acties – in dit luik kan u een nieuwe survey lanceren door op “New Survey” te klikken;
- Links: de links naar andere sites.



Figuur 6: scherm My eDossier

Klikt u op een survey, dan komt u bij het tabblad Surveys terecht van de aangeklikte survey.

Klikt u op een Dossier, dan komt u bij het tabblad Dossiers van het aangeklikte dossier (nl. de onderneming waarover wordt gerapporteerd) terecht.

2. Via het tabblad “Dossiers”

Via dit tabblad (zie Figuur 7: scherm Dossiers) kan u alle dossiers zichtbaar maken waartoe u toegang hebt,

enkel de dossiers zichtbaar maken die aan de geselecteerde filters voldoen, of de informatie van een dossier dat u via een ander tabblad hebt geselecteerd consulteren.

Klikt u op een dossier, dan krijgt u een scherm met aanvullende informatie over dat dossier en over de lijst met surveys. Klikt u op een van die surveys, dan komt u op het betrokken tabblad terecht.

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

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	

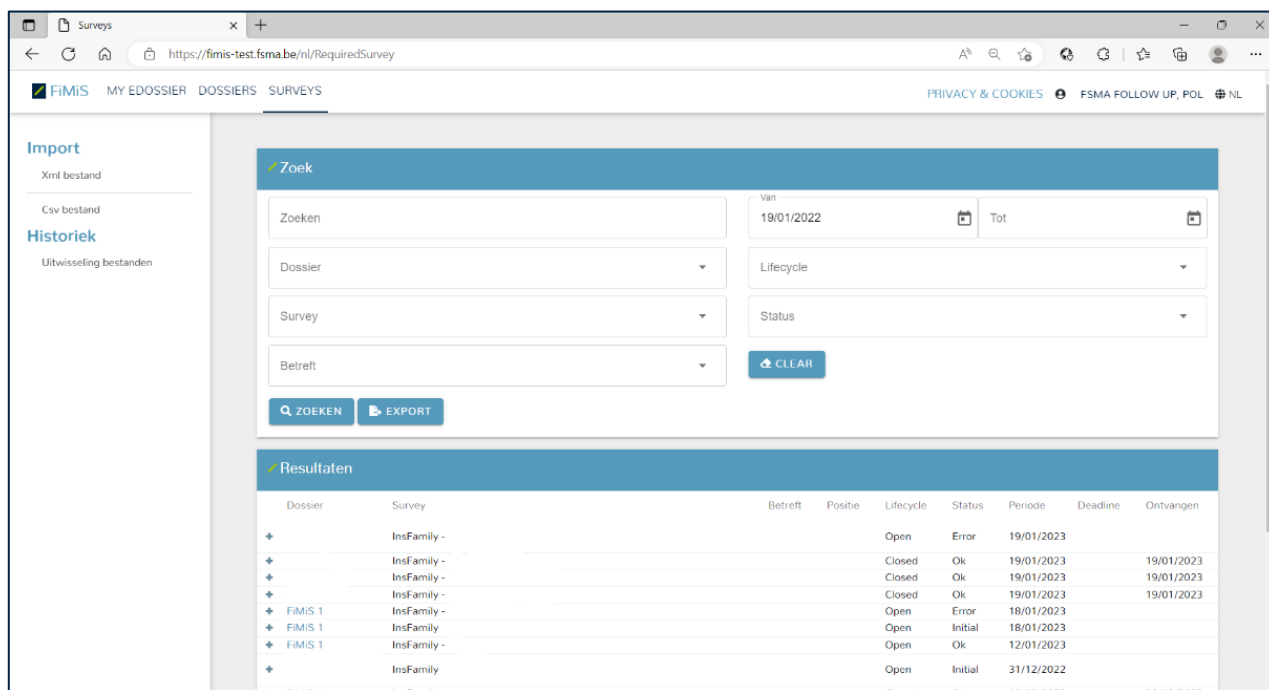
Items per page: 20 1 - 10 of 10

Figuur 7: scherm Dossiers

3. Via het tabblad “Surveys”

Via dit tabblad (zie Figuur 8: scherm Surveys) kan u alle surveys zichtbaar maken waarvoor u als contactpersoon bent aangesteld, ofwel enkel de surveys die aan de geselecteerde filters voldoen, ofwel de informatie van een survey die u via een ander tabblad hebt geselecteerd.

Klikt u op een survey, dan kan u de verschillende secties van die survey zien.



Figuur 8: scherm Surveys

4. Creatie nieuwe survey

Om een nieuwe survey te creëren dient u op het scherm “My eDossiers” (zie figuur 9: scherm “My eDossiers”) onder het luik “I want to” op “New Survey” te klikken. Het scherm “New Survey” zal worden geopend (zie figuur 9: scherm New survey).

Voor elke nieuwe kennisgeving van een ernstig ICT-incident, een update in een nieuwe fase in het kennisgevingsproces voor een reeds gerapporteerd incident (zie verder), of voor elke kennisgeving van een significante cyberdreiging dient op deze wijze een nieuwe survey gecreëerd te worden.

V. RICHTLIJNEN VOOR HET INVULLEN VAN DE DORA_INCIDENT- EN DORA_CYBERTHREAT-SURVEYS

1. Voorafgaand

*Met betrekking tot de kennisgeving van een **ernstig ICT-incident (DORA INCIDENT-survey)**:*

- Het kennisgevingsproces voor ernstige ICT-incidenten bestaat uit **drie fasen** (zie ook figuur 1: ICT-incident kennisgevingsproces): (1) de eerste kennisgeving, (2) het tussentijdse verslag en (3) het eindverslag. Voor elke fase van kennisgeving (initiële kennisgeving, tussentijds verslag, eindverslag) dient in FiMiS een nieuwe survey opgesteld te worden. Ingevoerde informatie uit surveys in het kader van eerdere kennisgevingen kan opnieuw opgeladen worden door in “previous survey” (zie ¹ in figuur 9: scherm New Survey) de eerder ingediende survey te selecteren.
- Zodra een DORA_INCIDENT-survey (die ofwel een eerste kennisgeving, tussentijdse verslag en eindverslag betreft) wordt ingediend, wordt deze **automatisch en onmiddellijk verstuurd** naar de ESAs. **Er is bijgevolg geen verbetering meer mogelijk van de survey zodra deze werd ingediend.** Verbeteringen van de eerste kennisgeving kunnen enkel nog aangebracht worden bij het indienen van tussentijdse verslag(en) (cf. supra). Verbeteringen aan de eerste kennisgeving en tussentijdse verslag(en) kunnen nog aangebracht worden bij het invoeren van het eindverslag (cf. supra). Zodra een eindverslag wordt ingediend, zijn er evenwel geen aanpassingen meer mogelijk.
- Eén veld in de DORA_INCIDENT-survey is definitief zodra het werd ingediend bij de eerste kennisgeving. Het betreft de **Incident Referentie Code die door de financiële instelling werd bepaald** (“Incident reference code assigned by the financial entity”) en die dient ingevuld te worden bij de eerste kennisgeving. De waarde die in dit veld wordt ingegeven is definitief aangezien deze referentie doorheen het hele incident kennisgevingsproces gebruikt wordt om het incident uniek te kunnen identificeren (zowel door de FSMA als door de ESAs).
- **Het wordt ten zeerste aangeraden de survey in elke fase van het incident-kennisgevingsproces met de nodige omzichtigheid, zo correct en zo volledig als mogelijk in te vullen.**

*Met betrekking tot de vrijwillige kennisgeving van een **cyberdreiging (DORA CYBERTHREAT-survey)**:*

- Voor de vrijwillige kennisgeving van een cyberdreiging dient slechts één survey te worden ingevuld. Ook deze kennisgeving wordt automatisch en onmiddellijk doorgestuurd naar de systemen van de ESAs. Zodra u deze kennisgeving heeft ingediend zijn er dus geen wijzigingen meer mogelijk.
- Het wordt ten zeerste aangeraden de survey voor de kennisgeving van een cyberdreiging met de nodige omzichtigheid, zo correct en zo volledig als mogelijk in te vullen.

2. Nieuwe DORA_INCIDENT- of DORA_CYBERTHREAT-survey creëren

The screenshot shows the 'New Survey' interface. On the left, there's a sidebar with 'Import' (containing 'Xml File' and 'Csv File') and 'History' (containing 'File exchange'). The main form area has a title bar 'New Survey'. Below it are four input fields: 'Survey *' (a dropdown menu currently showing 'DORA Incidents'), 'Dossier *' (a dropdown menu), 'Your reference' (a text input field), and 'Previous Survey' (a dropdown menu). A red circle with the number '1' and a red arrow points to the 'Previous Survey' dropdown. At the bottom right of the form is a button labeled 'Create a new survey' with a right-pointing arrow.

Figuur 9: scherm “New Survey”

Indien u de FSMA in kennis dient te brengen van een ernstig ICT-incident¹ of indien u de informatie over een bestaand incident wil aanvullen (ofwel voor het tussentijdse verslag, ofwel voor het eindverslag), dient u een nieuwe survey te creëren.

In het scherm “New Survey” (zie figuur 9) dient u minstens volgende velden aan te vullen:

- In het veld “Survey” dient u het type survey te kiezen (in dit geval DORA INCIDENTS).
- In het veld “Dossier” kan u aangeven voor welke instelling u een survey wenst te creëren.
- In het veld “Your reference” kan u een eigen referentie aan de survey toevoegen om deze later makkelijker te kunnen terugvinden.
- Indien de survey geen eerste kennisgeving betreft, maar een tussentijds verslag of eindverslag, kan u in het veld “Previous Survey” (zie ① in figuur 9) een eerder ingediende survey selecteren. Op die manier worden alle reeds ingevulde velden van deze eerdere survey opgeladen in deze nieuwe survey.
- Klik hierna op “Create a new survey” om naar het volgende scherm te gaan.

¹ Zie voor de classificatiecriteria de *regulatory technical standard* (RTS) “for the classification of ICT-related incidents and cyber threats” ([Delegated regulation - EU - 2024/1772 - EN - EUR-Lex](#)) of de pedagogische documentatie met betrekking tot DORA op de website van de FSMA ([DORA-verordening | FSMA](#)).

3. De DORA_INCIDENT-survey invullen

Het invullen van de DORA_INCIDENT-survey, die volledig werd opgesteld in lijn met de verwachtingen van de ESAs, verloopt over het algemeen zeer intuïtief. Er zijn echter een aantal zaken waar u rekening mee dient te houden.

The screenshot shows the FIMIS interface for the 'DORA Incident - DORA Incidents' survey. The left sidebar contains a 'Sections' menu with 'General information about the financial entity' and 'Notification'. Below this is an 'Actions' menu with options like 'Load Last Submitted Survey', 'Export Survey to PDF', 'Export Survey to Excel', 'Submit the Survey', and 'Back to Dashboard'. The main form area is titled 'General information about the financial entity' and includes fields for 'Type of report' (1.1), 'Name of the entity submitting the report' (1.2), 'Identification code of the entity submitting the report (LEI)' (1.3a), 'Identification code of the entity submitting the report (EU ID)' (1.3b), 'Type and identity of the financial entity affected' (1.4, 1.5, 1.6), and 'Primary contact person name' (1.7). Red circles and arrows highlight specific elements: circle 1 points to the 'Sections' sidebar, circle 2 points to the 'Type of report' dropdown, and circle 3 points to the 'Submit the Survey' button.

Figuur 10: Scherm 'General information about the financial entity'

a. Algemeen

- De survey is opgebouwd uit 2 secties (zie 1 in Figuur 10: Scherm “General information about the financial entity”), namelijk een sectie “General information about the financial entity” en een sectie “Notification”. U kan tussen beide secties navigeren door ofwel op “Next” te klikken, ofwel op de respectieve naam onder het luik “Sections”. Na het correct invullen van de sectie “General information about the financial entity” kan u navigeren naar de sectie “Notification”.
- Onder het luik “Actions” wordt u de mogelijkheid aangeboden om de survey te exporteren in pdf- of Excel-formaat. Hier wordt ook de mogelijkheid geboden om de laatst beschikbare survey op te laden (“Load Last Submitted Survey”). Aangezien een survey in het geval van de rapportering van ernstige ICT-incidenten of cyberdreigingen definitief is zodra hij werd ingediend, zal deze mogelijkheid echter in dit geval niet beschikbaar zijn. Een wijziging aan een eerdere kennisgeving van een ernstig ICT-incident kan enkel maar gebeuren door een nieuwe survey in een latere fase (tussentijds verslag of eindverslag) te creëren (cf. supra). **De wijziging van een kennisgeving van een significante cyberdreiging is niet meer mogelijk zodra deze werd doorgestuurd (cf. supra).**
- Verder is er nog een knop “Submit the Survey”, die blauw zal oplichten zodra alle ingevoerde gegevens gevalideerd zijn en er geen “errors” meer zijn.
- Hieronder bevindt zich nog een knop waarmee u kan terugkeren naar het algemene overzicht van alle surveys (“Back to Dashboard”).

BELANGRIJKE INFORMATIE

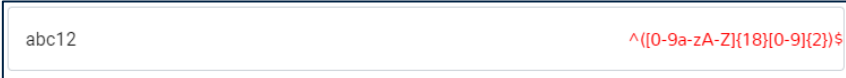
De verwachte waarde per in te vullen veld zal door de ESAs verduidelijkt worden in de betrokken *implementing technical standard* (ITS). Deze is nog niet gepubliceerd. In afwachting van de publicatie werd aan de FSMA een Excel-bestand ter beschikking gesteld door de ESAs waarin de verwachte waarden per veld worden verduidelijkt. Voor uw gemak hebben wij de betrokken tabel gekopieerd in Bijlage 1: lijst van in te vullen velden DORA_INCIDENT-survey. De nummering voor de velden die

gebruikt wordt in het Excel-bestand (en overgenomen in Bijlage 1) komt overeen met de nummering zoals opgenomen in de DORA_INCIDENT-survey in FiMiS. Dit zou u in staat moeten stellen om makkelijk de vereiste informatie per veld terug te kunnen vinden.

- Afhankelijk van het type kennisgeving dat u selecteert (initiële kennisgeving, tussentijds verslag, eindverslag of herclassificatie; zie 2 in figuur 10: Scherm “Algemene informatie over de financiële instelling”), zullen de validatieregels voor de sectie “Notification” beïnvloed worden en dienen meer of minder velden ingevuld te worden om de survey met betrekking tot de kennisgeving van een ernstig ICT-incident in te kunnen dienen.
- Het is mogelijk om een tussentijds verslag of een eindverslag in te dienen zonder eerst een eerste kennisgeving of tussentijds verslag in te dienen. Indien u dit wenst te doen, selecteert u bij het type rapport de fase van kennisgeving die u wenst in te dienen (zie 2 in figuur 10: Scherm “Algemene informatie over de financiële instelling”). Let er evenwel op dat het overslaan van een fase in het kennisgevingsproces u er niet van ontslaat om de gevraagde velden in deze overgeslagen fase toch in te vullen.
- Doorheen de survey zal u geregeld het plussymbool zien staan (+). Door op dit symbool te klikken kan u een lijn met een extra antwoordmogelijkheid toevoegen. In het geval van velden 1.4, 1.5 en 1.6 (zie 3 in figuur 10: Scherm “Algemene informatie over de financiële instelling”) kan u bijvoorbeeld extra lijnen toevoegen indien uw entiteit meerdere gereguleerde statuten heeft (bijvoorbeeld, een “Management Company” en een “Manager of alternative investment fund”).



b. Sectie “General information about the financial entity”

- In het geval er problemen zijn met het formaat van de ingevoerde waarde (“pattern check”) voor de LEI-code (maar ook voor datum- en tijdsaanduidingen en voor andere waardes zoals percentages) zal de foutboodschap in het veld zelf worden weergegeven en niet in de *Validation report* (zie figuur 11: foutmelding incorrecte LEI-code). Het formaat moet eerst verbeterd worden alvorens u verder kan gaan met de survey. Indien er een probleem is met de validiteit van de LEI-code (“check digits”) zal deze worden opgenomen in de “errors” (zie: V.6. Validation report: errors en warnings).



The image shows a rectangular input field. On the left side of the field, the text 'abc12' is entered. On the right side of the field, there is a red error message: '^([0-9a-zA-Z]{18}[0-9]{2})\$'.

Figuur 11: incorrect formaat LEI-code (“pattern check”)

- Er is geen specifieke controle voorzien voor de EU ID. Gegeven het ontbreken van deze controle op de EU ID en het feit dat in andere velden voornamelijk de LEI-code wordt gevraagd, raden wij u ten zeerste aan te opteren voor de LEI-code indien u de keuze heeft tussen beide.
- Zodra u alle gegevens correct heeft ingevuld zal het mogelijk zijn deze te valideren en te bewaren () en zo verder te gaan () naar de effectieve kennisgeving van het ernstige ICT-incident (sectie “Notification”).

Het invoeren van de gegevens in de Sectie “General information about the financial entity” dient enkel te gebeuren bij de eerste kennisgeving van een ernstig ICT-incident, of, indien u beslist de eerste kennisgeving

of het tussentijdse verslag over te slaan, respectievelijk bij het tussentijdse verslag of het eindverslag. Nadien zullen deze gegevens automatisch overgenomen worden zodra u bij de creatie van een nieuwe survey voor een tussentijds verslag of eindverslag verwijst naar een vorige survey door het veld “previous survey” aan te vullen (zie ① in figuur 9: scherm “New Survey”).

c. Sectie Notification

In Bijlage 1: lijst van in te vullen velden DORA_INCIDENT-survey kan u de vereiste informatie die gevraagd wordt per veld door nemen. De nummering die per veld in deze bijlage werd opgenomen, komt overeen met de nummering van de velden in de survey, wat u in staat stelt om makkelijk de benodigde informatie terug te kunnen vinden.

The screenshot displays the 'Notification' section of the FIMIS survey. The interface includes a left sidebar with navigation links and a main content area with various input fields and buttons. Red circles with numbers 1 through 5 and red arrows point to specific elements:

- 1**: Points to the survey header information on the left sidebar, including 'FIMIS 1', 'DORA_Incident', '20/01/2025', and 'Name: TEST2501205'.
- 2**: Points to the 'Incident reference code assigned by the financial entity' field (2.1), which contains the value 'YYYY-MM-DDThh:mm:ssZ (ISO 8601)'.
- 3**: Points to the 'Other relevant information' field (2.10) at the bottom of the form.
- 4**: Points to the 'Validate & Save' button at the top right and the 'Validate & Save' button at the bottom right of the form.
- 5**: Points to the 'Submit the Survey' button in the left sidebar.

The form fields include:

- Incident reference 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)
- Other relevant information (2.10)

Figuur 12: scherm luik "notification" - deel 1

Figuur 13: scherm luik "notification" - deel 2

In de sectie "Notification" zijn er evenwel ook een aantal punten die nuttig zijn om op voorhand te weten:

- Het is mogelijk om al informatie toe te voegen die gevraagd wordt in andere fases van het kennisgevingsproces, of om eerder ingevulde informatie te verbeteren. Om te navigeren tussen de drie fases van de kennisgeving volstaat het om op "initial", "intermediate" of "final" te klikken bij ¹ in Figuur 12: scherm luik "notification" - deel 1, of op "next" bij ⁴ in hetzelfde figuur.
- Voor sommige velden dient een **datum- en tijdsaanduiding** gegeven te worden (zie bv. ² in Figuur 12: scherm luik "notification" - deel 1). De ESAs gebruiken hiervoor de ISO8601 standaard. De FSMA heeft deze standaard als dusdanig overgenomen in deze survey. Bijgevolg dienen datum en tijd in volgend formaat genoteerd te worden: YYYY-MM-DDThh:mm:ss, waarbij
 - YYYY staat voor het jaartal in 4 cijfers
 - MM staat voor de maand in 2 cijfers
 - DD staat voor de dag in 2 cijfers
 - T de indicatie is dat wat erna volgt de tijdsaanduiding betreft
 - hh het uur betreft in 2 cijfers
 - mm de minuten betreft in 2 cijfers
 - ss de seconden betreft in 2 cijfers
 - Bijvoorbeeld:
 - Indien het incident ontdekt werd op **17 januari 2025 om 12u23** dient dit als volgt genoteerd te worden: **2025-01-17T12:23:00**.
 - Indien u de datum- en tijdsaanduiding niet volgens het correcte formaat heeft ingevoerd, zal er een foutmelding (zie figuur 14) in het veld verschijnen. U zal niet verder kunnen gaan met de survey (op "next" klikken, of navigeren tussen de fases van het kennisgevingsproces, of op "validate & save" klikken) zolang de datum- en tijdsaanduiding niet in het correcte formaat staan.

Figuur 14: foutmelding bij verkeerd formaat datum- en tijdsaanduiding ("pattern check")

- In sommige velden zal u een **duurtijd** moeten aangeven (bijvoorbeeld bij het veld met betrekking tot

de “service downtime” – zie ⁶ in Figuur 13: scherm luik “notification” - deel 2). De duurtijd dient uitgedrukt te worden in het formaat **DDD:HH:MM**, waarbij DDD het aantal dagen betreft, HH het aantal uren (die niet meer mogen bedragen dan 23) en MM het aantal minuten (die niet meer mogen bedragen dan 59).

- Bijvoorbeeld: een incident met een **duurtijd van 74 uur en 32 minuten** dient dus als volgt genoteerd te worden: **003:02:32**.
- In geval het formaat waarin de duurtijd werd ingegeven niet correct is, zal er een foutboodschap verschijnen in het veld. U dient het veld eerst te corrigeren alvorens u verder kan gaan (cf. datum- en tijdsaanduiding hierboven).

d. Herclassificatie van een ernstig ICT-incident naar een niet-ernstig ICT-incident

- In geval het ernstige ICT-incident dat eerder werd ingevoerd geherclassificeerd moet worden naar niet-ernstig op basis van een herbeoordeling van de criteria die het incident eerder wel als ernstig classificeerden², kan u dit doen door in de sectie “General information about the financial entity” in het veld “type of report” “major incident reclassified as non-major” te selecteren (zie ² in Figuur 10: Scherm “Algemene informatie over de financiële instelling”).
- Wanneer u dit doet, dient u de redenen van de herclassificatie te verduidelijken in het veld 2.10 “other relevant information” in de sectie “notification” bij de eerste kennisgeving (zie ³ in Figuur 12: scherm luik “notification” - deel 1).
- De correctheid en volledigheid van de redenen voor de herclassificatie kunnen na het indienen beoordeeld worden door de FSMA.

² Zie voor de classificatiecriteria de RTS “for the classification of ICT-related incidents and cyber threats” ([Delegated regulation - EU - 2024/1772 - EN - EUR-Lex](#)) of de pedagogische documentatie met betrekking tot het DORA op de [website van de FSMA](#).

4. De DORA_CYBERTHREAT-survey invullen



Figuur 15: scherm Significant Cyber Threats


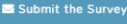
Voor de DORA_CYBERTHREAT-survey is er slechts één sectie die ingevuld dient te worden ("Significant Cyber Threats"). Voor de vereisten per in te vullen veld kan u in Bijlage 2: lijst van in te vullen velden DORA_CYBERTHREAT-survey de nodige informatie terugvinden. De nummers bij de velden in de DORA_CYBERTHREAT-survey komen overeen met de gebruikte nummers in Bijlage 2, wat u in staat moet stellen om makkelijk de benodigde informatie over de vereisten per veld terug te vinden.

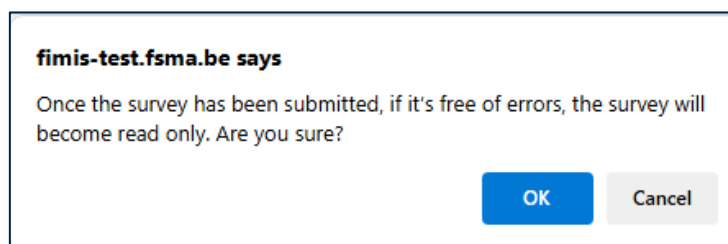
Het invullen van deze DORA_CYBERTHREAT-survey gebeurt op een gelijkaardige wijze als hierboven uitgelegd voor de DORA_INCIDENT-survey (zie vorig hoofdstuk).

Aldus dient er eveneens rekening gehouden te worden met bepaalde formaatvereisten – i.c. deze voor de LEI-code en voor de datum- en tijdsaanduiding (volgens ISO8601 – zie ① in Figuur 15: scherm Significant Cyber Threats). Deze vormvereisten zijn dezelfde als deze die al werden uitgelegd in het vorige deel van dit document (zie ook ② in Figuur 12: scherm luik "Notification" - deel 1). In geval er niet aan de vormvereisten wordt voldaan, zal een foutmelding verschijnen in het veld zelf. U dient deze eerst te verbeteren alvorens u verder kan gaan met het valideren en indienen van de survey. Zie voor nadere uitleg eveneens hierboven.

5. De DORA_INCIDENT- en DORA_CYBERTHREAT surveys indienen

- Zodra u alle gegevens correct heeft ingevuld zal het mogelijk zijn deze te valideren en te bewaren () en zo verder te gaan () naar een volgende sectie (zie ④ in Figuur 12: scherm luik "notification" - deel 1 of ② in Figuur 15: scherm "Significant Cyber Threats").
- In geval van fouten bij het invullen zullen deze verschijnen in het "Validation report". U dient deze eerst te verbeteren (zie hoofdstuk V.6. Validation report: errors en warnings).

- De verplichte velden bij de kennisgeving van een ernstig ICT-incident zijn afhankelijk van de fase van het kennisgevingsproces waarvoor u de survey wenst in te dienen. Verplichte velden bij het tussentijdse verslag of eindverslag zullen geen “error” veroorzaken bij het indienen van een survey voor een eerste kennisgeving.
- Wanneer u na het verbeteren van de aangegeven “errors” de survey definitief heeft kunnen valideren () kan u de survey indienen. Dit doet u door links op het scherm op  te klikken.
- Een pop-up scherm (zie figuur 16) zal verschijnen waarbij u uitgelegd wordt dat de survey “read only” zal worden en er bijgevolg dus geen wijzigingen meer aangebracht kunnen worden.



Figuur 16: boodschap bij het indienen van de survey

6. Validation report: errors en warnings

In geval u bepaalde velden niet of incorrect heeft ingevuld, zal FiMiS u dit aangeven in het validatierapport dat verschijnt in de linkerbovenhoek van het scherm van de survey wanneer u de ingegeven informatie wil valideren en bewaren (zie figuur 17: “Validation report”).



Figuur 17: Validation report

U kan de details van dit rapport consulteren door op de blauwe pijl naast “Validation report” te klikken (zie rode cirkel in figuur 17: “Validation report”). Twee types van problemen bij de ingevoerde gegevens kunnen aangegeven worden:

- **Errors:** deze betreffen verplichte velden die niet of incorrect werden ingevuld. Errors zijn blokkerend voor het effectief indienen van de kennisgeving en dienen dus verbeterd te worden.
- **Warnings:** deze betreffen niet of incorrect ingevulde velden die niet blokkerend zijn voor het effectief indienen van de kennisgeving.

Bij de DORA_INCIDENT-survey zullen beide types van problemen verschillen afhankelijk van de fase van de kennisgeving waarvoor u de survey indient. Bij het eindverslag zijn bijvoorbeeld veel meer gegevens vereist

dan bij de eerste kennisgeving.

De aangegeven errors en warnings zijn in lijn met de validatieregels zoals bepaald door de ESAs. U kan deze regels ook consulteren in Bijlage 1: lijst van in te vullen velden DORA_INCIDENT-survey in de laatste drie kolommen:

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

Voor de kennisgeving van een cyberdreiging zijn de errors en warnings opgenomen in de survey in lijn met de validatieregels zoals bepaald door de ESAs. U kan deze consulteren in de laatste kolom ("Mandatory field") van Bijlage 2: lijst van in te vullen velden DORA_CYBERTHREAT-survey.

Bijlage 1: lijst van in te vullen velden DORA_INCIDENT-survey



DORA Incident
reporting Template

Bron:

In afwachting van de definitieve publicatie van de betrokken ITS, is deze lijst enkel beschikbaar in het Engels.

Field Code	Field Name	Description	Field Type	Mandatory for initial notification	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. +33XXXXXXXX)	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. +33XXXXXXXX)	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>	Choice (multiple) populated by using ISO 3166 ALPHA-2 of the affected countries	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	Indication of how the major ICT-related incident has been discovered.	<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	Information about affected functional areas and business processes	<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

Bijlage 2: lijst van in te vullen velden DORA_CYBERTHREAT-survey



DORA significant
cyber threats Template

Bron:

In afwachting van de definitieve publicatie van de betrokken ITS, bestaat deze lijst enkel in het Engels.

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.

