РЕПУБЛИКА БЪЛГАРИЯ

КОМИСИЯ ЗА ФИНАНСОВ НАДЗОР

РЪКОВОДСТВО
ЗА ДОКЛАДВАНЕ НА СЪЩЕСТВЕНИ ИНЦИДЕНТИ С ИКТ И ЗНАЧИТЕЛНИ КИБЕРЗАПЛАХИ ДО КОМИСИЯТА ЗА ФИНАНСОВ НАДЗОР

(утвърдено със Заповед № З-127/29.05.2025 г. на председателя на Комисията за финансов надзор)

КФН КОМИСИЯ ЗА ФИНАНСОВ НАДЗОР

СЪДЪРЖАНИЕ

1. Речник на термините и съкращения

Термин	*Описание*
КФН	Комисия за финансов надзор
DORA	Digital Operational Resilience Act - Регламент (ЕС) 2022/2554 за цифрова и оперативна устойчивост
ИКТ	Информационни и комуникационни технологии
LEI	Legal Entity Identifier (LEI код)
Образци за докладване	Основни образци за докладване на инциденти, свързани с ИКТ и уведомяване за значителни киберзаплахи до Комисията за финансов надзор

2. Цел

Това ръководство цели да разясни задължението за докладване на съществени инциденти, както и доброволното уведомяване за значителни киберзаплахи, и се отнася до финансови субекти по смисъла на чл. 2, параграф 1 от Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14 декември 2022 година относно оперативната устойчивост на цифровите технологии във финансовия сектор и за изменение на регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014, (ЕС) № 909/2014 и (ЕС) 2016/1011 (DORA), които са поднадзорни на Комисията за финансов надзор лица.

3. Обща информация

При подаване на доклад до Комисията за финансов надзор, свързан със съществени инциденти с ИКТ или уведомление за значителни киберзаплахи, е препоръчително да следвате предоставената в това ръководство информация.

Подаването на доклади за съществени инциденти с ИКТ се извършва по образец. Образецът на доклад за съществени инциденти с ИКТ може да намерите **тук**.

Всички задължителни полета в образеца на доклад трябва да бъдат попълнени. При попълване на образеца неговата структура и форматиране не трябва да бъдат променяни.

Наименованието на докладите трябва да е съгласно конвенцията за именуване. Информация за конвенцията за именуване може да намерите **тук**.

Образец на уведомление за значителни киберзаплахи може да намерите **тук**.

Наименованието на уведомлението за значителни киберзаплахи трябва да е съгласно конвенцията за именуване. Информация за конвенцията за именуване може да намерите **тук**.

Типът на подаване (първоначално уведомление, неокончателен доклад, окончателен доклад или съществен инцидент, прекласифициран като несъществен) се избира в поле 1.1 на образеца за докладване на инциденти и съответства на типа на доклада.

Финансовите субекти трябва да подават докладите за инциденти и уведомленията за значителни киберзаплахи до Комисията за финансов надзор чрез защитен канал на имейл ict_contact_point@fsc.bg.

Докладите и уведомленията се изпращат чрез защитен канал, като се използва криптиране.

Инструкцията за криптиране може да намерите **тук**.

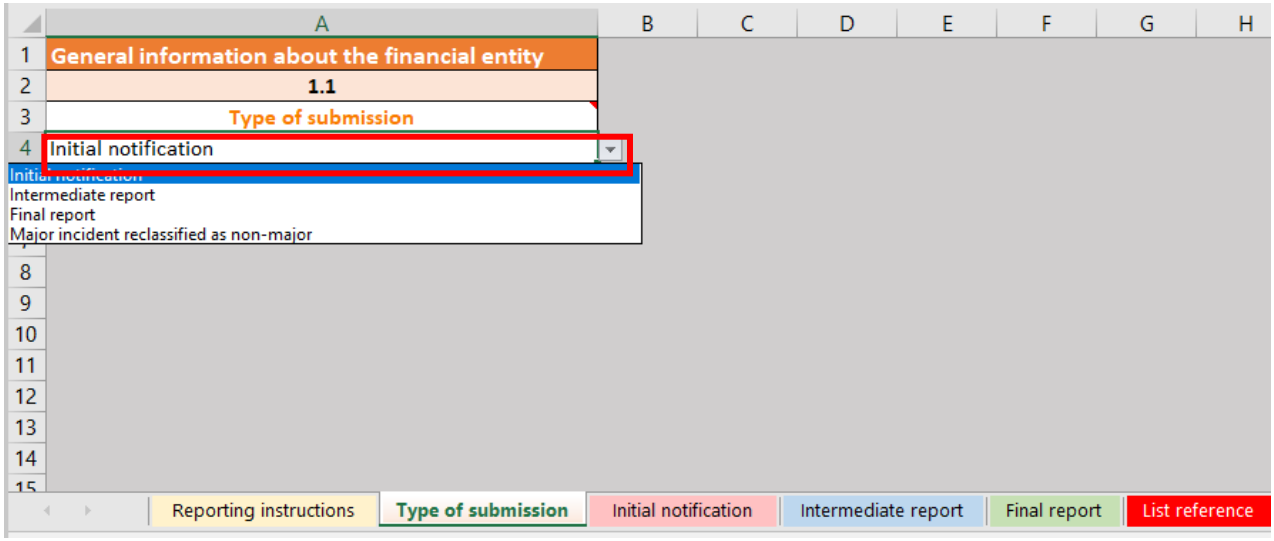
Публичният ключ на Комисията за финансов надзор за криптиране може да изтеглите **тук**.

4. Докладване на съществени инциденти, свързани с ИКТ

4.1. Как да подадете първоначално уведомление по DORA, относно съществен инцидент с ИКТ

4.1.1. Попълване на образеца за докладване на инцидент

Уверете се, че в поле 1.1 от образеца за докладване на съществен инцидент избраният тип подаване е „Първоначално уведомление“.



Уверете се, че всички задължителни полета за първоначалното уведомление са попълнени в образеца за докладване и че името на същото се придържа към конвенцията за именуване (вижте раздел 7).

4.1.2. Подаване на първоначално уведомление

Подайте първоначалното уведомление до КФН чрез защитен канал на имейл: ict_contact_point@fsc.bg

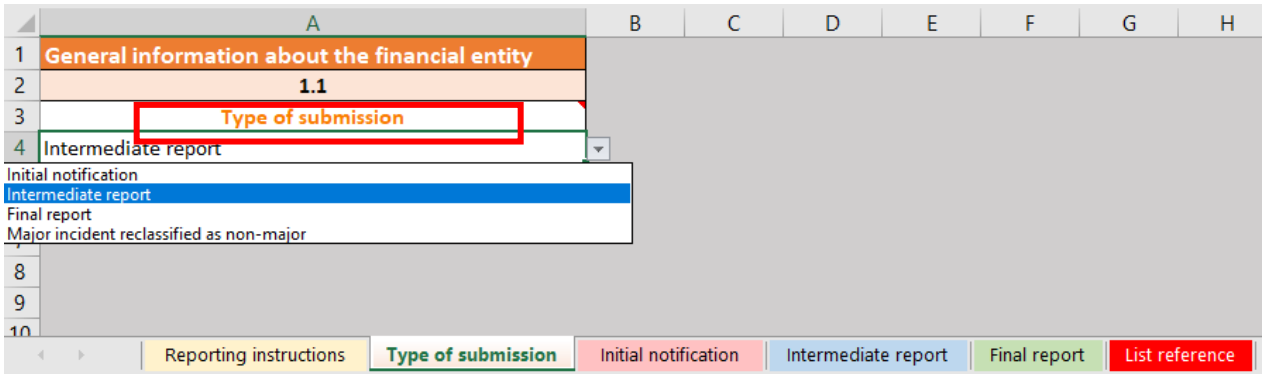
4.1.3. Референтен код на инцидента

След подаване на доклад ще получите референтен код на инцидента.

4.2. Как да подадете неокончателен доклад по DORA, свързан със съществен инцидент с ИКТ

4.2.1. Попълване на образеца за докладване на инцидент

Уверете се, че в поле 1.1 от образеца за докладване на съществен инцидент избраният тип подаване е „Неокончателен доклад“.



Попълнете съответния референтен код на инцидент в поле 3.1 на образеца за докладване.

Уверете се, че всички задължителни полета за неокончателния доклад са попълнени в образеца за докладване и че името на същия се придържа към конвенцията за именуване.

Уверете се, че информацията, подадена при първоначалното уведомление, е налична в попълнения образец с неокончателния доклад.

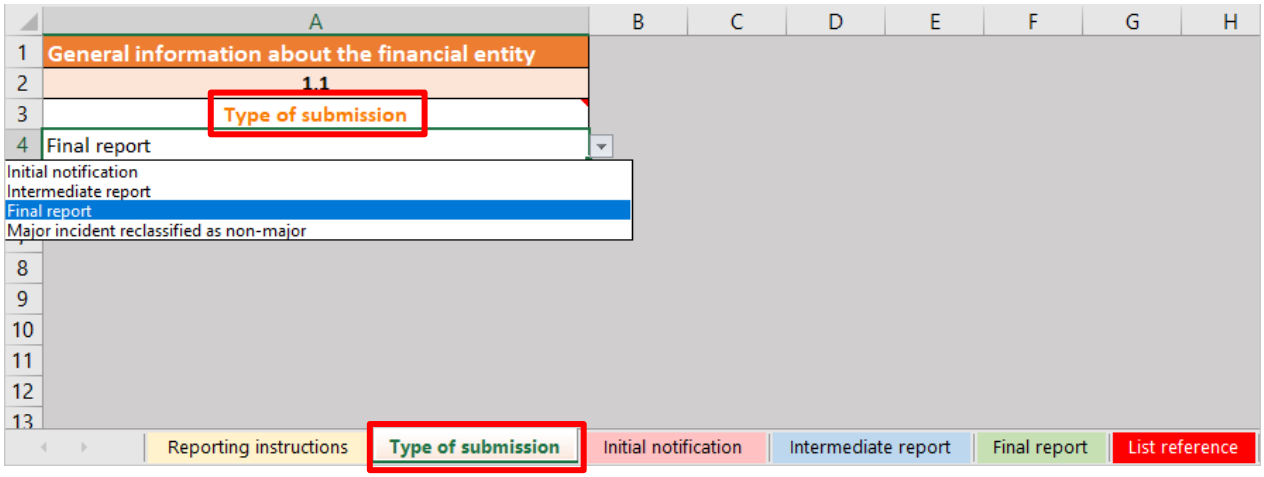
4.2.2. Подаване на неокончателен доклад

Подайте неокончателния доклад до КФН чрез защитен канал на имейл: ict_contact_point@fsc.bg

4.3. Как да подадете окончателен доклад по DORA, свързан със съществени инциденти с ИКТ

4.3.1. Попълване на образеца за докладване на инцидент

Уверете се, че в поле 1.1 от образеца за докладване на съществен инцидент избраният тип подаване е „Окончателен доклад“.



Уверете се, че всички задължителни полета за окончателния доклад са попълнени в образеца за докладване и че името на същия се придържа към конвенцията за именуване.

Уверете се, че информацията, подадена в неокончателния доклад, присъства и в окончателния доклад.

4.3.2. Подаване на окончателен доклад

Подайте окончателен доклад до КФН чрез защитен канал на имейл:

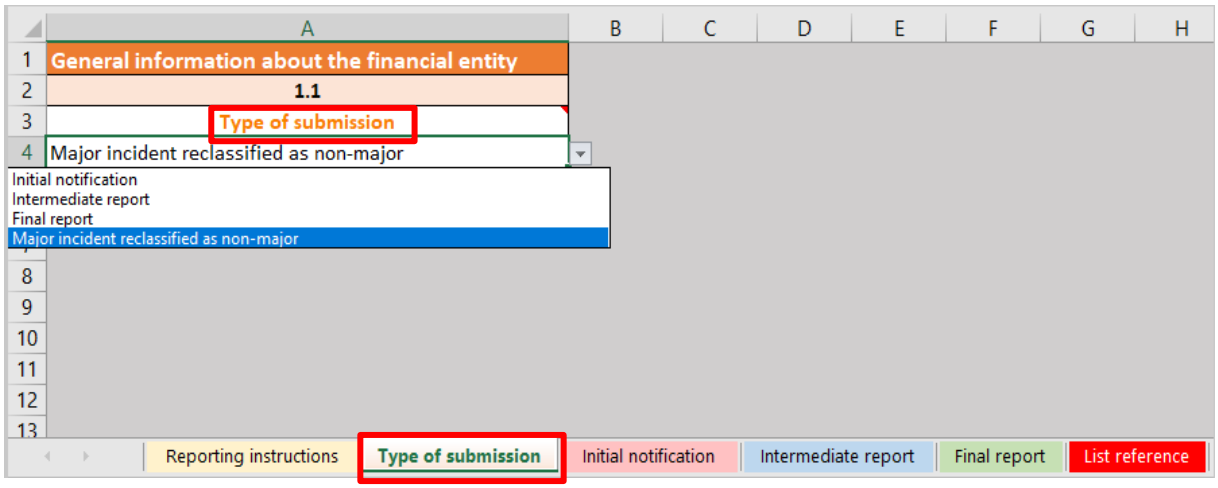
ict_contact_point@fsc.bg

5. Как да прекласифицирате съществен инцидент като несъществен

5.1. Попълване на образеца на докла за преквалифициране на съществен инцидент като несъществен

Когато докладът за съществен инцидент е успешно подаден, но при допълнителна оценка от страна на засегнатия финансов субект е установено, че инцидентът, докладван като съществен, към момента на класифицирането му не е изпълнил изискваните критерии за класификация и праговете за същественост, финансовият субект подава доклад за съществен инцидент, прекласифициран като несъществен инцидент.

Уверете се, че в поле 1.1 от образеца за докладване на съществен инцидент избраният тип подаване е „Съществен инцидент, прекласифициран като несъществен“.



Уверете се, че всички задължителни в доклада за съществен инцидент, прекласифициран като несъществен инцидент, са попълнени в образеца за докладване.

5.1.1. Подаване на доклад за прекласифициране на съществен инцидент като несъществен

Подайте доклад за прекласифициране на съществен инцидент като несъществен инцидент до КФН чрез защитен канал на имейл:

ict_contact_point@fsc.bg

6. Подаване на доклад за съществен инцидент с ИКТ, когато има два или повече отделни инцидента в един и същи ден

При възникване на друг, отделен инцидент в същия финансов субект, в рамките на същия ден, в който вече е подаден доклад, и който не е свързан с първия инцидент, се подава нов доклад, като в наименованието нотацията „n“ ще бъде 2, напр. XXXXXX_20250620_DIR_2.xlsx.

7. Конвенция на именуване на файла

Докладите и уведомленията трябва да се придържат към следната конвенция за именуване:

XXXXXX_YYYYMMDD_DIR_n.xlsx(zip)

където:

XXXXXX – е LEI кодът на финансовия субект.

YYYYMMDD – е датата на инцидента.

DIR – е кодът за идентифициране на доклади за съществени инциденти по DORA.

n – е цифровият идентификатор за инцидента, който се докладва за съответния ден. Първият докладван инцидент за деня трябва да използва 1. Това позволява да се докладва повече от един инцидент, когато такъв инцидент се случи на същата дата като друг докладван инцидент.

xlsx(zip) – е файловото разширение (.xlsx или .zip).

8. Докладване за значителни киберзаплахи

8.1. Попълване образеца на уведомление за значителни киберзаплахи

Свалете образеца за уведомления за значителни киберзаплахи.

Уверете се, че всички задължителни полета са попълнени в образеца, както и че името на файла се придържа към конвенцията за именуване.

8.2. Подаване на уведомление за значителни киберзаплахи

Подайте уведомление за значителни киберзаплахи до КФН чрез защитен канал на имейл: ict_contact_point@fsc.bg

8.3. Конвенция за наименуване на файла

Уведомлението трябва да се придържа към следната конвенция за именуване:

XXXXXX_YYYYMMDD_DCT_n.xlsx(zip)

където

XXXXXX – е LEI кодът на финансовия субект.

YYYYMMDD – е датата на киберзаплахата.

DCT – е кодът за идентифициране за уведомления за значителни киберзаплахи по DORA.

n – е цифровият идентификатор за киберзаплахата, която се докладва за съответния ден. Първата докладвана киберзаплаха за деня трябва да бъде номерирана 1. Това позволява да се докладва повече от една киберзаплаха на ден.

xlsx(zip) – е файловото разширение (.xlsx или .zip).

9. Въпроси и съдействие

При необходимост от съдействие относно докладването може да се обръщате към ИКТ звеното за контакт на Комисията за финансов надзор на тел. 0882 88 94 92.