К О М И С И Я З А Ф И Н А Н С О В Н А Д З О Р

ИНФОРМАЦИЯ ПО ПРИЛАГАНЕТО НА РЕГЛАМЕНТ (ЕС) 2022/2554 (DORA) ОТНОСНО ОПЕРАТИВНАТА УСТОЙЧИВОСТ НА ЦИФРОВИТЕ ТЕХНОЛОГИИ ВЪВ ФИНАНСОВИЯ СЕКТОР

Комисията за финансов надзор предоставя следната информация относно задълженията на субектите от небанковия финансов сектор в Република България и поднадзорни на Комисията за финансов надзор лица, произтичащи от Регламент (ЕС) 2022/2554[1].

Като част от законодателния пакет на Европейския съюз, ориентиран към цифровите финанси, който има за задача да насърчи технологичното развитие и да осигури финансова стабилност и защита на потребителите, Регламент (ЕС) 2022/2554 цели консолидиране и подобряване на изискванията във връзка с риска в областта на информационните и комуникационни технологии (ИКТ), както и осигуряване на оперативна устойчивост в сектора на финансовите услуги. За постигане на високо общо равнище на оперативна устойчивост на цифровите технологии, устойчивост на кибератаки и други инциденти, свързани с ИКТ, Регламент (ЕС) 2022/2554 установява единни изисквания за сигурността на мрежовите и информационни системи, които финансовите субекти е необходимо да спазват при извършване на своята дейност. Регламент (ЕС) 2022/2554 съдържа пет основни стълба, изграждащи рамка на оперативната устойчивост за финансовите субекти. Въвеждат се изисквания към финансовите субекти за управление на риска при ИКТ, изисквания за докладване на компетентния орган за съществени инциденти с ИКТ, както и уведомяване на доброволни начала за значителни киберзаплахи, изисквания за тестване на оперативната устойчивост на цифровите технологии, изисквания за стабилно управление на риска в областта на ИКТ, пораждан от трети страни и правила за сътрудничество.

Поднадзорните на Комисията за финансов надзор лица е необходимо да осигурят адекватна способност за защита и непрекъснатост на услугите, които предоставят като изпълнят задълженията си, произтичащи от Регламент (ЕС) 2022/2554 в срок до 17.01.2025 г. Регламент (ЕС) 2022/2554 се прилага ефективно от 18.01.2025 г.

---

[1] 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

Обхват

За да се осигури устойчивост срещу риска в областта на ИКТ в целия сектор на финансовите услуги, Регламент (ЕС) 2022/2554 се прилага за широк кръг от финансови субекти, както и за трети страни доставчици на услуги в областта на ИКТ. Компетентен орган по отношение на финансовите субекти от небанковия финансов сектор е Комисията за финансов надзор. На основание чл. 2, параграф 1 от Регламент (ЕС) 2022/2554 настоящата информация е насочена към следните поднадзорни на Комисията за финансов надзор лица, наричани по-долу „финансови субекти“:

1. Инвестиционните посредници, получили лиценз при условията и по реда на Закона за пазарите на финансови инструменти;

2. Доставчиците на услуги за криптоактиви, лицензирани от Комисията за финансов надзор[2] съгласно Регламент (ЕС) 2023/1114[3], ако Комисията за финансов надзор бъде определена за компетентен орган по същия регламент;

3. Издателите на токени, обезпечени с активи, лицензирани от Комисията за финансов надзор[4] съгласно Регламент (ЕС) 2023/1114;

4. Централните депозитари на ценни книжа по чл. 1, т. 5 от Закона за пазарите на финансови инструменти;

5. Централните контрагенти по чл. 1, т. 6 от Закона за пазарите на финансови инструменти;

6. Местата за търговия, получили лиценз при условията и по реда на Закона за пазарите на финансови инструменти;

7. Лицата, управляващи алтернативни инвестиционни фондове, с изключение на лицата, които управляват пряко или непряко алтернативни инвестиционни фондове, стойността на чиито активи в съвкупност не надхвърля стойностите, посочени в чл. 197, ал. 1, т. 1 и 2 от Закона за дейността на колективните инвестиционни схеми и на други предприятия за колективно инвестиране;

8. Управляващите дружества, получили лиценз при условията и по реда на Закона за дейността на колективните инвестиционни схеми и на други предприятия за колективно

---

[2] Със законопроекта за пазарите на криптоактиви, публикуван за обществени консултации на адрес: https://www.strategy.bg/publicconsultations/View.aspx?lang=bg-BG&Id=8517, се предлага Комисията за финансов надзор да бъде определена за компетентен орган за посочените лица;

[3] Регламент (ЕС) 2023/1114 на Европейския парламент и на Съвета от 31 май 2023 година относно пазарите на криптоактиви и за изменение на регламенти (ЕС) № 1093/2010 и (ЕС) № 1095/2010 и на директиви 2013/36/ЕС и (ЕС) 2019/1937;

[4] Със законопроекта за пазарите на криптоактиви, публикуван за обществени консултации на адрес: https://www.strategy.bg/publicconsultations/View.aspx?lang=bg-BG&Id=8517, се предлага Комисията за финансов надзор да бъде определена за компетентен орган за посочените лица

инвестиране;

9. Одобрените механизми за докладване и одобрените механизми за публикуване по чл. 1, т. 3 от Закона за пазарите на финансови инструменти;

10. Доставчиците на услуги за колективно финансиране по чл. 1, ал. 1, т. 5 от Закона за публичното предлагане на ценни книжа;

11. Администраторите на критични бенчмаркове по чл. 1, т. 7 от Закона за пазарите на финансови инструменти;

12. Застрахователните и презастрахователните предприятия, получили лиценз при условията и по реда на Кодекса за застраховането, с изключение на застрахователи без право на достъп до единния пазар по чл. 16 от Кодекса за застраховането;

13. Застрахователните посредници, презастрахователните посредници и посредниците, предлагащи застрахователни продукти като допълнителна дейност, които не са микро-, малки или средни предприятия, и са получили лиценз при условията и по реда на Кодекса за застраховането;

14. Пенсионноосигурителните дружества, получили лиценз при условията и по реда на Кодекса за социално осигуряване, които управляват фонд за допълнително доброволно пенсионно осигуряване по професионални схеми с повече от 15 осигурени лица.

Изисквания към финансовите субекти

I. Изисквания към финансовите субекти във връзка с управление на риска при ИКТ

С цел изпълнение на задълженията, установени с Регламент (ЕС) 2022/2554, финансовите субекти е необходимо да предприемат мерки във връзка с риска в областта на ИКТ, като отчетат размера и цялостния си рисков профил, естеството, мащаба и сложността на своите услуги, дейности и операции.

1. Установяване на рамка за управление на риска в областта на ИКТ

1.1. Финансовите субекти е необходимо да изградят рамка за управление на риска при ИКТ, която обхваща всички нива в управленската структура на съответното лице и включва следните елементи на информационната сигурност:

а) оценка и управление на риска;

б) управление на персонала;

в) физическа сигурност;

г) контрол на достъпа;

д) сигурност при избора (процес за оценка и одобрение на нови технологии и услуги);

е) планове и действия в извънредни ситуации и кризи.

1.2. Рамката за управление на риска при ИКТ трябва да осигурява възможности за идентифициране, защита, реакция и възстановяване на нормалното функциониране на ИКТ системите при възникване на инцидент.

1.3. Рамката за управление на риска при ИКТ е необходимо да съдържа:

а) стратегия за оперативна устойчивост на цифровите технологии съгласно чл. 6, параграф 8 от Регламент (ЕС) 2022/2554, а по преценка на финансовия субект и цялостна стратегия за прибягване до множество доставчици на ИКТ на равнище група или субект съгласно чл. 6, параграф 9 от същия регламент;

б) идентификация, класификация и процедури за подходящо документиране на всички поддържани от ИКТ работни функции, роли, отговорности и другите елементи съгласно предвиденото в чл. 8, параграф 1 от Регламент (ЕС) 2022/2554;

в) политики, процедури, протоколи и инструменти за сигурност на ИКТ, съгласно чл. 9, параграфи 2 и 4 от Регламент (ЕС) 2022/2554, които са в съответствие с допълнителните изисквания по дял II, глава I и II на Делегиран регламент (ЕС) 2024/1774[5];

г) политика за непрекъснатост на дейността на ИКТ съгласно чл. 11, параграфи 2 – 4 от Регламент (ЕС) 2022/2554, състояща се най-малко от предвидените в чл. 24 и 26 от Делегиран регламент (ЕС) 2024/1774 компоненти;

д) политики и процедури за съхраняване на резервни копия на данните съгласно чл. 12, параграф 1, буква „а“ от Регламент (ЕС) 2022/2554;

е) процедури и методи за възстановяване на информацията съгласно чл. 12, параграф 1, буква „б“ от Регламент (ЕС) 2022/2554;

ж) план за комуникация с клиенти и контрагенти при криза, включително и с обществеността, както и комуникационни политики за собствения си персонал и външни заинтересовани страни съгласно чл. 14, параграфи 1 и 2 от Регламент (ЕС) 2022/2554;

з) програма за тестване на оперативната устойчивост на ИКТ.

2. Извършване на преглед на установената рамка за управление на риска в областта на ИКТ

[5] Делегиран регламент (ЕС) 2024/1774 на Комисията от 13 март 2024 година за допълнение на Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета във връзка с регулаторните технически стандарти за определяне на инструментите, методите, процесите и политиките за управление на риска в областта на ИКТ и опростената рамка за управление на риска в областта на ИКТ

Финансовите субекти е необходимо да предвидят процедура, съгласно която рамката за управление на риска в областта на ИКТ и част от нейните елементи периодично или при възникване на определени предпоставки да подлежат на преглед и актуализация както следва:

а) рамката за управление на риска се документира и преразглежда най-малко веднъж годишно, а за финансовите субекти - микропредприятия (финансови субекти, различни от място на търговия, централен контрагент, регистър на трансакции или централен депозитар на ценни книжа, които имат под 10 служители и чиито годишен оборот и/или общо активи в годишния счетоводен баланс не надхвърля 2 милиона евро съгласно чл. 3, т. 60 от Регламент (ЕС) 2022/2554) периодично, както и при съществени инциденти с ИКТ;

б) финансовите субекти извършват при необходимост преглед на адекватността на процесите по идентификация, класификация и процедурите за документиране на всички поддържани ИКТ работни функции, роли, информационни активи и активите на ИКТ, но не по-малко от веднъж годишно;

в) финансовите субекти извършват преглед на политиката си за непрекъснатост на дейността на ИКТ и на плановете си за реакция и възстановяване на ИКТ съгласно чл. 11, параграф 6, ал. 3 от Регламент (ЕС) 2022/2554;

г) финансовите субекти извършват преглед на възникналите инциденти с ИКТ при прекъсване на дейността им от съществен инцидент с ИКТ съгласно чл. 13, параграф 2 от Регламент (ЕС) 2022/2554.

При поискване от Комисията за финансов надзор финансовите субекти, без финансовите субекти - микропредприятия, извършват уведомяване за промените, които са били предприети след посочения в буква „г“ преглед на възникналите инциденти с ИКТ съгласно чл. 13, параграф 2, ал. 2 от Регламент (ЕС) 2022/2554.

3. Извършване на периодични тестове

Елементите от рамката за управление на ИКТ риска, които подлежат на периодични тестове, включително при спазване на изискванията съгласно чл. 25 от Делегиран регламент (ЕС) 2024/1774, са:

а) плановете за непрекъснатост на дейността и плановете за реакция, и възстановяване на ИКТ съгласно чл. 11, параграф 4 и параграф 6, буква „а“ от Регламент (ЕС) 2022/2554;

б) плановете за комуникация при криза съгласно чл. 11, параграф 6, буква „б“ във връзка с чл. 14 от Регламент (ЕС) 2022/2554;

в) процедурите за съхраняване на резервни копия и процедурите, и методите за възстановяване на информацията съгласно чл. 12, параграф 2 от Регламент (ЕС) 2022/2554.

По отношение на плановете за непрекъснатост на дейността на ИКТ и плановете реакция и възстановяване на ИКТ тестването се извършва не по-малко от веднъж годишно, както и при съществени промени в системите на ИКТ, които поддържат критични или важни функции.

4. Изисквания към организационната структура

4.1. Лицата, които управляват и/или представляват финансовите субекти, носят отговорност за управлението на риска в областта на ИКТ и за изпълнението на всички действия във връзка с рамката за управление на риска в ИКТ. Във връзка с това ръководния орган на финансовия субект е задължен да:

а) въведе политики, които осигуряват поддържането на високи стандарти за наличността, автентичността, целостта и поверителността на данните;

б) определи ясни роли и отговорности за всички длъжности в организацията, свързани с ИКТ и правилата за осигуряване ефективна и навременна комуникация, сътрудничество и координация между тези длъжности;

в) приеме стратегия за оперативна устойчивост на цифровите технологии на финансовия субект;

г) определи нивото на толерантност към риска в областта на ИКТ за финансовия субект;

д) одобри, контролира и извършва преглед на изпълнението на политиката на финансовия субект за непрекъснатост на дейността на ИКТ, плановете за реакция и възстановяване на ИКТ;

е) одобри и извършва периодично преглед на плановете за извършване на вътрешен одит на ИКТ, на одитите на ИКТ и на съществените промени в тях;

ж) осигури и разпредели необходимия бюджет, свързан с изискванията за осигуряване на оперативната устойчивост на цифровите технологии, включително за програмите за повишаване на осведомеността, за сигурността на ИКТ и обученията на служителите за оперативна устойчивост на цифровите технологии;

з) одобри и извършва периодично преглед на политиката на финансовия субект относно споразуменията за използването на услуги в областта на ИКТ, предоставяни от трети страни, доставчици на такива услуги;

и) въведе канали за докладване на корпоративно ниво по отношение на споразуменията, сключени с трети страни доставчици на услуги в областта на ИКТ, използването на такива услуги, планираните съществени промени по отношение на

третите страни, доставчици на услуги в областта на ИКТ, и отражението им върху критичните или важни функции на ИКТ.

4.2. В зависимост от естеството, мащаба, сложността и нивото на риск в областта на ИКТ, както и действащата организационна структура, управителните органи на финансовите субекти е необходимо да обезпечат създаването или обособяването на най-малко на следните функции:

а) контролна функция за управление и надзор на риска в областта на ИКТ съгласно чл. 6, параграф 4 от Регламент (ЕС) 2022/2554;

б) одиторска функция, свързана с извършване на регулярен вътрешен одит на рамката за управление на риска в областта на ИКТ съгласно чл. 6, параграф 6 от Регламент (ЕС) 2022/2554;

в) функция за осъществяване на наблюдение върху сключените договори с трети страни доставчици на услуги в областта на ИКТ съгласно чл. 5, параграф 3 от Регламент (ЕС) 2022/2554, ако не е възложено на член на висшето ръководство на финансовия субект да упражнява такъв надзор;

г) функция за управление на кризи съгласно чл. 11, параграф 7 от Регламент (ЕС) 2022/2554;

д) функция за връзки с обществеността и медиите съгласно чл. 13, параграф 3 от Регламент (ЕС) 2022/2554.

Съвместяването на определените по-горе функции с други функции в рамките на финансовия субект може да е приемливо, ако същото не поражда конфликти на интереси, не застрашава ефективното изпълнение на задълженията и служителят отделя достатъчно време за изпълнение на функциите.

Одиторската функция не може да бъде съвместявана с други контролни функции в рамките на финансовия субект.

5. Изисквания за обучения

5.1. Финансовите субекти трябва да разполагат с необходимия оперативен капацитет и персонал за събиране на информация за уязвими места, киберзаплахи и инциденти с ИКТ, в това число кибератаки и извършване на анализ на въздействието им върху оперативната устойчивост на използваните цифрови технологии.

5.2. Членовете на управителните органи на финансовите субекти е необходимо да притежават и поддържат необходимите знания и умения с оглед извършването на адекватна оценка на рисковете в областта на ИКТ и тяхното въздействие върху дейността на финансовите субекти.

Необходимо е финансовите субекти да включат в плановете за обучение на служителите задължителни модули за повишаване на осведомеността за сигурността на ИКТ и обучения за оперативна устойчивост на цифровите технологии. Тези обучения следва да се провеждат на членовете на управителните органи и всички служители в организацията, като нивото на сложност на отделните модули се съобразява със спецификите на длъжностите и обхвата на техните функции. По преценка на управителните органи на финансовия субект в обученията могат да бъдат включени и трети страни, доставчици на ИКТ, с които финансовия субект има сключени договори.

6. Пропорционално приложение спрямо финансови субекти - микропредприятия

Финансовите субекти – микропредприятия могат да не прилагат изискванията на чл. 5, параграф 3, чл. 6, параграф 4 и 6, чл. 8, параграф 3 и 7, чл. 11, параграфи 3, 7 и 10, чл. 12, параграф 4 и чл. 13, параграф 7 от Регламент (ЕС) 2022/2554, както и други изисквания, когато е изрично посочено.

7. Опростена рамка за управление на риска

7.1. На основание чл. 16, параграф 1 от Регламент (ЕС) 2022/2554 следните финансови субекти прилагат опростена рамка за управление на риска в областта на ИКТ:

а) малки и невзаимосвързани инвестиционни посредници по чл. 12, параграф 1 от Регламент (ЕС) 2019/2033[6];

б) институции за професионално пенсионно осигуряване, които управляват пенсионни схеми, в които участват общо по-малко от 100 членове.

Спрямо тези финансови субекти са въведени изисквания да създадат документирана рамка за управление на риска в областта на ИКТ, която съдържа общи, всеобхватни насоки и правила, насочени към запазване на наличността, целостта и поверителността на данните.

7.2. Опростената рамка за управление на риска в областта на ИКТ подлежи на периодичен преглед и актуализация при възникване на съществени инциденти с ИКТ и указания от надзорния орган.

7.3. Допълнителните изисквания относно елементите на опростената рамка за управление на ИКТ рискове са уредени в дял III на Делегиран регламент (ЕС) 2024/1774.

[6] Регламент (ЕС) 2019/2033 на Европейския парламент и на Съвета от 27 ноември 2019 година относно пруденциалните изисквания за инвестиционните посредници и за изменение на регламенти (ЕС) № 1093/2010, (ЕС) № 575/2013, (ЕС) № 600/2014 и (ЕС) № 806/2014

II. Изисквания към финансовите субекти във връзка с докладването пред компетентните органи за съществени инциденти с ИКТ и уведомяването им на доброволни начала за значителни киберзаплахи

1. Управление на инциденти

Финансовият субект разработва процес за управление на инциденти, свързани с ИКТ съгласно чл. 17 от Регламент (ЕС) 2022/2554. Процесът за управление на инциденти, свързани с ИКТ е необходимо да позволява на финансовият субект да:

а) определя, въвежда и прилага мерки за откриване, управление, документиране и съобщаване на инциденти в областта на ИКТ съгласно чл. 17, параграф 1 от Регламент (ЕС) 2022/2554;

б) класифицира инцидентите с ИКТ и определя тяхното въздействие съгласно чл. 18 от Регламент (ЕС) 2022/2554, като използва за критерии броя и/или значимостта на клиентите или финансовите контрагенти, засегнати от инцидента, продължителността и географския обхват на инцидента, загубата на данни в резултат на инцидента, критичната значимост на засегнатите услуги и икономическите последици, произтекли от инцидента;

в) докладва за съществени инциденти, свързани с ИКТ, на Комисията за финансов надзор съгласно чл. 19 от Регламент (ЕС) 2022/2554, като съдържанието на докладите за съществени инциденти с ИКТ и на уведомлението за значителни киберзаплахи е предвидено да бъде определено с регулаторни технически стандарти по чл. 20, параграф 1 от Регламент (ЕС) 2022/2554.

2. Класифициране на инциденти с ИКТ и киберзаплахи

2.1. Финансовите субекти документират всички инциденти с ИКТ и значителни киберзаплахи с цел последователно и интегрирано наблюдение, реакция и проследяване на инцидентите с ИКТ, преодоляване на причините за проявлението им и превенция срещу повторната им поява.

2.2. При възникване на инцидент с ИКТ е необходимо финансовите субекти да го класифицират и определят въздействието му при спазване на критериите по чл. 18, параграф 1 от Регламент (ЕС) 2022/2554 и глава първа от Делегиран регламент (ЕС) 2024/1772[7].

[7] Делегиран регламент (ЕС) 2024/1772 на Комисията от 13 март 2024 година за допълнение на Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета по отношение на регулаторните технически стандарти, с които се определят подробно критериите за класифициране на инциденти с ИКТ и киберзаплахи, праговете на същественост и информацията в докладите за съществени инциденти

2.3 Финансовите субекти класифицират киберзаплахите като значими при спазване на критериите по чл. 18, параграф 2 от Регламент (ЕС) 2022/2554 и глава трета от Делегиран регламент (ЕС) 2024/1772.

3. Докладване за съществени инциденти с ИКТ

3.1. При настъпване на съществен инцидент с ИКТ финансовите субекти е необходимо да уведомят ИКТ звеното за контакт на Комисията за финансов надзор на имейл: ict_contact_point@fsc.bg. Възникнал инцидент се счита за съществен инцидент, когато е засегнал критични услуги и са достигнати праговете на същественост, съгласно чл. 9 от Делегиран регламент (ЕС) 2024/1772.

3.2. С Делегиран регламент (ЕС) 2024/1772 се определят и правилата относно повтарящи се инциденти – такива инциденти, които поотделно не са съществени, но в съвкупност следва да бъдат разгледани като съществен инцидент, когато отговарят на изискванията, посочени в чл. 8, параграф 2 от същия регламент. Финансовите субекти оценяват наличието на повтарящи се инциденти на месечна основа.

3.3. Финансовите субекти предоставят на Комисията за финансов надзор в съответствие с регулаторните технически стандарти по чл. 20, параграф 1 от Регламент (ЕС) 2022/2554:

а) първоначално уведомление;

б) неокончателен (междинен) доклад;

в) окончателен доклад.

Първоначално уведомление

Финансовите субекти класифицират инцидента своевременно и без ненужно забавяне, но не по-късно от 24 часа след установяването му.

При възникване на ИКТ инцидент, който е класифициран като съществен, финансовите субекти следва да подадат ранно предупреждение без ненужно забавяне, при всички положения в рамките на 24 часа до ИКТ звеното за контакт.

Когато инцидент с ИКТ е класифициран като съществен, финансовите субекти подават първоначален доклад до ИКТ звеното за контакт.

ИКТ звеното за контакт своевременно потвърждава получаването на първоначалния доклад от финансовия субект за съществен инцидент с ИКТ.

ИКТ звеното за контакт определя уникален код на получения доклад, който недвусмислено идентифицира подателя на доклада и докладвания инцидент.

При предоставяне на актуализация на първоначалния доклад, на междинните доклади и окончателен доклад, свързани със същия инцидент финансовите субекти посочват уникалния код, определен от ИКТ звеното за контакт.

Финансовите субекти предоставят в първоначалните си доклади обща информация, която описва основните характеристики на инцидента и предполагаемите последствия, въз основа на информацията, която е налична веднага, след като той е класифициран като съществен.

Неокончателен (междинен) доклад

Финансовите субекти подават междинен доклад, когато обичайните дейности са възобновени и протичат нормално, като информират ИКТ звеното за контакт за това обстоятелство.

Финансовите субекти подават междинен доклад, когато извънредните мерки са преустановени.

Междинният доклад съдържа подробно описание на инцидента и последствията от него.

Когато обичайните дейности все още не са възстановени, финансовите субекти следва да предоставят междинен доклад на ИКТ звеното за контакт в рамките на 72 часа от подаването на първоначалния доклад.

Финансовите субекти актуализират вече предоставената информация в първия междинен доклад при настъпване на значителни промени в процеса на справяне с инцидента или в случаите, когато инцидентът не е бил разрешен в рамките на 72 часа, поради което финансовите субекти би трябвало да подадат допълнителен междинен доклад.

Допълнителен междинен доклад следва да бъде подаден и при изрично искане от ИКТ звеното за контакт.

В случаите, когато инцидентът е разрешен, преди да са изминали 24 часа от класифицирането му като съществен, финансовите субекти трябва да се стремят да подадат първоначалния и междинния доклад едновременно в срок до 24 часа.

Окончателен доклад

Финансовите субекти предоставят окончателен доклад на ИКТ звеното за контакт, след като бъде извършен анализ на първопричините, независимо дали вече са приложени мерки за редуциране или окончателната първопричина е установена, и са налице действителни данни, които да заместят всички потенциални прогнози.

Финансовите субекти предоставят окончателния доклад на ИКТ звеното за контакт в максимален срок до един месец, след подаване на първоначалното уведомяване.

Финансовите субекти, които се нуждаят от удължаване на този срок, е необходимо да се свържат с ИКТ звеното за контакт преди изтичането на срока и да предоставят

подходяща обосновка за закъснението, както и нова прогнозна дата за окончателния доклад.

Ако финансовите субекти могат да предоставят цялата информация, която се изисква в окончателния доклад в рамките на 24 часовия период след класифицирането на инцидента като съществен, те трябва да се стремят да предоставят едновременно информацията свързана с първоначалния, междинния и окончателния доклад.

В окончателния си доклад финансовите субекти следва да включат изчерпателна информация за първопричината, ако вече е известна, обобщение на предприетите или планираните мерки за отстраняване на проблема и предотвратяване на повторната му поява в бъдеще.

3.4. Финансовите субекти е необходимо да уведомят своите клиенти за възникналите съществени инциденти с ИКТ, от които има последици за финансовите интереси на клиентите, както и за предприетите мерки за ограничаване на неблагоприятните последици от тях съгласно чл. 19, параграф 3 от Регламент (ЕС) 2022/2554. Редът и начините за уведомяване се установяват съгласно чл. 24, параграф 1 от Делегиран регламент (ЕС) 2024/1774.

3.5. Финансовите субекти могат да възлагат на трета страна доставчик на услуги задълженията за докладване на съществени ИКТ инциденти. В случай на възлагане на задължения за докладване финансовият субект отговаря за изпълнението на изискванията за докладване на инциденти и са задължени да уведомят Комисията за финансов надзор веднага след сключване на договора за възлагане на докладването, но не по-късно от първото уведомление или докладване. Финансовите субекти предоставят на надзорния орган името, данните за контакт и идентификационния код на третата страна, която ще подава от тяхно име уведомленията или докладите за съществени инциденти с ИКТ.

4. Съвместно предоставяне на първоначално уведомление, междинен и окончателен доклад

Финансовите субекти могат да комбинират подаването на първоначалното уведомление, междинния доклад и окончателния доклад, когато редовните дейности са се възстановили или анализът на първопричината е приключил, и при условие че са спазени приложимите срокове.

5. Прекласифициране на съществени инциденти, свързани с ИКТ

Когато след допълнителна оценка финансовия субект стигне до заключението, че свързаният с ИКТ инцидент, за който преди това е било докладвано като съществен, в нито един момент не е отговарял на критериите и праговете за класифициране, финансовия

субект уведомява Комисията за финансов надзор, че е прекласифицирал инцидента с ИКТ от съществен в незначителен, като предоставя информацията за това прекласифициране.

6. Доброволно уведомяване за значителни киберзаплахи

6.1. Финансовите субекти могат на доброволен принцип да уведомят Комисията за финансов надзор за значителни киберзаплахи съгласно чл. 19, параграф 2 от Регламент (ЕС) 2022/2554.

По отношение на съдържанието на докладите за съществени инциденти с ИКТ и значителни киберзаплахи, както и във връзка със стандартизирането на формулярите, образците и процедурите, с които финансовите субекти докладват пред компетентните органи, са разработени регулаторни технически стандарти и технически стандарти за изпълнение с ясни насоки за докладването на инциденти, за да се осигури стандартизиран подход във всички финансови субекти, в съответствие с чл. 20, ал. 1, букви „а“ и „б“ от Регламент (ЕС) 2022/2554. Прилагането на тези стандарти е от съществено значение за ефективното управление на инциденти с ИКТ и спазване на нормативните изисквания.

III. Изисквания към финансовите субекти във връзка с тестване на оперативната устойчивост на цифровите технологии

1. Общи принципи

С оглед извършване на оценка на нивото на подготовка за преодоляване и справяне с евентуалното възникване на инциденти с ИКТ финансовите субекти, с изключение на финансови субекти - микропредприятия, въвеждат всеобхватна програма за тестване на оперативната устойчивост на цифровите технологии като неразделна част от рамката за управление на риска в областта на ИКТ.

С програмата се установяват слабостите и пропуските в оперативната устойчивост на цифровите технологии на финансовия субект и при спазване на принципа на пропорционалност се въвеждат корективни мерки за отстраняването им.

При изпълнение на програмата финансовите субекти следват подход, основан на риска като вземат предвид рисковете в областта на ИКТ, специфичните рискове, на които съответният финансов субект е или би могъл да бъде изложен, критичността на информационните активи и на предоставяните услуги, както и други фактори, които считат за подходящи.

Програмата за тестване на оперативната устойчивост на цифровите технологии съдържа набор от оценки, тестове, методи, практики и инструменти. Програмата предвижда провеждането на подходящи тестове като например оценка и изследване на уязвимите места, анализ на приложенията с отворен код, оценки на сигурността на мрежата, анализ на пропуските, преглед на физическата сигурност, преглед на

използваните програмни продукти, преглед на първичния код, тестване на различни сценарии, тестване на съвместимостта, тестване на функционирането, тестване по цялата верига и тестване за проникване.

Тестовете могат да се извършват от служител/и на финансовия субект (вътрешни лица) или от външни за него лица при осигуряване на гаранция, че тестването се извършва независимо. Когато тестовете се извършват от вътрешни лица, финансовия субект осигурява необходимите ресурси и гарантира, че няма конфликт на интереси по време на всички етапи на проектиране и провеждане на теста.

2. Периодичност на провеждане на тестването

2.1. Финансовите субекти извършват най-малко веднъж годишно подходящи тестове за всички системи и приложения на ИКТ, поддържащи критични или важни функции.

2.2. Финансовите субекти определят в своята програма за тестване на оперативната устойчивост на цифровите технологии периодичността на провеждане на тестове на системите и приложенията по изречение първо.

2.3. Централните депозитари на ценни книжа и централните контрагенти извършват оценки на уязвимите места преди внедряване или вторично внедряване на приложения и инфраструктурни компоненти и на услуги в областта на ИКТ, поддържащи критични или важни функции.

3. Облекчен режим за финансови субекти – микропредприятия

Финансовите субекти – микропредприятия, отчитайки факторите, посочени в чл. 25, параграф 3 от Регламент (ЕС) 2022/2554, извършват следните форми на тестове, посочени примерно в чл. 25, параграф 1 от същия регламент:

а) оценки и сканиране на уязвимите места;

б) анализ на приложенията с отворен код;

в) оценки на сигурността на мрежата;

г) анализ на пропуските;

д) преглед на физическата сигурност;

е) анкети и сканиране на програмните продукти;

ж) преглед на първичния код, когато такъв преглед е осъществим;

з) тестване на различни сценарии;

и) тестване на съвместимостта;

й) тестване на функционирането;

к) тестване по цялата верига;

л) тестване за проникване.

4. Обстойно тестване чрез проникване (Threat-led penetration testing или TLP тестване)

4.1. На основание чл. 26, параграф 8, ал. 3 от Регламент (ЕС) 2022/2554 Комисията за финансов надзор определя с решение финансовите субекти, от които се изисква да извършват TLP тестване, съгласно критериите, установени в регулаторни и технически стандарти, издадени на основание чл. 26, параграф 11 от същия регламент.

4.2. Определените с решение на Комисията за финансов надзор финансови субекти провеждат TLP тестване най-малкото веднъж на всеки три години. Комисията за финансов надзор може да намали или увеличи тази честота предвид рисковия профил на съответния финансов субект и други оперативни обстоятелства, установени при извършване на преглед за определяне на задължените за провеждане на TLP тестване финансови субекти.

4.3. Съгласно чл. 26, параграф 2 от Регламент (ЕС) 2022/2554 на TLP тестване подлежат някои или всички критични и/или важни ИКТ функции, чрез тестване на оперативните производствени системи. Всеки финансов субект сам оценява кои критични и важни ИКТ функции е необходимо да бъдат обхванати от тестването. Въз основа на оценката финансовият субект трябва да представи за одобрение в Комисията за финансов надзор точен обхват на ИКТ функциите, които ще бъдат тествани.

4.4. Когато TLP тестването обхваща трети страни доставчици на ИКТ, финансовите субекти гарантират, че тези трети страни участват в тестването, като съответният финансов субект продължава да е изцяло отговорен за спазването на Регламента.

4.5. На основание чл. 26, параграф 8 от Регламент (ЕС) 2022/2554 всяко трето по ред TLP тестване трябва да бъде извършено задължително от външни лица.

4.6. Участниците в TLP тестването трябва да управляват по подходящ начин риска от потенциално увреждане на данни или друго смущение в критичните или важните функции.

4.7. При приключване на TLP тестването финансовият субект или външното лице, провело тестването, предоставя на Комисията за финансов надзор обобщение на констатациите и плановете за корективни мерки, както и документацията, която доказва, че тестването за проникване е било проведено в съответствие с изискванията.

5. Лица, провеждащи TLP тестване

5.1. Както вътрешните, така и външните лица, провеждащи TLP тестване, трябва да отговарят на изискванията по чл. 27, параграф 1 от Регламент (ЕС) 2022/2554.

5.2. Финансовите субекти, които използват вътрешни лица, трябва да получат одобрение за това от Комисията за финансов надзор. За издаване на одобрение от

Комисията за финансов надзор трябва да бъде установено, че са изпълнени изискванията по чл. 27, параграф 2, букви „б“ и „в“ от Регламент (ЕС) 2022/2554.

5.3. При използването на външни лица финансовите субекти гарантират, че в договорите с тези лица изискват добро управление на резултатите от TLP тестването, както и че обработването на данни при тестването не поражда рискове за финансовия субект.

IV. Изисквания във връзка с управлението на риска в областта на ИКТ, пораждан от трети страни

1. Общи принципи

1.1. Финансовите субекти управляват риска в областта на ИКТ, възникващ от трети страни като част от рамката за управление на риска в областта на ИКТ съобразно принципа на пропорционалност, като вземат предвид естеството, мащаба, сложността и значението на зависимостите във връзка с ИКТ и рисковете, свързани с договорите за услуги в областта на ИКТ, сключени с трети страни доставчици на услуги в областта на ИКТ, отчитат характера на съответната услуга и потенциалното въздействие на тези рискове върху непрекъснатостта и наличността на финансовите услуги и дейности.

1.2. Финансовите субекти приемат и редовно преразглеждат стратегията за риска в областта на ИКТ, пораждан от трети страни. Стратегията за риска в областта на ИКТ, възникващ от трети страни, включва политика за използването на услуги в областта на ИКТ, поддържащи критичните или важните функции, предоставяни от трети страни доставчици на такива услуги. След извършване на оценка на цялостния рисков профил на финансовия субект и на мащаба и сложността на предоставяните услуги ръководните органи редовно извършват преглед на идентифицираните рискове по отношение на сключените договори за използване на услуги в областта на ИКТ, поддържащи критични или важни функции.

1.3. С приемането на Делегиран регламент (ЕС) 2024/1773 се хармонизират правилата по отношение съдържанието на политиката относно договорните споразумения за използването на услуги в областта на ИКТ, поддържащи критични или важни функции, предоставяни от трети страни доставчици на услуги в областта на ИКТ, като се отчитат размера, структурата, вътрешната организация и сложността на осъществяваните от финансовите субекти дейности.

2. Регистър на договорите с трети страни доставчици на ИКТ

2.1. Финансовите субекти поддържат и своевременно актуализират регистър за всички договори за услуги в областта на ИКТ, сключени с трети страни доставчици на такива услуги. Информацията за сключените договори се документира по подходящ

начин, като тази касаеща договори за услуги на ИКТ свързани с критични и/или важни функции, се обособява. По отношение на съдържанието на регистъра по чл. 28, параграф 3 от Регламент (ЕС) 2022/2554 и във връзка със задължителната информация, която следва да бъде включена в договорните споразумения за услуги в областта на ИКТ, предстои да бъдат приети технически стандарти за определяне на стандартните образци за целите на регистъра на договорите, включително на информацията, която е обща за всички договорни споразумения за услуги в областта на ИКТ.

2.2. Веднъж годишно финансовите субекти предоставят на Комисията за финансов надзор информация за сключените нови договори за услуги в областта на ИКТ, третите страни доставчици на такива услуги, вида на договорните споразумения и за предоставяните услуги и функции в областта на ИКТ. Финансовите субекти са длъжни да уведомят Комисията за финансов надзор за намерението си да сключат договор с трета страна доставчик на ИКТ, за критични и/или важни функции, както и когато дадена функция се е трансформирала в критична или важна.

2.3. При поискване от Комисията за финансов надзор финансовите субекти са длъжни да предоставят пълния регистър на сключените договори с трети страни, както и всяка друга относима информация с оглед на упражняването на ефективен надзор върху финансовия субект.

3. Сключване на договор за услуги с трета страна доставчик на ИКТ

3.1. Финансовите субекти могат да сключват договори за услуги само с трети страни доставчици на услуги в областта на ИКТ, които прилагат определени стандарти за сигурност на информацията.

3.2. Когато предмет на договора е възлагането на критични или важни функции, преди сключването му, финансовите субекти е необходимо да установят, че третите страни доставчици на услуги в областта на ИКТ отговарят на най-високите стандарти за сигурност на информацията.

3.3. Преди да сключат договор за услуги в областта на ИКТ с трета страна доставчик на ИКТ, финансовите субекти:

а) извършват преценка дали услугите в областта на ИКТ са свързани с поддържането на критична или важна функция;

б) извършват предварителна оценка за спазването на надзорните изисквания за възлагане на услугите;

в) идентифицират и оценят, включително и риска от концентрация в областта на ИКТ съгласно чл. 29 от Регламент (ЕС) 2022/2554;

г) идентифицират и оценяват потенциалните конфликти на интереси, които договорът може да породи.

3.4. При сключването на договор за услуги в областта на ИКТ финансовите субекти включват уговорки в него, които гарантират че прекратяването на договора няма да прекъсне осъществяването на дейността им, да засегне непрекъснатостта и качеството на предоставяните на клиентите услуги или да доведе до нарушаване на регулаторните изисквания.

3.5. В договора за услуги в областта на ИКТ се включват уговорки относно неговото прекратяването при настъпване на всяко едно от следните обстоятелства:

а) съществено нарушение на приложимите нормативни актове или на задълженията по договора, извършено от третата страна;

б) възникване на обстоятелства, които могат да променят изпълнението на предоставяните функции, включително съществени промени в условията на договора или такива, свързани с третата страна доставчик на услуги в областта на ИКТ;

в) установяване на слабости в управлението на риска в областта на ИКТ от третата страна, включително свързани с осигуряването на наличността, автентичността, целостта и поверителността на данните;

г) в случай, че условията на договора или други свързани с него обстоятелства възпрепятстват осъществяването на ефективен надзор върху финансовия субект от надзорния орган.

3.6. Договорите с трети страни доставчици на ИКТ трябва да включват ясни разпоредби относно правата и задълженията на страните, допустимост и условия за възлагане на дейности на подизпълнители, местоположение на услугите и защита на данните и др. В чл. 30 от Регламент (ЕС) 2022/2554 е регламентирано задължителното съдържание на договорите с трети страни доставчици на услуги в областта на ИКТ.

3.7. Финансовите субекти е необходимо да разполагат с алтернативни решения и преходни планове в случай на оттегляне на третата страна доставчик на услуги в областта на ИКТ и на съответните данни, както и за сигурното им предаване на алтернативни доставчици или за реинтегрирането им в собствените системи, както и за осигуряване на непрекъснатост на дейността.

4. Изходни планове и одити

4.1. За възлагане на услуги в областта на ИКТ, поддържащи критични или важни функции, финансовите субекти въвеждат изходни планове. Изходните планове трябва да бъдат изчерпателни, добре документирани, съответстващи на принципа на

пропорционалност. Те подлежат на периодично преразглеждане, актуализиране и тестване.

4.2. В изходните планове се включват и оценяват рисковете, свързани с трета страна доставчик на услуги в областта на ИКТ като прекратяване на дейността, влошаване на качеството на предоставяните услуги, възникване на съществен риск, свързан изпълнението на съответната услуга или прекратяването на договора.

4.3. Въз основа на подход, основан на риска финансовите субекти предварително определят честотата и обхвата на одитите на третата страна доставчик на услуги в областта на ИКТ. За определянето на елементите на одитите финансовите субекти се придържат към общоприетите одитни стандарти и съответните насоки от надзорните органи за използването и въвеждането на такива одитни стандарти. При реализиране на одитен ангажимент по договори, които съдържат технически елементи със значителна сложност, вътрешните или външни одитори е необходимо да притежават подходящи знания, умения и опит, за да извършат ефективно съответните одити и оценки.

V. Изисквания към финансовите субекти във връзка с обмена на информация и разузнавателни сведения за киберзаплахи и уязвими места

1. С цел подобряване на оперативната устойчивост на цифровите технологии в областта на ИКТ, чрез повишаване на осведомеността за киберзаплахите и тяхното предотвратяване или ограничаване, финансовите субекти могат да обменят помежду си информация и разузнавателни сведения за киберзаплахи, включително показатели за застрашена сигурност, тактики, техники и процедури, предупреждения във връзка с киберсигурността и инструменти за конфигуриране. Обменът на информация се извършва с оглед подпомагане на защитата срещу киберзаплахи, техниките за откриването им, надграждане на стратегиите за ограничаване на риска или на етапите на реакция и възстановяване.

2. Обменът на информация се извършва в рамките на общности от финансови субекти, които се ползват с необходимото доверие, посредством сключването на споразумения. В споразуменията за обмен на информация могат да участват финансовите субекти, трети страни доставчици на услуги в областта на ИКТ и публични органи. За осъществяване на ефективен обмен на информация между посочените субекти, в споразуменията може да се предвиди и използването на специални информационни платформи.

3. В споразуменията е необходимо да бъде гарантирана поверителността на споделената информация, спазването на етични правила, защитата на личните данни и търговската тайна, както и приложимото право в областта на конкуренцията.

4. Финансовите субекти са задължени да уведомяват Комисията за финансов надзор, когато участват или се присъединяват към споразумение за обмен на информация и разузнавателни сведения за киберзаплахи и уязвими места, както и при прекратяване на участието си в него.