Насоки

EBA/GL/2019/04

28 ноември 2019 г.

Насоки на ЕБО относно управление на риска в областта на ИКТ и сигурността

Спазване на насоките и задължения за докладване

Статут на настоящите насоки

1. Настоящият документ съдържа насоки, издадени съгласно член 16 от Регламент (ЕС) № 1093/2010 [1] . Съгласно член 16, параграф 3 от Регламент (ЕС) № 1093/2010, компетентните органи и финансовите институции полагат всички усилия за спазване на насоките.

2. В насоките е представено становището на ЕБО за подходящите надзорни практики в Европейската система за финансов надзор или за това как следва да се прилага правото на Европейския съюз в дадена област. Компетентните органи, както са определени в член 4, параграф 2 от Регламент (ЕС) № 1093/2010, и за които се отнасят тези насоки, трябва да ги спазват, като ги включат в практиките си по подходящ начин (напр. като изменят своята правна рамка или надзорни процеси), включително когато насоките са насочени основно към институциите.

Изисквания за докладване

3. Съгласно член 16, параграф 3 от Регламент (ЕС) № 1093/2010, най-късно до ([дд.мм.гггг]) компетентните органи трябва да уведомят ЕБО дали спазват или възнамеряват да спазват настоящите насоки, а в противен случай — да изложат причините за неспазването им. При липса на уведомление в този срок ЕБО ще счита компетентните органи за неспазващи изискванията. Уведомленията следва да се изпратят с помощта на формуляр, намиращ се на уебсайта, ЕБО, на адрес compliance@eba.europa.eu, като се посочи референтен номер „EBA/GL/2019/04“. Уведомленията следва да бъдат подадени от лица, оправомощени да докладват за наличието на съответствие от името на техните компетентни органи. Всяка промяна в статута на спазването трябва също да се докладва на ЕБО.

4. Уведомленията се публикуват на уебсайта на ЕБО съгласно член 16, параграф 3.

[1] Регламент (ЕС) № 1093/2010 на Европейския парламент и на Съвета от 24 ноември 2010 г. за създаване на Европейски надзорен орган (Европейски банков орган), за изменение на Решение № 716/2009/ЕО и за отмяна на Решение 2009/78/ЕО на Комисията (ОВ L 331, 15.12.2010 г., стр. 12).

Предмет, обхват и определения

Предмет

5. Настоящите насоки се основават на разпоредбите на член 74 от Директива 2013/36/ЕС (ДКИ) относно вътрешното управление и произтичат от мандата за разработване на насоки в член 95, параграф 3 от Директива (ЕС) 2015/2366 (ДПУ2).

6. В настоящите насоки се определят мерките за управление на риска, които финансовите институции (както са определени в точка 9 по-долу) трябва да предприемат в съответствие с член 74 от Директивата за капиталовите изисквания (ДКИ), за да управляват своите рискове в областта на ИКТ и сигурността за всички дейности и които доставчиците на платежни услуги (ДПУ, определени в точка 9 по-долу) трябва да предприемат в съответствие с член 95, параграф 1 от ДПУ2, за да управляват операционните рискове и рисковете, свързани със сигурността (по-нататък „рисковете в областта на ИКТ и сигурността“), свързани с предоставяните от тях платежни услуги. В насоките са включени изисквания относно информационната сигурност, включително киберсигурността, доколкото информацията се съхранява в ИКТ системи.

Обхват на прилагане

7. Настоящите насоки се прилагат във връзка с управлението на рисковете в областта на ИКТ и сигурността в рамките на финансовите институции (както е определено в точка 9). За целите на настоящите насоки понятието „рискове в областта на ИКТ и сигурността“ се отнася до операционните рискове и рисковете, свързани със сигурността, по член 95 от ДПУ2 за предоставянето на платежни услуги.

8. За ДПУ (както са определени в точка 9) настоящите насоки се прилагат към дейността им по предоставяне на платежни услуги в съответствие с обхвата и мандата по член 95 от ДПУ2. За институциите (както са определени в точка 9) настоящите насоки се прилагат към всички дейности, които те предоставят.

Адресати

9. Настоящите насоки са предназначени за финансовите институции, които за целите на настоящите насоки са 1) ДПУ, както са определени в член 4, параграф 11 от ДПУ2, и 2) институции, а именно кредитни институции и инвестиционни посредници съгласно определението в член 4, параграф 1, точка 3 от Регламент (ЕС) № 575/2013. Насоките се прилагат и към компетентните органи съгласно определението в член 4, параграф 1, точка 40 от Регламент (ЕС) № 575/2013, включително Европейската централна банка, по отношение на въпроси, свързани със задачите, възложени ѝ съгласно Регламент (ЕС) № 1024/2013, и към компетентните органи по ДПУ2, както е посочено в член 4, параграф 2, буква и) от Регламент (ЕС) № 1093/2010.

Определения

10. Освен ако не е посочено друго, термините, използвани и дефинирани в Директива 2013/36/ЕС (ДКИ), Регламент (ЕС) № 575/2013 (РКИ) и Директива (ЕС) 2015/2366 (ДПУ2), имат същото значение в насоките. В допълнение, за целите на настоящите насоки се прилагат следните определения:

Риск в областта на ИКТ и сигурността	Риск от загуба поради нарушаване на поверителността, нарушение на целостта на системи и данни, неподходящи или неналични системи и данни, или невъзможност за промяна на информационни технологии (ИТ) в приемлив срок и с разумни разходи, когато изискванията на средата или дейността се променят (т.е. бързина на извършване на промяна) [2] . Това включва рискове за сигурността, произтичащи от неподходящи или неуспешни вътрешни процеси или външни събития, включително кибератаки или неадекватна физическа сигурност.
Ръководен орган	(а) За кредитните институции и инвестиционните посредници този термин има същото значение като определението в член 3, параграф 1, точка 7) от Директива 2013/36/ЕС. (б) За платежните институции или институциите за електронни пари този термин означава директори или лица, отговарящи за управлението на платежните институции и институциите за електронни пари, и, където е приложимо, за лицата, отговарящи за управлението на дейностите, свързани с платежните услуги, на платежните институции и институциите за електронни пари. (в) За ДПУ, посочени в член 1, параграф 1, букви в), д) и е) от Директива (ЕС) 2015/2366, този термин има значението, което е определено от приложимото законодателство на ЕС или национално законодателство.
Операционен или свързан със сигурността инцидент	Отделно събитие или поредица от свързани събития, които не са планирани от финансовата институция и което има или вероятно ще има неблагоприятно въздействие върху целостта, наличността, поверителността и/или автентичността на услугите.
Висше ръководство	(а) За кредитните институции и инвестиционните посредници този термин има същото значение като определението в член 3, параграф 1, точка (9) от Директива 2013/36/ЕС. (б) За платежните институции и институциите за електронни пари този термин означава физически лица, които

[2] Определение от „Насоки на ЕБО относно общите процедури и методологии за процеса на надзорен преглед и оценка“ от 19 декември 2014 г. (EBA/GL/2014/13), изменени с EBA/GL/2018/03.

	упражняват изпълнителни функции в институцията и които са отговорни и подотчетни на ръководния орган за ежедневното управление на институцията. (в) За ДПУ, посочени в член 1, параграф 1, букви в), д) и е) от Директива (ЕС) 2015/2366, този термин има значението, което е определено от приложимото законодателство на ЕС или национално законодателство.
Рисков апетит	Съвкупното равнище и видове рискове, които доставчиците на платежни услуги и институциите са готови да поемат в рамките на своя капацитет за поемане на риск, в съответствие с техния бизнес модел, за да постигнат своите стратегически цели.
Функция за одит	(а) За кредитните институции и инвестиционните посредници функцията за одит е посочена в раздел 22 от Насоките на ЕБО относно вътрешното управление (EBA/GL/2017/11). (б) За доставчици на платежни услуги, различни от кредитни институции, функцията за одит трябва да бъде независима в рамките на доставчика на платежни услуги или от него и може да бъде функция за вътрешен и/или външен одит.
Проекти в областта на ИКТ	Всеки проект или част от него, в който системи и услуги в областта на ИКТ се променят, заменят, изваждат от употреба или се внедряват. ИКТ проектите могат да бъдат част от по-широки програми за трансформиране на ИКТ или на дейността.
Трета страна	Организация, която е встъпила в бизнес отношения или договори с предприятие за предоставяне на продукт или услуга[3].
Информационен актив	Съвкупност от информация, материална или нематериална, която е важно да бъде защитена.
ИКТ актив	Актив от софтуер или хардуер, който се намира в бизнес средата.
ИКТ системи[4]	Създаване на ИКТ като част от механизъм или свързваща мрежа, която подпомага дейността на финансова институция.
ИКТ услуги[5]	Услуги, предоставяни от ИКТ системи на един или повече вътрешни или външни потребители. Примерите включват въвеждане на данни, съхранение на данни, услуги за обработка и отчитане на данни, както и услуги за наблюдение, подпомагане на бизнеса и вземане на решения.

[3] Определение от основните елементи на Г-7 за управление на кибер риска, свързан с трети страни, във финансовия сектор.
[4] Определение от „Насоки за оценка на риска по отношение на ИКТ в рамките на процеса на надзорен преглед и оценка (ПНПО)“ (EBA/GL/2017/05).
[5] Пак там.

Изпълнение

Дата на прилагане

11. Насоките се прилагат от 30 юни 2020 г.

Отмяна

12. Насоките относно мерките за сигурност по отношение на операционните рискове и рисковете, свързани със сигурността (EBA/GL/2017/17), издадени през 2017 г., ще бъдат отменени с настоящите насоки на датата, на която настоящите насоки станат приложими.

Насоки относно управление на риска в областта на ИКТ и сигурността

1.1. Пропорционалност

1. Всички финансови институции следва да спазват разпоредбите, съдържащи се в настоящите насоки, по начин, който е пропорционален и при който се отчита мащаба на финансовите институции, вътрешната им организация и естеството, обхвата, сложността и степента на риск на услугите и продуктите, които финансовите институции предоставят или възнамеряват да предоставят.

1.2. Управление и стратегия

1.2.1. Управление

2. Ръководният орган следва да гарантира, че финансовите институции разполагат с подходяща рамка за вътрешно управление и вътрешен контрол по отношение на рисковете в областта на ИКТ и сигурността. Ръководният орган следва да определи ясни роли и отговорности по отношение на функциите, свързани с ИКТ, управлението на риска за информационната сигурност и непрекъсваемостта на дейността, включително тези за ръководния орган и неговите комитети.
3. Ръководният орган следва да гарантира, че броят и уменията на персонала на финансовите институции са адекватни за поддържане на техните оперативни нужди в областта на ИКТ и на техните процеси по управление на риска в областта на ИКТ и сигурността на текуща база, както и за гарантиране изпълнението на техните стратегии в областта на ИКТ. Ръководният орган следва да гарантира, че разпределеният бюджет е подходящ за изпълнение на горепосоченото. Освен това, финансовите институции следва да гарантират, че всички членове на персонала, включително заемащите ключови

позиции, ежегодно или по-често, ако е необходимо, преминават подходящо обучение относно рисковете в областта на ИКТ и на сигурността, включително относно информационната сигурност (вж. също раздел 1.4.7).

4. Ръководният орган носи обща отговорност за определяне, одобряване и надзор на изпълнението на стратегията на финансовите институции по отношение на ИКТ като част от цялостната им бизнес стратегия, както и за създаването на ефективна рамка за управление на риска по отношение на рисковете в областта на ИКТ и сигурността.

1.2.2. Стратегия

5. Стратегията в областта на ИКТ следва да бъде приведена в съответствие с цялостната бизнес стратегия на финансовите институции и следва да определя:

   а) по какъв начин следва да се развиват ИКТ на финансовите институции, за да подкрепят ефективно тяхната бизнес стратегия и да участват в нея, включително развитието на организационната структура, промените в ИКТ системата и ключови зависимости от трети страни;

   б) планираната стратегия и развитието на архитектурата на ИКТ, включително зависимостите от трети страни;

   в) ясни цели, свързани с информационната сигурност, с акцент върху ИКТ системите и ИКТ услугите, персонала и процесите.

6. Финансовите институции следва да изготвят планове за действие, съдържащи мерки, които да се предприемат за постигане на целта на стратегията в областта на ИКТ. Те следва да се свеждат до знанието на всички служители, за които се отнасят (включително изпълнители по договори и трети страни – доставчици, когато е приложимо и относимо). Плановете за действие следва да се преразглеждат периодично, за да се гарантира тяхната относимост и целесъобразност. Финансовите институции следва също така да установят процеси за наблюдение и измерване на ефективността на изпълнението на своята стратегия в областта на ИКТ.

1.2.3. Използване на трети страни — доставчици

7. Без да се засягат Насоките на ЕБО за възлагане на дейности на външни изпълнители (EBA/GL/2019/02) и член 19 от ДПУ2, финансовите институции следва да гарантират ефективността на мерките за редуциране на риска, определени в тяхната рамка за управление на риска, включително мерките, посочени в настоящите насоки, когато оперативните функции за платежни услуги и/или ИКТ услуги и ИКТ системи на която и да е дейност се възлагат на външни изпълнители, включително на субекти от групата, или при използването на трети страни.

8. За да се осигури непрекъсваемост на ИКТ услуги и ИКТ системи, финансовите институции следва да гарантират, че договорите и споразуменията за нивото на обслужване (както при нормални обстоятелства, така и в случай на прекъсване на услуга — вж. също раздел 1.7.2) с доставчиците (външни изпълнители, лица от групата или трети страни - доставчици) включват следното:

а) подходящи и пропорционални цели и мерки, свързани с информационната сигурност, включително изисквания като минимални изисквания за киберсигурност; спецификации за жизнения цикъл на данните на финансовата институция; всякакви изисквания относно криптиране на данни, сигурност на мрежата и процеси за наблюдение на сигурността, както и местоположението на центровете за данни;

б) процедури за действие при инциденти, засягащи оперативната дейност и сигурността, включително ескалация и докладване.

9. Финансовите институции следва да наблюдават и да търсят потвърждение за нивото на съответствие на тези доставчици с целите, мерките и целевите показатели по отношение на сигурността на финансовата институция.

1.3. Рамка за управление на риска в областта на ИКТ и сигурността

1.3.1. Организация и цели

10. Финансовите институции следва да идентифицират и управляват своите рискове в областта на ИКТ и сигурността. ИКТ функцията(ите), отговаряща(и) за ИКТ системи, процеси и операции по сигурността, следва да разполага с подходящи процеси и механизми за контрол, за да гарантира, че всички рискове се идентифицират, анализират, измерват, наблюдават, управляват, докладват и поддържат в границите на рисковия апетит на финансовата институция, както и че проектите и системите, които те изпълняват, и дейностите, които извършват, са в съответствие с външните и вътрешните изисквания.

11. Финансовите институции следва да възложат отговорността за управление и надзор на рисковете в областта на ИКТ и сигурността на контролната функция, придържайки се към изискванията на раздел 19 от Насоките на ЕБО относно вътрешното управление (EBA/GL/2017/11). Финансовите институции следва да гарантират независимостта и обективността на тази контролна функция, като я отделят по подходящ начин от процесите, свързани с операциите в областта на ИКТ. Тази контролна функция следва да се отчита пряко пред ръководния орган и да отговаря за наблюдението и контрола на спазването на рамката за управление на риска в областта на ИКТ и сигурността. Тя следва да гарантира, че рисковете в областта на ИКТ и сигурността се идентифицират, измерват, оценяват, управляват, наблюдават и докладват. Финансовите институции следва да гарантират, че тази контролна функция не носи отговорност за провеждане на вътрешен одит.

Функцията за вътрешен одит следва, в съответствие с основан на риска подход, да има капацитета да извършва независим преглед и да осигурява обективно потвърждение за съответствието на всички свързани с ИКТ и със сигурността дейности и звена на дадена финансова институция с политиките и процедурите на финансовата институция и с външните изисквания, като се спазват изискванията на раздел 22 от Насоките на ЕБО относно вътрешното управление (EBA/GL/2017/11).

12. Финансовите институции следва да определят и възлагат ключови роли и отговорности, както и съответни йерархични линии, за да може рамката за управление на риска в областта на ИКТ и сигурността да бъде ефективна. Тази рамка следва да бъде напълно интегрирана в цялостните процеси на управление на риска на финансовите институции и да бъде приведена в съответствие с тях.

13. Рамката за управление на риска в областта на ИКТ и сигурността следва да включва процедури за:

    а) определяне на рисковия апетит по отношение на рисковете за ИКТ и сигурността в съответствие с рисковия апетит на финансовата институция;
    б) идентифициране и оценяване на рисковете в областта на ИКТ и сигурността, на които е изложена финансовата институция;
    в) определяне на мерки за смекчаване на последиците, включително контроли, с цел редуциране на рисковете в областта на ИКТ и сигурността;
    г) наблюдение на ефективността на тези мерки, както и броя на докладваните инциденти, включително за доставчиците на платежни услуги, за инцидентите, докладвани в съответствие с член 96 от ДПУ2, които засягат свързаните с ИКТ дейности, и предприемане на действия за коригиране на мерките, при необходимост;
    д) докладване на ръководния орган относно рисковете и проверките в областта на ИКТ и сигурността;
    е) идентифициране и оценяване дали съществуват някакви рискове за ИКТ и за сигурността, произтичащи от всякакви значителни промени в ИКТ системи или услуги, процеси или процедури в областта на ИКТ, и/или след всеки значим оперативен или свързан със сигурността инцидент.

14. Финансовите институции следва да гарантират, че рамката за управление на риска в областта на ИКТ и сигурността се документира и се подобрява непрекъснато въз основа на „извлечени поуки“ по време на нейното прилагане и наблюдение. Рамката за управление на риска в областта на ИКТ и сигурността следва да бъде одобрявана и преглеждана поне веднъж годишно от ръководния орган.

1.3.2. Определяне на функциите, процесите и активите

15. Финансовите институции следва да определят, установят и поддържат актуализирана съпоставка на техните бизнес функции, роли и поддържащи процеси, за да определят значението на всяко едно от тях и техните взаимозависимости, свързани с рисковете в областта на ИКТ сигурността.

16. Освен това финансовите институции следва да идентифицират, установят и поддържат актуална съпоставка на информационните активи, подпомагащи техните бизнес функции и поддържащи процеси, като например ИКТ системи, персонал, изпълнители по договори, трети страни и зависимости от други вътрешни и външни системи и процеси, за да могат най-малкото да управляват информационните активи, които подпомагат техните критични бизнес функции и процеси.

1.3.3. Класификация и оценка на риска

17. Финансовите институции следва да класифицират по критичност установените стопански функции, поддържащи процеси и информационни активи, посочени в точки 15 и 16.

18. За да определи критичността на тези идентифицирани бизнес функции, поддържащи процеси и информационни активи, финансовите институции следва като минимум да вземат под внимание изискванията за поверителност, цялостност и достъпност. Следва да има ясно определена отчетност и отговорност за информационните активи.

19. Когато се извършва оценка на риска, финансовите институции следва да преглеждат адекватността на класификацията на информационните активи и относимата документация.

20. Финансовите институции следва да определят рисковете в областта на ИКТ и сигурността, които оказват въздействие върху установените и класифицирани бизнес функции, поддържащи процеси и информационни активи, според тяхната критичност. Тази оценка на риска следва да се извършва и документира ежегодно или на по-кратки интервали, ако е необходимо. Такива оценки на риска следва да се извършват и при всякакви значителни промени в инфраструктурата, процесите или процедурите, засягащи бизнес функциите, поддържащите процеси или информационните активи, и съответно текущата оценка на риска на финансовите институции следва да бъде актуализирана.

21. Финансовите институции следва да гарантират, че непрекъснато наблюдават заплахи и уязвимости, свързани с техните бизнес процеси, поддържащи функции и информационни активи, и следва редовно да правят преглед на рисковите сценарии, които оказват въздействие върху тях.

1.3.4. Редуциране на риска

22. Въз основа на оценките на риска финансовите институции следва да определят кои мерки са необходими за редуциране на идентифицираните рискове в областта на ИКТ и сигурността до приемливи нива и дали са необходими промени в съществуващите бизнес процеси, мерки за контрол, ИКТ системи и ИКТ услуги. Финансовата институция следва да вземе предвид времето, необходимо за внедряване на тези промени, както и времето за предприемане на подходящи междинни мерки за редуциране на риска, за да минимизират рисковете в областта на ИКТ и сигурността и те да останат в рамките на рисковия апетит на финансовата институция, свързан с ИКТ и сигурността.

23. Финансовите институции следва да определят и прилагат мерки за редуциране на идентифицираните рискове в областта на ИКТ и сигурността и за защита на информационните активи в съответствие с тяхната класификация.

1.3.5. Докладване

24. Финансовите институции следва да докладват на ръководния орган резултатите от оценката на риска по ясен и своевременен начин. Това докладване не засяга

задължението на доставчиците на платежни услуги да предоставят на компетентните органи актуализирана и всеобхватна оценка на риска в съответствие с член 95, параграф 2 от Директива (ЕС) 2015/2366.

1.3.6. Одит

25. Управлението, системите и процесите на финансовата институция във връзка с нейните рискове в областта на ИКТ и сигурността следва да бъдат одитирани периодично от одитори с достатъчно знания, умения и опит в областта на рисковете за ИКТ и сигурността и на плащанията (за доставчиците на платежни услуги), за да се осигури независимо потвърждение за ръководния орган на тяхната ефективност. Одиторите следва да бъдат независими в рамките на финансовата институция или от нея. Честотата и фокусът на такива одити следва да бъдат съизмерими със съответните рискове в областта на ИКТ и сигурността.

26. Ръководният орган на финансовата институция следва да одобрява плана за одит, включително всички одити на ИКТ и всякакви съществени промени в него. Планът за одит и неговото изпълнение, включително честотата на одита, следва да отразяват и да бъдат пропорционални на присъщите на финансовата институция рискове в областта на ИКТ и сигурността и следва редовно да бъдат актуализирани.

27. Следва да бъде установен официален процес на последващо проследяване, включително разпоредби за навременна проверка и отстраняване на критични констатации от одита в областта на ИКТ.

1.4. Информационна сигурност

1.4.1. Политика в областта на информационната сигурност

28. Финансовите институции следва да разработят и документират политика за информационна сигурност, която следва да определя общоприетите принципи и правила за защита на поверителността, целостта и наличността на данните и информацията на финансовите институции и на техните клиенти. За доставчиците на платежни услуги тази политика е посочена в документа относно политиката по сигурността, който трябва да бъде приет в съответствие с член 5, параграф 1, буква ѝ) от Директива (ЕС) 2015/2366. Политиката в областта на информационната сигурност следва да бъде съобразена с целите на финансовата институция по отношение на информационната сигурност и да се основава на относимите резултати от процеса за оценка на риска. Политиката следва да бъде одобрена от ръководния орган.

29. Политиката следва да включва описание на основните роли и отговорности на управлението на информационната сигурност и следва да определя изискванията към персонала и изпълнителите по договори, процесите и технологиите във връзка с информационната сигурност, приемайки, че персоналът и изпълнителите по договори на всички равнища имат отговорности за гарантиране на информационната сигурност на финансовите институции. Политиката следва да гарантира поверителността, целостта и наличността на критичните логически и физически активи, ресурси и чувствителни данни на финансовата институция, независимо дали се отнася за съхранявани неактивни данни, данни в процес на прехвърляне или съхранявани активни оперативни данни. За политиката в областта на информационната сигурност следва да се уведомяват всички служители и изпълнители на финансовата институция.

30. Въз основа на политиката за информационната сигурност финансовите институции следва да установят и прилагат мерки за сигурност за редуциране на рисковете за ИКТ и сигурността, на които са изложени. Тези мерки следва да включват:

    а) организация и управление в съответствие с точки 10 и 11;
    б) логическа сигурност (раздел 1.4.2);
    в) физическа сигурност (раздел 1.4.3);
    г) сигурност на операциите в областта на ИКТ (раздел 1.4.4);
    д) наблюдение на сигурността (раздел 1.4.5);
    е) прегледи, оценка и тестване на информационната сигурност (раздел 1.4.6);
    ж) обучение и осведоменост по въпросите на информационната сигурност (раздел 1.4.7).

1.4.2. Логическа сигурност

31. Финансовите институции следва да определят, документират и прилагат процедури за логически контрол на достъпа (управление на самоличността и достъпа). Тези процедури следва да бъдат внедрени, прилагани, наблюдавани и периодично преразглеждани. Процедурите следва също така да включват контрол за наблюдение на аномалии. Чрез тези процедури следва да бъдат изпълнявани като минимум следните елементи, а терминът „потребител“ следва да включва и техническите потребители:

    а) **Необходимост да се знае, най-малка привилегия и разделение на задължения:** финансовите институции следва да управляват правата на достъп до информационните активи и поддържащите ги системи въз основа на принципа „необходимост да се знае“, включително за достъп от разстояние. На потребителите следва да се предоставят права за минимален достъп, които са строго необходими за изпълнение на техните задължения (принцип на „най-малка привилегия“), т.е. да се предотврати неоправдан достъп до голям набор от данни или да се предотврати разпределянето на комбинации от права на достъп, които могат да се използват за заобикаляне на мерки за контрол (принцип на „разделение на задълженията“).

б) **Отговорност на потребителите:** финансовите институции следва да ограничават във възможно най-голяма степен използването на общи и споделени потребителски профили и да гарантират, че потребителите могат да бъдат идентифицирани за действията, извършвани в ИКТ системите.

в) **Привилегировани права на достъп:** финансовите институции следва да осъществяват строг контрол върху привилегирования достъп до системата чрез строго ограничаване и внимателно наблюдение на профилите с по-високи права на достъп (например профили на администратори). За да се гарантира сигурност на комуникациите и да се намали риска, дистанционен достъп за администриране на критични ИКТ системи следва да се предоставя само на принципа „необходимост да се знае“ и когато се използват много надеждни решения за установяване на идентичността.

г) **Проследяване действията на потребителите:** като минимум, всички действия на привилегировани потребители следва да бъдат регистрирани и наблюдавани. Регистрите на достъпа следва да бъдат защитени, с цел предотвратяване на неразрешено изменение или заличаване и съхранявани за период, който е съизмерим с критичността на определените бизнес функции, помощни процеси и информационни активи в съответствие с раздел 1.3.3, без да бъдат засягани изискванията за запазване, определени в законодателството на ЕС и националното законодателство. Финансовата институция следва да използва тази информация за улесняване на процеса на идентифициране и разследване на аномални действия, които са били открити при предоставянето на услуги.

д) **Управление на достъпа:** права на достъп следва да се предоставят, отнемат или изменят своевременно в съответствие с предварително установени работни процеси за одобрение, които включват собственика на информацията, подлежаща на оценяване (собственик на информационния актив). В случай на прекратяване на трудово правоотношение правата на достъп следва своевременно да бъдат отнети.

е) **Подновяване на сертификата за достъп:** правата на достъп следва да бъдат преглеждани периодично, за да се гарантира, че потребители не притежават прекомерни привилегии и че правата на достъп са отнети, когато вече не са необходими.

ж) **Методи за установяване на идентичността:** финансовите институции следва да прилагат методи за установяване на идентичността, които са достатъчно надеждни, за да гарантират адекватно и ефективно спазване на политиките и процедурите за контрол на достъпа. Методите за установяване на идентичността следва да бъдат съизмерими с критичността на оценяваните ИКТ системи, информация или процес. Това следва да включва, като минимум, сложни пароли или по-строги методи за установяване на идентичността (като например двуфакторна автентификация), на базата на относим риск.

32. Електронният достъп чрез приложни програми до данни и ИКТ системи следва да бъде ограничен до минимално необходимия за изпълнение на съответната услуга.

1.4.3. Физическа сигурност

33. Следва да бъдат определени, документирани и приложени физически мерки за сигурност на финансовите институции за защита на техните помещения, центрове за данни и чувствителни зони от нерегламентиран достъп и от опасности, свързани с околната среда.

34. Физическият достъп до ИКТ системи следва да бъде предоставян само на лица, които имат разрешение за това. Разрешение следва да бъде предоставяно в съответствие със задачите и отговорностите на лицето и да бъде ограничено до лица, които са подходящо обучени и наблюдавани. Физическият достъп следва редовно да бъде преглеждан, за да се гарантира, че ненужните права за достъп се отнемат незабавно, когато не са необходими.

35. Подходящи мерки за защита от опасности, свързани с околната среда, следва да бъдат съизмерими със значението на сградите и критичността на операциите или на ИКТ системите, намиращи се в тези сгради.

1.4.4. Сигурност на операциите в областта на ИКТ

36. Финансовите институции следва да прилагат процедури за предотвратяване възникването на проблеми със сигурността в ИКТ системите и ИКТ услугите и следва да сведат до минимум тяхното въздействие върху предоставянето на ИКТ услуги. Тези процедури следва да включват следните мерки:

    а) идентифициране на потенциални уязвимости, които следва да бъдат оценявани и отстранявани, като се гарантира актуализиране на софтуера и фърмуера, включително софтуера, предоставен от финансовите институции на техните вътрешни и външни потребители, чрез инсталиране на критично важни за сигурността обновявания или чрез прилагане на компенсаторни контролни механизми;
    б) внедряване на защитени базови конфигурации във всички компоненти на мрежата;
    в) извършване на сегментация на мрежата, използване на системи за предотвратяване на загуба на данни и за криптиране на мрежовия трафик (в съответствие с класификацията на данните);
    г) прилагане на защита на крайните точки, включително на сървъри, работни станции и мобилни устройства; финансовите институции следва да оценяват дали крайните точки отговарят на стандартите за сигурност, определени от тях, преди да им бъде предоставен достъп до корпоративната мрежа;
    д) гарантиране наличието на механизми за проверка на целостта на софтуера, фърмуера и данните;
    е) криптиране на данните в режим на покой и в режим на движение (в съответствие с класификацията на данните).

37. Освен това, на текуща основа, финансовите институции следва да определят дали промените в съществуващата оперативна среда оказват влияние върху съществуващите

мерки за сигурност или налагат приемане на допълнителни мерки за редуциране по подходящ начин на съответните рискове. Тези промени следва да бъдат част от официалния процес на финансовите институции за управление на промените, чрез който следва да се гарантира, че промените се планират, проверяват, документират, одобряват и внедряват по подходящ начин.

1.4.5. Наблюдение на сигурността

38. Финансовите институции следва да въведат и прилагат политики и процедури за откриване на аномални дейности, които биха могли да окажат влияние върху информационната сигурност на финансовите институции, и да реагират подходящо на тези събития. Като част от това постоянно наблюдение, финансовите институции следва да прилагат подходящи и ефективни мерки за откриване и докладване на физическо или логическо вмешателство, както и нарушения на поверителността, целостта и достъпността на информационните активи. Процесите за постоянно наблюдение и откриване следва да обхващат:

    а) относими вътрешни и външни фактори, включително бизнес и административни функции, свързани с информационните и комуникационните технологии;
    б) операции за установяване на злоупотреба с достъп от трети страни или други лица и вътрешна злоупотреба с достъп;
    в) потенциалните вътрешни и външни заплахи.

39. Финансовите институции следва да въведат и прилагат процеси и организационни структури, за да идентифицират и постоянно да наблюдават заплахи за сигурността, които биха могли да окажат съществено въздействие върху способността им да предоставят услуги. Финансовите институции следва активно да следят развитието на технологиите, за да гарантират, че са наясно с рисковете за сигурността. Финансовите институции следва да прилагат мерки за откриване, например за идентифициране на възможни случаи на изтичане на информация, зловредни кодове и други заплахи за сигурността, както и общоизвестни уязвими точки в софтуера и хардуера, и следва да извършват проверка за нови актуализации, относими към сигурността.

40. Процесът за наблюдение на сигурността следва също така да помага финансовата институция да разбере естеството на оперативни инциденти или инциденти, свързани със сигурността, да установява тенденции и да подпомага провежданите от организацията разследвания.

1.4.6. Прегледи, оценка и тестване на информационната сигурност

41. Финансовите институции следва да извършват различни прегледи, оценки и тестване на информационната сигурност, за да се гарантира ефективното установяване на уязвимости в техните ИКТ системи и ИКТ услуги. Финансовите институции например могат да извършват анализ на отклоненията спрямо стандартите за информационна сигурност, прегледите за нормативно съответствие, вътрешните и външните одити на информационните системи или прегледите на физическата сигурност. Освен това,

институцията следва да обмисли добри практики, като например прегледи на изходни кодове, оценки на уязвимостта, тестове за проникване и упражнения с червени отбори (red team exercises).

42. Финансовите институции следва да внедрят и прилагат рамка за тестване на информационната сигурност, която да потвърждава надеждността и ефективността на техните мерки за информационна сигурност, и да гарантират, че в тази рамка са взети под внимание заплахи и слаби места, установени в процеса на наблюдение на заплахите и оценка на риска в областта на ИКТ и сигурността.

43. Рамката за тестване на информационната сигурност следва да гарантира, че тестовете:

    а) се извършват от независими проверители с достатъчно знания, умения и опит за тестване на мерки за информационна сигурност и които не участват в разработването на тези мерки;

    б) включват тестове за установяване на уязвимости и тестове за проникване (включително тестове за проникване във връзка с установени заплахи, когато е необходимо и целесъобразно), съизмерими със степента на риска, установен при бизнес процеси и системи.

44. Финансовите институции следва да извършват текущи и повтарящи се тестове на мерките за сигурност. За всички ИКТ системи (точка 17) тези тестове следва да бъдат извършвани поне веднъж годишно, а за ДПУ те ще бъдат част от подробната оценка на рисковете за сигурността, свързани с платежните услуги, които те предоставят, в съответствие с член 95, параграф 2 от ДПУ2. Системите, които не са от критично значение, следва да бъдат тествани редовно, като се прилага основан на риска подход, но най-малко веднъж на всеки 3 години.

45. Финансовите институции следва да гарантират, че се провеждат тестове на мерките за сигурност в случай на промени в инфраструктурата, процесите или процедурите и ако промените са направени поради големи оперативни инциденти или инциденти, свързани със сигурността, или поради въвеждането на нови или значително променени критични приложения, които са видими и/или достъпни през интернет.

46. Финансовите институции следва да наблюдават и оценяват резултатите от тестовете на сигурността и да актуализират своите мерки за сигурност съобразно тях, без необосновано забавяне, когато се отнася за критични ИКТ системи.

47. По отношение на ДПУ, рамката за тестване следва също да обхваща мерките за сигурност, свързани с 1) платежни терминали и устройства, които се използват за предоставяне на платежни услуги, (2) платежни терминали и устройства, които се използват за установяване на идентичността на ползвателите на платежни услуги (ППУ), и (3) устройства и софтуер, предоставени от ДПУ на ППУ за генериране/получаване на код за установяване на идентичността.

48. Въз основа на наблюдаваните заплахи за сигурността и направените промени тестването следва да се провежда така, че да включва сценарии на относими и известни потенциални атаки.

1.4.7. Обучение и осведоменост по въпросите на информационната сигурност

49. Финансовите институции следва да създадат програма за обучение, която включва периодични програми за осведоменост по въпросите на сигурността, за всички служители и изпълнители по договори, за да се гарантира, че те са обучени да изпълняват своите задължения и отговорности съгласно съответните политики и процедури за сигурност, за намаляване на човешки грешки, кражби, измами, злоупотреби или загуби и начини за справяне с рисковете, свързани с информационната сигурност. Финансовите институции следва да гарантират, че програмата за обучение осигурява обучение на всички служители и изпълнители по договори поне веднъж годишно.

1.5. Управление на операции в областта на ИКТ

50. Финансовите институции следва да управляват своите операции в областта на ИКТ въз основа на документирани и внедрени процеси и процедури (които за доставчиците на платежни услуги включват документа относно политиката по сигурността в съответствие с член 5, параграф 1, буква й) от ДПУ2), които са одобрени от ръководния орган. Този набор от документи следва да определя начина, по който финансовите институции извършват, наблюдават и контролират своите системи и услуги в областта на ИКТ, включително документирането на критични дейности в областта на ИКТ, и следва да дава възможност на финансовите институции да поддържат актуална инвентаризация на ИКТ активи.

51. Финансовите институции следва да гарантират, че изпълнението на техните операции в областта на ИКТ да съответства на техните бизнес изисквания. Финансовите институции следва да поддържат и подобряват, когато е възможно, ефективността на своите операции в областта на ИКТ, включително, но не само, и на необходимостта да се обмислят начини за свеждане до минимум на потенциални грешки, произтичащи от неавтоматизирано изпълнение на задачи.

52. Финансовите институции следва да прилагат процедури за регистриране и наблюдение на критични операции в областта на ИКТ, за да се даде възможност за откриване, анализ и коригиране на грешки.

53. Финансовите институции следва да поддържат актуална инвентаризация на своите ИКТ активи (включително ИКТ системи, мрежови устройства, бази данни и др.). Инвентаризацията на ИКТ активите следва да съхранява конфигурацията на ИКТ активите, както и връзките и взаимозависимостите между различните ИКТ активи, за да се създадат условия за подходяща конфигурация и процес на управление на промените.

54. Инвентаризацията на активите в областта на ИКТ следва да бъде достатъчно подробна, за да позволи бързото идентифициране на актив в областта на ИКТ, неговото местоположение, класификация за сигурност и собственост. Взаимозависимостите между активи следва да бъдат документирани, за да се подпомогне реагирането при инциденти, свързани със сигурността, и оперативни инциденти, включително кибератаки.

55. Финансовите институции следва да наблюдават и управляват жизнения цикъл на активите в областта на ИКТ, за да се гарантира, че те продължават да отговарят и подпомагат изискванията на бизнеса и управлението на риска. Финансовите институции следва да следят дали техните активи в областта на ИКТ се поддържат от техните външни или вътрешни доставчици и разработчици и дали всички относими обновявания и актуализации се прилагат въз основа на документирани процеси. Рисковете, произтичащи от остарели или неподдържани ИКТ активи, следва да бъдат оценявани и ограничавани.

56. Финансовите институции следва своевременно да прилагат процеси за изпълнение и планиране на капацитета, както и наблюдение на процесите с цел предотвратяване, разкриване и реагиране при значими проблеми във връзка с ефективността на ИКТ системите и недостига на капацитет в областта на ИКТ.

57. Финансовите институции следва да определят и прилагат процедури за създаване на резервни копия и възстановяване на данни и ИКТ системи, за да се гарантира, че те могат да бъдат възстановени според изискванията. Обхватът и честотата на създаване на резервни копия следва да бъдат определени в съответствие с изискванията за възстановяване на дейността и критичността на данните и ИКТ системите, както и да бъдат преценявани в съответствие с извършената оценка на риска. Периодично следва да бъдат извършвани практически тестове на изпълнението на процедурите за създаване на резервни копия и възстановяване.

58. Финансовите институции следва да гарантират, че резервните копия на данни и ИКТ системи се съхраняват по сигурен начин и са на достатъчно отдалечено разстояние от местонахождението на основния център, така че да не бъдат изложени на същите рискове.

3.5.1 Управление на инциденти и проблеми в областта на ИКТ

59. Финансовите институции следва да установят и прилагат процес на управление на инциденти и проблеми, за да наблюдават и регистрират оперативните и свързаните със сигурността инциденти в областта на ИКТ и да дават възможност на финансовите институции да продължават или да възобновяват своевременно критични бизнес функции и процеси при възникване на смущения. Финансовите институции следва да определят подходящи критерии и прагове за класифициране на събития като оперативни инциденти или инциденти, свързани със сигурността, както е посочено в раздел „Определения“ от настоящите насоки, както и показатели за ранно предупреждение, които следва да служат като сигнали за ранно откриване на тези инциденти. Такива критерии и прагове за доставчиците на платежни услуги не засягат класификацията на сериозни инциденти в съответствие с член 96 от ДПУ2 и Насоките за докладване на големи инциденти по ДПУ2 (EBA/GL/2017/10).

60. За да бъде сведено до минимум въздействието на неблагоприятните събития и да бъде възможно навременно възстановяване, финансовите институции следва да въведат подходящи процеси и организационни структури, за да се гарантира последователно и

интегрирано наблюдение, обработка и последващи действия при оперативни инциденти и инциденти, свързани със сигурността, както и да се гарантира, че основните причини са идентифицирани и отстранени, за да бъде предотвратено възникването на повтарящи се инциденти. В процеса на управление на инциденти и проблеми следва да бъдат установени:

а) процедурите за идентифициране, проследяване, регистриране, категоризиране и класифициране на инциденти по даден приоритет, въз основа на критичност на дейността;

б) ролите и отговорностите за различните сценарии на инциденти (напр. грешки, неизправности, кибератаки);

в) процедури за управление на проблеми с цел идентифициране, анализиране и разрешаване на първопричините за един или повече инциденти — финансовата институция следва да анализира оперативни инциденти или инциденти, свързани със сигурността, които е възможно да засегнат финансовата институция и които са били идентифицирани или са възникнали в рамките на организацията и/или извън нея, както и да взема предвид ключовите поуки, извлечени от тези анализи, и съответно да актуализира мерките за сигурност;

г) ефективни планове за вътрешна комуникация, включително уведомяване за инциденти и процедури за ескалация, които обхващат също така жалби на клиенти, свързани със сигурността, за да се гарантира, че:

   i) инциденти с потенциално силно неблагоприятно въздействие върху критични ИКТ системи и ИКТ услуги се докладват на съответното висше ръководство и висшето ръководство в областта на ИКТ;

   ii) ръководният орган е информиран при всеки конкретен случай на значими инциденти и, най-малкото, е информиран за въздействието, реакцията и допълнителните контролни мерки, които да бъдат определени в резултат на инцидентите.

д) процедури за реагиране при инциденти, за да бъдат смекчени въздействията, свързани с инцидентите, и за своевременно пълно възобновяване и осигуряване на обслужването;

е) специфични планове за външна комуникация за критични бизнес функции и процеси, с цел:

   i) сътрудничество със съответни заинтересовани страни, за ефективно реагиране и възстановяване при инцидент;

   ii) своевременно предоставяне на информация на външни страни (напр. клиенти, други участници на пазара, надзорния орган) по подходящ начин и в съответствие с приложимите регулации.

1.6. Управление на проекти и промени в областта на ИКТ

1.6.1. Управление на проекти в областта на ИКТ

61. Финансовата институция следва да прилага програма и/или процес за управление на проекти, в която са определени роли, отговорности и задължения за ефективно подпомагане изпълнението на стратегията в областта на ИКТ.

62. Финансовата институция следва да наблюдава по подходящ начин и да редуцира рискове, произтичащи от портфолиото на проектите в областта на ИКТ (управление на програмата), като взема предвид и рисковете, които могат да възникнат от взаимозависимостите между различни проекти и зависимости на множество проекти, базирани върху едни и същи ресурси и/или експертен опит.

63. Финансовата институция следва да създаде и прилага политика за управление на проекти в областта на ИКТ, която включва като минимум:

    а) цели на проекта;
    б) роли и отговорности;
    в) оценка на риска на проекта;
    г) план на проекта, график и стъпки;
    д) основни етапи;
    е) изисквания за управление на промените.

64. Политиката за управление на проекти в областта на ИКТ следва да гарантира, че изискванията за информационна сигурност се анализират и одобряват от функция, която е независима от функцията, отговорна за разработването.

65. Финансовата институция следва да гарантира, че всички сфери, засегнати от проекта в областта на ИКТ, са представени в екипа по проекта и че екипът по проекта разполага със знания, изисквани за осигуряване на сигурно и успешно изпълнение на проекта.

66. Създаването и напредъкът по проекти в областта на ИКТ и свързаните с тях рискове следва да бъдат докладвани на ръководния орган, поотделно или като цяло, в зависимост от важността и мащаба на проектите в областта на ИКТ, редовно и при конкретни случаи, ако е подходящо. Финансовите институции следва да включват риска по проекта в своята рамка за управление на риска.

1.6.2. Придобиване и разработване на ИКТ системи

67. Финансовите институции следва да разработват и прилагат процес, който урежда придобиването, разработването и поддръжката на ИКТ системи. Този процес следва да бъде разработен, като се използва основан на риска подход.

68. Финансовата институция следва да гарантира, че преди придобиване или разработване на ИКТ системи функционалните и нефункционалните изисквания (включително изисквания за информационна сигурност) са ясно определени и одобрени на съответното ръководно бизнес ниво.

69. Финансовата институция следва да гарантира, че са въведени мерки за редуциране на риска от неволно изменение или умишлено манипулиране на ИКТ системите по време на разработването и внедряването в продукционната среда.

70. Финансовите институции следва да разполагат с методология за тестване и одобряване на ИКТ системите преди използването им за пръв път. В тази методология следва да бъде отчетена критичността на бизнес процеси и активи. С тестването следва да се гарантира, че новите ИКТ системи функционират според очакванията. Те следва, също така, да използват тестови среди, които адекватно отразяват продукционната среда.

71. Финансовите институции следва да тестват ИКТ системи, ИКТ услуги и мерки за информационна сигурност, за да откриват потенциални слабости в сигурността, нарушения и инциденти.

72. Финансовата институция следва да използва отделни среди в областта на ИКТ, за да гарантира адекватно разделение на задълженията и да смекчи въздействието на непроверени промени в продукционните системи. По-конкретно, финансовата институция следва да гарантира изолирането на продукционните среди от среди за разработване, тестване и други непродукционни среди. Финансовата институция следва да гарантира целостта и поверителността на продукционните данни в непродукционни среди. Достъпът до продукционни данни е ограничен до упълномощени потребители.

73. Финансовите институции следва да прилагат мерки за защита на целостта на изходните кодове на ИКТ системите, които са разработени в рамките на институцията. Те следва също да документират разработването, внедряването, функционирането и/или конфигурирането на ИКТ системите изчерпателно, за да бъде намалена всякаква ненужна зависимост от експерти по тематиката. Документирането на ИКТ системата следва да съдържа, когато е относимо, най-малкото документация за потребителя, техническа документация за системата и оперативни процедури за работа.

74. Процесите на финансовата институция за придобиване и разработване на ИКТ системи следва да бъдат прилагани и за ИКТ системи, разработени или управлявани от крайните потребители с бизнес функция извън ИКТ организацията (напр. приложни програми за крайни потребители), като се използва основан на риска подход. Финансовата институция следва да поддържа регистър на тези приложни програми, които подпомагат изпълнението на критични бизнес функции или процеси.

1.6.3. Управление на промените в ИКТ

75. Финансовите институции следва да установят и прилагат процес за управление на промени в ИКТ, за да гарантират, че всички промени в ИКТ системите се записват, тестват, оценяват, одобряват, прилагат и потвърждават по контролиран начин. Финансовите институции следва да се справят с промените по време на извънредни ситуации (т.е. промени, които трябва да бъдат въведени възможно най-бързо), следвайки процедури, осигуряващи адекватни предпазни механизми.

76. Финансовите институции следва да определят дали промените в съществуващата оперативна среда влияят на съществуващите мерки за сигурност или изискват приемането на допълнителни мерки за редуциране на относимите рискове. Тези промени следва да бъдат в съответствие с формалния процес за управление на промени на финансовите институции.

1.7. Управление на непрекъсваемостта на дейността

77. Финансовите институции следва да установят надежден процес за управление на непрекъсваемостта на дейността (УНД) с цел максимално да увеличат възможностите си за непрекъснато предоставяне на услуги и ограничаване на загубите в случай на сериозно прекъсване на дейността в съответствие с член 85, параграф 2 от Директива 2013/36/ЕС и Дял VI от Насоките на ЕБО относно вътрешното управление (EBA/GL/2017/11).

1.7.1. Анализ на въздействието върху дейността

78. Като част от надеждното управление на непрекъсваемостта на дейността финансовите институции следва да извършват анализ на въздействието върху дейността (АВД), като анализират доколко дейността им е изложена на сериозни смущения и оценяват потенциалното им въздействие (включително относно поверителността, целостта и наличността), количествено и качествено, като използват вътрешни и/или външни данни (например данни за трети страни, имащи отношение към определен бизнес процес или публично достъпни данни, които могат да бъдат от значение за АВД), както и сценариен анализ. В АВД следва също така да бъде отчитана критичността на идентифицираните и класифицираните бизнес функции, подпомагащите процеси, третите страни и информационните активи, както и техните взаимозависимости, в съответствие с раздел 1.3.3.

79. Финансовите институции следва да гарантират, че техните ИКТ системи и ИКТ услуги са проектирани и приведени в съответствие с техния АВД, например с резерв от някои критични компоненти, за предотвратяване на прекъсвания, причинени от събития, оказващи въздействие върху тези компоненти.

1.7.2. Планиране на непрекъсваемостта на дейността

80. Въз основа на своите АВД финансовите институции следва да изготвят планове за осигуряване на непрекъсваемост на дейността (планове за непрекъсваемост на дейността, ПНД), които следва да бъдат документирани и одобрени от техните ръководни органи. В плановете следва специално да бъдат разглеждани рисковете, които биха могли да окажат неблагоприятно въздействие върху ИКТ системите и ИКТ услугите. Плановете следва да подпомагат целите за защита и, ако е необходимо, за възстановяване на поверителността, целостта и наличността на техните бизнес функции, подпомагащи процеси и информационни активи. При разработването на тези планове финансовите институции следва да се координират със съответните вътрешни и външни заинтересовани страни, по целесъобразност.

81. Финансовите институции следва да въведат ПНД, за да се гарантира, че те могат да реагират подходящо на възможни сценарии за прекъсване на определена дейност и да бъдат способни да възстановят операциите по свои критични бизнес дейности след прекъсвания в рамките на целеви срок за възстановяване (ЦСВ, максималното време, в рамките на което дадена система или процес трябва да бъдат възстановени след инцидент) и целеви момент на възстановяване (ЦМВ, максималният времеви период, за който е приемливо да бъдат загубени данни, в случай на инцидент). В случай на сериозни сътресения в дейността, които водят до активиране на конкретни планове за непрекъсваемост на дейността, финансовите институции следва да приоритизират действията за непрекъсваемост на дейността, прилагайки основан на риска подход, който може да бъде основан на оценките на риска, извършени съгласно раздел 1.3.3. За ДПУ, това може да включва, например, улесняване на по-нататъшната обработка на критични трансакции, докато усилията за възстановяване продължават.

82. Финансовата институция следва да разгледа набор от различни сценарии в своя ПНД, включително силно утежнени, но правдоподобни хипотези, на които тя би могла да бъде изложена, включително сценарии на кибератаки, и следва да оцени потенциалното въздействие на тези сценарии. Въз основа на тези сценарии, финансовата институция следва да опише как се осигурява непрекъсваемостта на ИКТ системите и услугите, както и информационната сигурност на финансовата институция.

1.7.3. Планове за реакция и възстановяване

83. Въз основа на АВД (точка 78) и на правдоподобните сценарии (точка 82), финансовите институции следва да разработят планове за реакция и възстановяване. В тези планове следва да бъде уточнено какви условия биха могли да провокират задействане на плановете и какви действия следва да бъдат предприемани, за да се гарантират наличността, непрекъсваемостта и възстановяването поне на критично важните ИКТ системи и ИКТ услуги на финансовите институции. Плановете за реакция и възстановяване следва да бъдат насочени към постигане на целите за възстановяване на операциите на финансовите институции.

84. В плановете за реакция и възстановяване следва да бъдат взети предвид както краткосрочни, така и дългосрочни варианти за възстановяване. Плановете следва:

    а) да бъдат съсредоточени върху възстановяване на операциите на критични бизнес функции, подпомагащи процеси, информационни активи и техните взаимозависимости, за да бъдат избегнати неблагоприятни въздействия върху функционирането на финансовите институции и върху финансовата система, включително върху платежни системи и потребители на платежни услуги, както и да се гарантира изпълнението на незавършени платежни трансакции;

    б) да бъдат документирани и предоставени на разположение на бизнес и помощните звена и да бъдат лесно достъпни в случай на извънредна ситуация;

в) да бъдат актуализирани в съответствие с поуките, извлечени от инциденти, тестове, установени нови рискове и заплахи, и променени цели и приоритети по отношение на възстановяването.

85. В плановете следва също да бъдат взети предвид алтернативни варианти, при които възстановяването може да не е осъществимо в краткосрочен план поради разходи, рискове, логистика или непредвидени обстоятелства.

86. Освен това, като част от плановете за реакция и възстановяване, финансовата институция следва да обмисли и приложи мерки за осигуряване на непрекъсваемост, с цел намаляване на вреди при неизпълнение от страна на доставчици — трети страни, които са от ключово значение за непрекъсваемостта на ИКТ услугите на финансовата институция (в съответствие с разпоредбите на Насоките на ЕБО за възлагане на дейности на външни изпълнители (EBA/GL/2019/02) във връзка с плановете за непрекъсваемост на дейността).

1.7.4. Тестване на планове

87. Финансовите институции следва периодично да тестват своите ПНД. По-специално те следва да гарантират, че ПНД на техните критични бизнес функции, подпомагащи процеси, информационни активи и техните взаимозависимости (включително онези, предоставени от трети страни, когато е относимо) ще бъдат тествани най-малко веднъж годишно в съответствие с точка 89.

88. ПНД следва да бъдат актуализирани поне веднъж годишно, въз основа на резултатите от тестовете, сведенията относно съществуващи текущи заплахи и поуките, извлечени от предишни събития. Всякакви изменения относно целите на възстановяването (включително ЦСВ и ЦМВ) и/или промени в бизнес функции, подпомагащи процеси и информационни активи, също следва да бъдат взети предвид, когато е относимо, като основа за актуализиране на ПНД.

89. Тестването от страна на финансовите институции на техните ПНД следва да покаже, че те са в състояние да поддържат жизнеспособността на своите дейности до възстановяване на критичните операции. По-специално, те следва:

а) да включват тестване на подходящ набор от силно утежнени, но правдоподобни сценарии, включително онези, които са взети предвид при разработването на ПНД (както и тестване на услуги, предоставяни от трети страни, когато е приложимо); това следва да включва прехвърлянето на критични бизнес функции, подпомагащи процеси и информационни активи, към средата за възстановяване при бедствие и доказване, че те могат да бъдат изпълнявани по този начин в рамките на достатъчно представителен период от време, както и че след това нормалното функциониране може да бъде възстановено;

б) да бъдат проектирани така, че да подлагат на съмнение предположенията, на които се основават ПНД, включително рамката за управление и плановете за комуникация при извънредни ситуации; и

в) да включват процедури за проверка на способностите на техните служители и изпълнители по договори, ИКТ системи и ИКТ услуги да реагират адекватно на сценариите, определени в точка 89, буква а).

90. Резултатите от тестовете следва да бъдат документирани и всички установени недостатъци, произтичащи от тестовете, следва да бъдат анализирани, разгледани и докладвани на ръководния орган.

1.7.5. Комуникация при кризи

91. В случай на прекъсване или извънредна ситуация, както и по време на изпълнението на ПНД, финансовите институции следва да гарантират, че разполагат с ефективни мерки за комуникация при кризи, така че всички относими вътрешни и външни заинтересовани страни, включително компетентните органи, когато това се изисква от националните регулации, както и съответните доставчици (външни изпълнители, лица от групата или трети страни - доставчици) да бъдат информирани своевременно и по подходящ начин.

1.8. Управление на връзките с ползвателите на платежни услуги

92. Доставчиците на платежни услуги следва да въведат и прилагат процеси за повишаване на осведомеността на ППУ относно рисковете за сигурността, свързани с платежните услуги, като предоставят на ППУ помощ и насоки.

93. Помощта и насоките, предлагани на ППУ, следва да бъдат актуализирани в контекста на нови заплахи и уязвимости, а ППУ следва да бъдат уведомявани относно промените.

94. Когато функционалността на продукта позволява, ДПУ следва да дават възможност на ППУ да деактивират специфични функционалности за разплащане, свързани с платежните услуги, предоставяни от ДПУ на ППУ.

95. Когато в съответствие с член 68, параграф 1 от Директива (ЕС) 2015/2366 ДПУ е одобрил ограничения за разходи на платеца при платежни трансакции, осъществявани чрез конкретни платежни инструменти, ДПУ следва да предостави на платеца опцията да регулира тези ограничения до максималния договорен лимит.

96. Доставчиците на платежни услуги следва да предоставят на ППУ възможността да получават известия относно инициирани и/или неуспешни опити за иницииране на платежни трансакции, с което да им дадат възможност да откриват неправомерно или злонамерено използване на техни сметки.

97. Доставчиците на платежни услуги следва да информират ППУ относно актуализациите на процедури по сигурността, които засягат ППУ във връзка с предоставянето на платежни услуги.

98. ДПУ следва да предоставят на ППУ помощ по всякакви въпроси, искания за помощ и известия за аномалии или въпроси, засягащи сигурността на платежните услуги. ППУ следва да бъдат подходящо информирани как могат да получават такава помощ.