EBA/GL/2017/05

11/09/2017

Насоки

Насоки за оценка на риска в областта на информационните и комуникационните технологии (ИКТ) в рамките на процеса на надзорен преглед и оценка (ПНПО)

1. Спазване на насоките задълженията за докладване

Статут на насоките

1. Този 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 правото на Съюза следва да се прилага в дадена област. Компетентните органи, както са дефинирани в член 4, параграф 2 от Регламент (ЕС) № 1093/2010, 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 отчетност

3. Съгласно член 16, параграф 3 от Регламент (ЕС) № 1093/2010, най-късно до 13.09.2017 компетентните органи са длъжни да уведомят ЕБО дали спазват или възнамеряват да спазват тези насоки, в противен случай - за причините за неспазване. При липса на уведомление в този срок ЕБО счита, че компетентните органи не спазват изискването за отчетност. Уведомленията трябва да се изпратят чрез подаване на формата, намираща се на уебсайта на ЕБО, на адрес compliance@eba.europa.eu, като се посочи референтен номер ‘EBA/GL/2017/05’. Уведомленията следва да се подават 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 отчита пред ЕБО.

4. Уведомленията се публикуват на уебсайта на ЕБО в съответствие с член 16, параграф 3.

[1] Регламент (ЕС) № 1093/2010 на Европейския парламент и на Съвета от 24 ноември 2010 година 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).

2. Предмет, обхват и определения

Предмет и обхват на прилагане

5. Настоящите насоки, изготвени съгласно член 107, параграф 3 от Директива 2013/36/ЕС[2], имат за цел да гарантират сближаването на надзорните практики при оценката на риска за информационните и комуникационните технологии (ИКТ) в рамките на процеса на надзорен преглед и оценка (ПНПО), посочен в член 97 от Директива 2013/36/ЕС и допълнително уточнен в Насоките на ЕБО относно общите процедури и методологии за процеса на надзорен преглед и оценка (ПНПО)[3]. По-конкретно, настоящите насоки определят критериите за оценка, които следва да прилагат компетентните органи при надзорната оценка на управлението и стратегията на институциите по отношение на ИКТ, както и надзорната оценка на експозициите и контролните механизми по отношение на риска за ИКТ на институциите. Насоките съставляват неразделна част от Насоките на ЕБО относно ПНПО.

6. Компетентните органи следва да прилагат настоящите Насоки в съответствие с нивото на прилагане на ПНПО, посочено в Насоките на ЕБО относно ПНПО, и в съответствие с модела на минимална ангажираност и изискванията за пропорционалност, установени в него.

Адресати

7. Насоките са предназначени за компетентните органи, както са определени в член 4, параграф 2, подточка i) от Регламент (ЕС) № 1093/2010.

Определения

8. Освен ако не е посочено друго, термините, използвани и дефинирани в Директива 2013/36/ЕС, Регламент (ЕС) № 575/2013 и определенията от Насоките на ЕБО относно ПНПО, имат същото значение в настоящите насоки. В допълнение, за целите на настоящите насоки се прилагат следните определения:

ИКТ системи	Създаване на ИКТ като част от механизъм или взаимосвързваща мрежа, които подпомагат дейността на институция.
ИКТ услуги	Услуги, предоставяни от ИКТ системи на един или повече

[2] Директива 2013/36/ЕС на Европейския парламент и на Съвета от 26 юни 2013 година относно достъпа до осъществяването на дейност от кредитните институции и относно пруденциалния надзор върху кредитните институции и инвестиционните посредници, за изменение на Директива 2002/87/ЕО и за отмяна на Директиви 2006/48/ЕО и 2006/49/ЕО (1) — ОВ L 176, 27.6.2013 г.

[3] Насоки 2014/13 на ЕБО

	вътрешни или външни потребители. Примерите включват въвеждане на данни, съхранение на данни, обработка на данни и услуги за отчитане, както и услуги за наблюдение, подпомагане на бизнеса и вземане на решения.
Риск за достъпа и непрекъсваемостта на ИКТ	Рискът от неблагоприятно въздействие върху функционирането и достъпа на ИКТ системи и данни, включително неспособността за своевременно възстановяване на услугите на институцията поради неизправности в хардуерните или софтуерните компоненти на ИКТ; слабости в управлението на ИКТ системите; или всяко друго събитие, както е обяснено подробно в приложението.
Риск за сигурността на ИКТ	Рискът от неразрешен достъп до ИКТ системи и данни в или извън институцията (напр. кибератаки), както е обяснено подробно в приложението.
Риск от промени в ИКТ	Рискът, произтичащ от неспособността на институцията да управлява своевременно и контролирано промените в системата на ИКТ, по-специално по отношение на големи и сложни промени в програмите, както е обяснено подробно в приложението.
Риск за целостта на ИКТ данните	Рискът, че данните, съхранявани и обработвани от ИКТ системи, са непълни, неточни или несъответстващи на различните ИКТ системи, например в резултат на слаби или липсващи механизми за контрол на ИКТ по време на различните етапи от жизнения цикъл на ИКТ данните (т.е. проектиране на архитектурата на данните, изграждане на модела с данните и/или речниците на данни, проверка на входящите данни, контролиране на извличането, прехвърлянето и обработката на данните, включително изходящите данни), които нарушават способността на дадена институция да предоставя услуги и да осъществява управление (на риска) и на финансовата информация по подходящ и своевременен начин, както е обяснено подробно в приложението.
Риск от изнасяне на дейност, свързана с ИКТ	Рискът, че привличането на трета страна или друга структура от групата (изнасяне на дейност в рамките на групата) за предоставяне на ИКТ системи или свързани с тях услуги ще окаже неблагоприятно въздействие върху работата на институцията и управлението на риска, както е обяснено подробно в приложението.

3. Въвеждане

Дата на прилагане

9. Настоящите насоки се прилагат от 1 януари 2018 г.

4. Изисквания за оценка на риска за ИКТ

Дял 1 — Общи разпоредби

10. Компетентните органи следва да извършват оценката на риска за ИКТ и договореностите за управление и стратегията за ИКТ като част от процеса на ПНПО в съответствие с модела на минимална ангажираност и критериите за пропорционалност, определени в дял 2 от Насоките на ЕБО относно ПНПО. По-конкретно, това означава, че:

    а) честотата на оценката на риска за ИКТ би зависила от модела на минимална ангажираност, според определената категория на институцията по ПНПО, както и специфичната за нея програма за извършване на надзорни проверки; и

    б) дълбочината, детайлите и интензивността на оценката на ИКТ следва да бъдат пропорционални на размера, структурата и оперативната среда на институцията, както и на естеството, мащаба и сложността на нейните дейности.

11. Принципът на пропорционалност се прилага в настоящите насоки по отношение на обхвата, честотата и интензивността на надзорните ангажименти и диалога с институцията и надзорните изисквания за стандартите, които институцията следва да покрива.

12. Компетентните органи могат да използват и да вземат под внимание работата, която вече е извършена от институцията или от компетентния орган в контекста на оценката на други рискове или елементи на ПНПО за извършване на актуализация на оценката. По-конкретно, при извършването на оценките, посочени в настоящите насоки, компетентните органи следва да изберат най-подходящия подход за надзорна оценка и методологията, която е най-подходяща и пропорционална за институцията, като компетентните органи следва да използват съществуващата и налична документация (напр. относимите доклади и други документи, срещи със съответните лица, ангажирани с функцията управление на риска, резултати от инспекции на място), за да предоставят информация за оценката на компетентните органи.

13. Компетентните органи следва да обобщят констатациите от своите оценки на критериите, посочени в настоящите насоки, и да ги използват, за да направят заключения относно оценката на елементите на ПНПО, както е посочено в Насоките на ЕБО относно ПНПО.

14. По-конкретно, оценката на управлението и стратегията за ИКТ, извършена в съответствие с дял 2 от настоящите насоки, следва да доведе до констатации, които се вземат предвид при обобщаването на констатациите от оценката на вътрешното управление и елементи на механизмите за контрол на ПНПО в рамките на институцията, както е посочено в дял 5 от насоките на ЕБО относно ПНПО, както и да бъдат отразени в съответната оценка на този елемент на ПНПО. Освен това компетентните органи следва да имат предвид, че всяко значително неблагоприятно

въздействие на оценката на стратегията за ИКТ върху бизнес стратегията на институцията или всякакви опасения, че институцията може да не разполага с достатъчно ИКТ ресурси и ИКТ възможности за изпълнение и подкрепа на важни планирани стратегически промени, трябва се отрази при анализа на бизнес модела, извършен в съответствие с дял 4 от Насоките на ЕБО относно ПНПО.

15. Резултатът от оценката на риска за ИКТ, посочен в дял 3 от настоящите насоки, следва да се отрази при заключенията от оценката на операционния риск и следва да се разглежда като фактор за съответния резултат, както е посочено в дял 6.4 от Насоките на ЕБО относно ПНПО.

16. Трябва да се има предвид, че въпреки че компетентните органи като цяло оценяват подкатегориите рискове като част от основните категории (т.е. рискът за ИКТ ще бъде оценен като част от операционния риск), когато компетентните органи разглеждат някои подкатегории като съществени, те могат да ги оценяват на индивидуална основа. За тази цел, ако рискът за ИКТ е идентифициран като съществен риск от компетентния орган, настоящите насоки съдържат таблица за оценка (Таблица 1), която следва да се използва за определяне на самостоятелна оценка за подкатегория риск за ИКТ вследствие на цялостния подход за оценяване на рисковете за капитала в Насоките на ЕБО относно ПНПО.

17. За да се прецени дали рискът за ИКТ трябва да се счита за съществен и поради това има вероятност да бъде оценен и определен като отделна подкатегория на операционния риск, компетентните органи могат да използват критериите, посочени в раздел 6.1 от Насоките на ЕБО относно ПНПО.

18. При прилагането на настоящите насоки компетентните органи следва, когато е уместно, да вземат предвид неизчерпателния списък подкатегориите и рисковите сценарии, свързани с ИКТ риска, посочени в приложението, като вземат под внимание факта, че приложението акцентира върху рисковете за ИКТ, които могат да доведат до загуби с голяма тежест. Компетентните органи могат да изключат някои от рисковете за ИКТ, включени в таксономията, ако не съответстват на тяхната оценка. От институциите се очаква да поддържат собствени таксономии за риска, вместо да използват таксономията за риска за ИКТ, посочена в приложението.

19. В случай че настоящите насоки се прилагат по отношение на трансгранични банкови групи и техните дружества и е създадена надзорна колегия, ангажираните компетентни органи следва, в контекста на сътрудничеството си за оценка на ПНПО в съответствие с раздел 11.1 от Насоките на ЕБО относно ПНПО, да координират в максимална възможна степен точния и подробен обхват на всеки информационен елемент по последователен начин за всички дружества от групата.

Дял 2 — Оценка на управлението и стратегията на институциите за ИКТ

2.1 Общи принципи

20. Компетентните органи следва да преценят дали общото управление и рамката за вътрешен контрол на институцията надлежно обхващат ИКТ системите и свързаните с тях рискове и дали ръководният орган разглежда и управлява по подходящ начин тези аспекти, тъй като ИКТ са неразделна част от правилното функциониране на институцията.

21. При извършването на тази оценка компетентните органи следва да се позовават на изискванията и стандартите за добро вътрешно управление и на мерките за контрол на риска, посочени в Насоките на ЕБО относно вътрешното управление (GL 44)[4] и в международните насоки в тази област, доколкото те са приложими предвид спецификата на системите и рисковете за ИКТ.

22. Оценката в настоящия дял не обхваща специфичните елементи на управлението на ИКТ системата, управлението на риска и механизмите за контрол, насочени към управлението на специфични рискове за ИКТ, разгледани в дял 3 от настоящите насоки, но акцентира върху следните области:

    а) стратегия за ИКТ — дали институцията има стратегия за ИКТ, която се управлява по подходящ начин и съответства на бизнес стратегията на институцията;

    б) цялостност на вътрешното управление — дали общите механизми за вътрешно управление на институцията са подходящи по отношение на ИКТ системите в институцията; и

    в) риск за ИКТ в рамката за управление на риска на институцията — дали управлението на риска на институцията и рамката за вътрешен контрол защитават по подходящ начин ИКТ системите на институцията.

23. Буква а), посочена в параграф 22, която предоставя информация за елементите на управление на институцията, следва да се използва основно за оценката на бизнес модела, разгледана в дял 4 от Насоките на ЕБО относно ПНПО. Букви б) и в) допълват оценките на темите, обхванати от дял 5 от Насоките на ЕБО относно ПНПО, и оценката, описана в настоящите Насоки, следва да се използва в съответната оценка съгласно дял 5 от Насоките на ЕБО относно ПНПО.

24. Резултатът от тази оценка следва да дава информация, когато е уместно, за оценката на управлението на риска и на механизмите за контрол в дял 3 от настоящите насоки.

[4] Насоки на ЕБО относно вътрешното управление, GL 44, 27 септември 2011 г.

2.2 Стратегия за ИКТ

25. В рамките на този раздел компетентните органи следва да преценят дали институцията разполага със стратегия за ИКТ: която подлежи на адекватен надзор от ръководния орган на институцията; която е в съответствие с бизнес стратегията, особено за поддържане на ИКТ актуални и за планиране или прилагане на важни и сложни промени в ИКТ; и която подпомага бизнес модела на институцията.

2.2.1 Разработване на стратегия и адекватност на ИКТ

26. Компетентните органи следва да оценят дали институцията разполага с рамка, пропорционална на естеството, мащаба и сложността на своите ИКТ дейности, за подготовката и развитието на стратегията за ИКТ в институцията. При извършването на оценката компетентните органи трябва да отчетат дали:

    а) висшето ръководство [5] на бизнес линиите е включено по подходящ начин в определянето на стратегическите приоритети на институцията в областта на ИКТ и на свой ред висшето ръководство на ИКТ функцията е наясно с разработването, проектирането и иницииране на важни бизнес стратегии и инициативи за гарантиране на непрекъснато съгласуване между ИКТ системите, ИКТ услугите и ИКТ функцията (т.е. лицата, които отговарят за управлението и внедряването на тези системи и услуги) и бизнес стратегията на институцията, както и дали ИКТ са ефективно актуализирани;

    б) стратегията в областта на ИКТ е документирана и подкрепена от конкретни планове за изпълнение, по-специално по отношение на важните етапи и планирането на ресурсите (включително финансови и човешки ресурси), за да се гарантира, че те са реалистични и позволяват изпълнението на стратегията за ИКТ;

    в) институцията периодично актуализира своята стратегия за ИКТ, по-специално при промяна на бизнес стратегията, за да гарантира непрекъснато съгласуване между ИКТ и средносрочните бизнес цели с дългосрочните цели, планове и дейности; и

    г) ръководният орган на институцията одобрява стратегията за ИКТ, плановете за изпълнение и наблюдава изпълнението ѝ.

2.2.2 Изграждане на стратегия за ИКТ

27. Ако стратегията за ИКТ в институцията изисква изпълнението на важни и сложни промени в ИКТ или промени, които имат съществени последици за бизнес модела на институцията, компетентните органи следва да оценят дали институцията разполага с контролна рамка, съответстваща на нейния размер, нейните ИКТ дейности, както и на нивото на дейностите за промяна, за да спомогне за ефективното прилагане на стратегията за ИКТ в институцията. При

[5] Висше ръководство и ръководен орган, както е определено в Директива 2013/36/ЕС от 26 юни 2013 г., в член 3, параграф 7 „ръководен орган“ и член 3, параграф 9 „висше ръководство“.

извършването на тази оценка компетентните органи следва да вземат предвид дали рамката за контрол:

а) включва управленски процеси (напр. наблюдение и докладване на напредъка и бюджета) и съответните органи (напр. офис за управление на проекти, ръководна група за ИКТ или еквивалентна на нея), за да подпомогне ефективно изпълнението на стратегическите програми за ИКТ;

б) е определила и разпределила ролите и отговорностите за изпълнение на стратегическите програми за ИКТ, обръщайки специално внимание на опита на основните заинтересовани страни в организирането, управлението и наблюдението на важни и сложни ИКТ промени и управлението на по-широките организационни и човешки въздействия (напр. управление на съпротивата срещу промяна, обучение, комуникация).

в) ангажира функциите на независимия контрол и вътрешния одит, за да гарантира, че рисковете, свързани с прилагането на стратегията за ИКТ, са идентифицирани, оценени и ефективно редуцирани и че съществуващата рамка за управление на стратегията за ИКТ е ефективна; и

г) съдържа процес на планиране и преглед на планирането, който осигурява гъвкавост, за да отговори на важни установени проблеми (напр. срещани проблеми при изпълнението или закъснения) или външни събития (напр. важни промени в бизнес средата, технологични проблеми или иновации), за да се гарантира своевременно адаптиране на стратегическия план за изпълнение.

2.3 Общо вътрешно управление

28. В съответствие с дял 5 от Насоките на ЕБО относно ПНПО компетентните органи следва да преценят дали институцията има подходяща и прозрачна корпоративна структура, която е „пригодна за целта“, и дали е приложила подходящи договорености за управление. По отношение на ИКТ системите и в съответствие с Насоките на ЕБО относно вътрешното управление тази оценка следва да включва оценка дали институцията показва:

а) стабилна и прозрачна организационна структура с ясни отговорности по отношение на ИКТ, включително ръководния орган и неговите комитети, както и че основните отговорни лица за ИКТ (напр. главен директор по информационните системи („CIO“), главен оперативен директор („COO“) или еквивалентна роля) имат подходящ пряк или непряк достъп до ръководния орган, за да се гарантира, че важната информация или въпроси, свързани с ИКТ, се докладват по подходящ начин, обсъждат се и се взема решение на ниво ръководен орган; и

б) че ръководният орган знае и взема мерки за преодоляване на рисковете, свързани с ИКТ;

29. В допълнение към раздел 5.2 от Насоките на ЕБО относно ПНПО компетентните органи следва да преценят дали политиката и стратегията на институцията за изнасяне на дейности, свързани с ИКТ вземат предвид, когато е относимо, въздействието на изнесените дейности в областта на ИКТ върху бизнеса и бизнес модела на институцията.

2.4 Риск за ИКТ в рамката за управление на риска на институцията

30. При оценката на управлението на риска и вътрешните механизми за контрол на институцията, прилагани в рамките на институцията, както е предвидено в дял 5 от Насоките на ЕБО относно ПНПО, компетентните органи следва да преценят дали рамката за управление на риска на институцията и вътрешния контрол защитава ИКТ системите на институцията по подходящ начин, който съответства на размера и дейностите на институцията и на нейния рисков профил по отношение на ИКТ, както е определено в дял 3. По-конкретно, компетентните органи следва да определят дали:

    а) склонността към поемане на риск и процесът за вътрешна оценка на адекватността на капитала (ВААК) обхващат рисковете за ИКТ като част от по-широката категория на операционния риск за дефиниране на цялостната стратегия за риска и определяне на вътрешния капитал; и

    б) рисковете за ИКТ са в обхвата на рамките за управление на риска и вътрешния контрол на цялата институция.

31. Компетентните органи следва да извършат оценката съгласно буква а) по-горе, като вземат предвид както очакваните, така и неблагоприятните сценарии, например сценариите, включени в специфичния за институцията или надзорния стрес тест.

32. По отношение на буква б), компетентните органи следва да оценят дали функциите на независимия контрол и вътрешен одит, посочени в параграф 104, буква а), параграф 104, буква г), параграф 105, буква а) и параграф 105, буква в) от Насоките на ЕБО относно ПНПО, са подходящи за гарантиране на достатъчно ниво на независимост между ИКТ и функциите за контрол и одит, като се има предвид големината и рисковият профил по отношение на ИКТ на институцията.

2.5 Резюме на констатациите

33. Тези резултати следва да бъдат отразени в обобщението на констатациите по дял 5 от Насоките на ЕБО относно ПНПО и следва да бъдат част от съответното оценяване в съответствие със съображенията, посочени в таблица 3 от Насоките на ЕБО относно ПНПО.

34. За оценката на стратегията за ИКТ трябва да се вземе предвид следното при извършването на горната оценка:

    а) ако компетентните органи стигнат до заключението, че рамката за управление на институцията е неподходяща за разработването и прилагането на стратегията за ИКТ на институцията в съответствие с раздел 2.2, тогава това следва да намери отражение в оценката на вътрешното управление на институцията в дял 5 от Насоките на ЕБО относно ПНПО в точка 87, буква а);

    б) ако компетентните органи стигнат до извода от горните оценки в раздел 2.2, че ще има значително отклонение между стратегията за ИКТ и бизнес стратегията, което може да има значително неблагоприятно въздействие върху дългосрочните бизнес и/или финансови цели на институцията, устойчивостта на институцията и/или бизнес модела

или областите/видовете бизнес на институцията, които са определени като най-съществени в параграф 62, буква а) от Насоките на ЕБО относно ПНПО, това следва да намери отражение в оценката на бизнес модела в дял 4 от Насоките относно ПНПО в точка 70, буква б) и точка 70, буква в); и

в) ако компетентните органи стигнат до извода от горните оценки в раздел 2.2, че институцията може да няма достатъчно ИКТ ресурси и възможности за внедряване на ИКТ за изпълнение и подкрепа на важни планирани стратегически промени, това би трябвало да намери отражение в оценката на бизнес модела в дял 4 от Насоките на ЕБО относно ПНПО в точка 70, буква б).

Дял 3 — Оценка на експозицията и механизмите за контрол на рисковете, свързани с ИКТ

3.1 Общи положения

35. Компетентните органи следва да преценят дали институцията е идентифицирала, оценила и редуцирала надлежно рисковете, свързани с ИКТ. Този процес трябва да бъде част от рамката за управление на операционния риск и да съответства на подхода, приложим към операционния риск.

36. Компетентните органи първо трябва да идентифицират съществените присъщи рискове за ИКТ, на които институцията е или може да бъде изложена, последвано от оценка на ефективността на рамката, процедурите и механизмите за контрол на институцията за управление на рисковете за ИКТ с цел редуциране на тези рискове. Резултатът от оценката трябва да бъде отразен в обобщение на констатациите, което се използва в оценката на операционния риск съгласно Насоките относно ПНПО. Когато рискът за ИКТ се счита за съществен и компетентните органи желаят да определят индивидуален резултат, тогава таблица 1 следва да се използва за определяне на оценка като рискова подкатегория на операционния риск.

37. При извършване на оценката съгласно настоящия дял компетентните органи следва да използват всички налични източници на информация, както е посочено в параграф 127 от дял 6 от Насоките за ЕБО за ПНПО, например дейностите по управление на риска на институцията, отчитането и резултатите, като основа за определяне на приоритетите на тяхната надзорна оценка. Компетентните органи следва да използват и други източници на информация за извършване на тази оценка, включително следното, където е уместно:

    а) самооценка на рисковете и механизмите за контрол за ИКТ (ако е предоставена в информацията за процеса за вътрешна оценка на адекватността на капитала (ВААК);
    б) свързаната с ИКТ управленска информация (УИ), предоставена на ръководния орган на институцията, например периодично и произтичащо от инциденти докладване на риска за ИКТ (включително в базата данни за загубите от операционен риск), данни за рисковата експозиция към ИКТ от функцията на управлението на риска на институцията;
    в) свързаните с ИКТ констатации от вътрешния и външния одит, които се докладват на одитния комитет на институцията.

3.2 Идентифициране на съществени рискове за ИКТ

38. Компетентните органи следва да идентифицират съществените рискове за ИКТ, на които институцията е или би могла да бъде изложена, като следват стъпките по-долу.

3.2.1 Преглед на рисковия профил на ИКТ в институцията

39. При прегледа на рисковия профил на институцията в областта на ИКТ компетентните органи следва да разгледат цялата относима информация относно рисковите експозиции на институцията по отношение на рисковете за ИКТ, включително информацията по параграф 37, и установените съществени недостатъци или слабости в организацията на ИКТ и механизмите за контрол на цялата институция съгласно дял 2 от настоящите насоки, и когато е уместно, преразглеждане на тази информация по пропорционален начин. Като част от този преглед компетентните органи следва да разгледат:

а) потенциалното въздействие на значително прекъсване на ИКТ системите на институцията върху финансовата система на национално или международно равнище;

б) дали институцията може да бъде обект на рискове за сигурността на ИКТ или на рискове за достъпа и непрекъсваемостта на ИКТ, дължащи се на зависимостта от интернет, приемане на новаторски ИКТ решения или други бизнес канали за дистрибуция, които биха могли да я направят по-вероятна цел за кибератаки;

в) дали институцията може да бъде в изложена в по-голяма степен на рискове за сигурността на ИКТ, рискове за достъпа и непрекъсваемостта на ИКТ, рискове за целостта на ИКТ данните или рискове от промени в ИКТ поради сложността (напр. в резултат на сливания или придобивания) или моралното остаряване на нейните ИКТ системи;

г) дали институцията осъществява съществени промени в своите ИКТ системи и/или ИКТ функции (напр. в резултат на сливания, придобивания, продажби или замяна на основните си ИКТ системи), което може да окаже неблагоприятно въздействие върху стабилността или правилното функциониране на ИКТ системите и може да доведе до съществени рискове за достъпа и непрекъсваемостта на ИКТ, рискове за сигурността на ИКТ, рискове от промяна на ИКТ или рискове за целостта на ИКТ данните;

д) дали институцията е изнесла дейности, свързани с нейните ИКТ услуги или ИКТ системи в рамките на групата или извън нея, които могат да я изложат на съществени рискове, свързани с изнесените дейности в областта на ИКТ;

е) дали институцията прилага агресивни мерки за намаляване на разходите за ИКТ, които могат да доведат до намаляване на необходимите инвестиции в ИКТ, ресурси и експертни познания в областта на информационните технологии и могат да увеличат експозицията на всички видове рискове за ИКТ в таксономията;

ж) дали местоположението на важни ИКТ операции/центрове за данни (напр. региони, страни) може да изложи институцията на природни бедствия (напр. наводнения, земетресения), политическа нестабилност или трудово-правни конфликти и граждански вълнения, които могат да доведат до съществено увеличение на рисковете за достъпа и непрекъсваемостта на ИКТ и рисковете за сигурността на ИКТ.

3.2.2 Преглед на критичните ИКТ системи и услуги

40. Като част от процеса за идентифициране на рисковете за ИКТ с потенциално значимо пруденциално въздействие върху институцията, компетентните органи следва да преразгледат документацията от институцията и да формулират становище относно това кои ИКТ системи и

услуги са от решаващо значение за адекватното функциониране, достъп, непрекъсваемост и сигурност на основните дейности на институцията.

41. За тази цел компетентните органи следва да преразгледат методологията и процесите, прилагани от институцията за идентифициране на критичните ИКТ системи и услуги, като се има предвид, че някои ИКТ системи и услуги може да се считат за критични от институцията от гледна точка на непрекъсваемост на дейността и достъпа, сигурността (напр. предотвратяване на измами) и/или поверителността (напр. поверителни данни). При извършването на прегледа компетентните органи следва да вземат предвид, че критичните ИКТ системи и услуги трябва да изпълняват поне едно от следните условия:

    а) те поддържат основните бизнес дейности и канали за разпространение (напр. банкомати, интернет и мобилно банкиране) на институцията;

    б) те поддържат съществени управленски процеси и корпоративни функции, включително управление на риска (напр. системи за управление на риска и системи за управление на касовите наличности);

    в) към тях се прилагат към специални правни или регулаторни изисквания (ако има такива), които налагат повишени изисквания за достъп, устойчивост, поверителност или сигурност (напр. законодателство за защита на данните или възможни „цели за времето на възстановяване“ (RTO, максималният срок, в който трябва да бъде възстановена дадена система или процес след инцидент) и „Цел за момент на възстановяване“ (RPO, максималният период, през който данните могат да бъдат загубени в случай на инцидент) за някои системно важни услуги (ако и когато е приложимо);

    г) те обработват или съхраняват поверителни или чувствителни данни, неразрешеният достъп до които може значително да повлияе на репутацията на институцията, финансовите резултати или стабилността и непрекъсваемостта на нейната дейност (напр. бази данни с чувствителна информация за клиентите); и/или

    д) те предоставят базисни функционалности, които са жизненоважни за адекватното функциониране на институцията (напр. телекомуникационни услуги и услуги за свързване, услуги за сигурност на ИКТ и кибернетична сигурност).

3.2.3 Идентифициране на съществените рискове за ИКТ за критичните ИКТ системи и услуги

42. Като се вземат предвид извършените проверки на рисковия профил на ИКТ на институцията и критичните ИКТ системи и услуги, посочени по-горе, компетентните органи следва да изготвят становище за съществените рискове за ИКТ, които според тяхната надзорна преценка могат да окажат значително пруденциално въздействие върху критичните ИКТ системи и услуги на институцията.

43. Когато оценяват потенциалното въздействие на рисковете за ИКТ върху критичните ИКТ системи и услуги на дадена институция, компетентните органи следва да разгледат:

    а) финансовото въздействие, включително (но не само) загуба на средства или активи, потенциални компенсации за клиентите, правни разходи и разходи за възстановяване, договорни щети, загубени приходи;

    б) възможността за прекъсване на дейността, като се има предвид (но не само) критичността на засегнатите финансови услуги; броят на потенциално засегнатите клиенти и/или клонове и служители;

    в) потенциалното въздействие върху репутацията на институцията въз основа на критичността на засегнатите банкови услуги или оперативна дейност (напр. кражба на данни за клиентите); външния профил/видимост на засегнатите ИКТ системи и услуги (напр. мобилни или онлайн банкови системи, пунктове за продажба, банкомати или платежни системи);

    г) регулаторното въздействие, включително възможността за публична критика от страна на регулатора, глоби или дори промяна на разрешенията;

    д) стратегическото въздействие върху институцията, например ако стратегическият продукт или бизнес план са компрометирани или откраднати.

44. След това компетентните органи следва да съотнесат идентифицираните рискове за ИКТ, които се считат за съществени, към посочените по-долу категории ИКТ рискове, за които в приложението са дадени допълнителни описания и примери за съответните рискове. Компетентните органи следва да вземат предвид рисковете за ИКТ в приложението като част от оценката по дял 3:

    а) риск за достъпа и непрекъсваемост на ИКТ;
    б) риск за сигурността на ИКТ;
    в) риск от промени в ИКТ;
    г) риск за целостта на ИКТ данните;
    д) риск от изнасяне на дейности, свързани с ИКТ.

    Съотнасянето има за цел да подпомогне компетентните органи при определянето на рисковете, които са съществени (ако има такива) и следователно трябва да бъдат предмет на по-тесен и/или по-задълбочен преглед на посочените нататък в документа стъпки за оценка.

3.3 Оценка на механизмите за контрол за редуциране на съществени рискове за ИКТ

45. За да оценят остатъчната експозиция на риска за ИКТ на институцията, компетентните органи следва да преразгледат начина, по който институцията идентифицира, наблюдава, оценява и редуцира съществените рискове, установени от компетентните органи в оценката по-горе.

46. За тази цел, за идентифицираните съществени рискове за ИКТ, компетентните органи следва да преразгледат приложимите:

    а) политика за управление на риска за ИКТ, процеси и прагове за допустимост на риска;

    б) организационна рамка, управление и контрол;

    в) обхват и констатации от вътрешния одит; и

    г) рискови контроли за ИКТ, специфични за идентифицирания съществен риск за ИКТ.

47. Оценката следва да вземе предвид резултатите от анализа на цялостната рамка за управление на риска и вътрешния контрол, както е посочено в дял 5 от Насоките на ЕБО, както и управлението и стратегията на институцията, разгледани в дял 2 от настоящите насоки, тъй като съществените недостатъци, установени в тези области, могат да повлияят на способността на институцията да управлява и редуцира рисковете, свързани с ИКТ. Когато е уместно, компетентните органи следва също така да използват източниците на информация в параграф 37 от настоящите насоки.

48. Компетентните органи следва да извършват следните стъпки на оценка по начин, който е пропорционален на естеството, мащаба и сложността на дейностите на институцията, и като прилагат надзорен преглед, който съответства на рисковия профил на институцията.

3.3.1 Политика за управление на риска, процеси и прагове на допустимост на риск

49. Компетентните органи следва да преценят дали институцията има подходящи политики за управление на риска, процеси и прагове за допустимост на риск за идентифицираните съществени рискове за ИКТ. Те могат да бъдат част от рамката за управление на операционния риск или отделен документ. За тази оценка компетентните органи следва да вземат предвид дали:

    а) политиката за управление на риска е формализирана и одобрена от ръководния орган и съдържа достатъчно насоки относно склонността на институцията за поемане на риск в областта на ИКТ и основните преследвани цели за управление на риска за ИКТ и/или прилаганите прагове за допустимост на риска за ИКТ; съответната политика за управление на риска за ИКТ следва също така да бъде сведена до знанието на всички заинтересовани страни;

    б) приложимата политика обхваща всички съществени елементи за управлението на риска на идентифицираните съществени рискове за ИКТ;

    в) институцията е въвела процеси и основни процедури за идентификация (напр. „Самооценки на механизмите за контрол на риска“ (RCSA), анализ на рисковите сценарии) и наблюдение на съответните съществени рискове за ИКТ; и

    г) институцията има отчетност за управление на риска за ИКТ, която осигурява навременна информация на висшето ръководство и на ръководния орган, и която дава възможност на висшето ръководство и/или на ръководния орган за оценка и наблюдение дали плановете и мерките за редуциране на риска за ИКТ на институцията са съвместими с одобрената склонност за поемане на риск и/или допустими прагове (когато е приложимо) и за наблюдение на промени в съществените рискове за ИКТ.

3.3.2 Рамка за организационно управление и контрол

50. Компетентните органи следва да оценят как приложимите роли и отговорности за управление на риска са вградени и интегрирани във вътрешната организация за управление и контрол на идентифицираните съществени рискове за ИКТ. В тази връзка компетентните органи следва да оценят дали институцията демонстрира:

а) ясни роли и отговорности за идентифициране, оценка, наблюдение, редуциране, отчитане и контрол на включения съществен риск за ИКТ;

б) отговорностите и ролите, свързани с риска, са ясно съобщени, разпределени и вградени във всички съответни части (напр. видове дейност, ИТ) и процеси на организацията, включително ролите и отговорностите за събиране и обобщаване на информацията за риска и докладването ѝ на висшето ръководство и/или на ръководния орган;

в) дейностите по управлението на риска за ИКТ се извършват с подходящи като брой и качество човешки и технически ресурси. За да се оцени надеждността на приложимите планове за редуциране на риска, компетентните органи следва да преценят дали институцията е отделила достатъчно финансови средства и/или други необходими ресурси за изпълнението им;

г) подходящо проследяване и отговор на ръководния орган във връзка с важни констатации на независимите контролни функции по отношение на риска(овете) за ИКТ, като се взема предвид възможното възлагане на някои аспекти на комитет, когато такъв съществува; и

д) изключенията от приложимите разпоредби и политики в областта на ИКТ се записват и подлежат на документиран преглед и докладване от независимата контролна функция, с акцент върху свързаните с това рискове.

3.3.3 Обхват и констатации на вътрешния одит

51. Компетентните органи следва да преценят дали функцията за вътрешен одит е ефективна по отношение на проверката на приложимата рамка за контрол на риска за ИКТ, като прави преглед дали:

а) рамката за контрол на риска за ИКТ се одитира с необходимото качество, дълбочина и честота и е съобразена с размера, дейностите и рисковия профил по отношение на ИКТ на институцията;

б) планът за одит включва одити на критичните рискове за ИКТ, установени от институцията;

в) важните констатации от одита на ИКТ, включително съгласуваните действия, се докладват на ръководния орган; и

г) одитните констатации в областта на ИКТ, включително съгласуваните действия, се проследяват и докладите за напредъка се преразглеждат периодично от висшето ръководство и/или одитния комитет.

3.3.4 Механизми за контрол на рисковете за ИКТ, които са специфични за идентифицираните съществени рискове за ИКТ

52. По отношение на идентифицираните съществени рискове за ИКТ, компетентните органи следва да преценят дали институцията има създадени специфични механизми за контрол по отношение на тези рискове. Следващите раздели съдържат неизчерпателен списък на конкретните механизми за контрол, които трябва да се вземат предвид при оценката на съществените рискове, идентифицирани в точка 3.2.3, които са разпределени в следните категории рискове за ИКТ:

а) рискове за достъпа и непрекъсваемостта на ИКТ;
б) рискове за сигурността на ИКТ;
в) рискове в следствие от промени на ИКТ;
г) рискове за целостта на ИКТ данните;
д) рискове, свързани с изнасянето на дейности в областта на ИКТ.

А) Механизми за контрол за управление на рисковете за достъпа и непрекъсваемостта на ИКТ

53. В допълнение към изискванията в Насоките на ЕБО относно ПНПО (параграфи 279—281) компетентните органи следва да оценят дали институцията има създадена подходяща рамка за идентифициране, разбиране, измерване и редуциране на рисковете за достъпа и непрекъсваемостта на ИКТ.

54. За тази оценка, компетентните органи следва по-специално да вземат предвид дали рамката:

а) идентифицира критичните процеси в областта на ИКТ и съответните поддържащи ИКТ системи, които трябва да бъдат част от плановете за бизнес устойчивост и непрекъсваемост посредством:

i. цялостен анализ на зависимостите между критичните бизнес процеси и поддържащите системи;

ii. определяне на цели за възстановяване за поддържащите ИКТ системи (напр. обикновено определяни от бизнеса и/или от нормативните разпоредби от гледна точка на целта за времето на възстановяване (RTO) и целта за момент на възстановяване (RPO);

iii. подходящи планове за действие при непредвидени обстоятелства, даващи възможност за достъп, непрекъсваемост и възстановяване на критични системи и услуги в областта на ИКТ, които да сведат прекъсването на дейностите на институцията до приемливи граници.

б) има политики и стандарти за бизнес устойчивост, за контрол на непрекъсваемостта на средата , както и оперативни контроли, които включват:

i. мерки за предотвратяване на възможността даден сценарий, инцидент или бедствие да засегнат както системите за производство, така и системите за възстановяване на ИКТ;

ii. процедури за резервно копиране и възстановяване на ИКТ системи за критичен софтуер и данни, с които се гарантира, че тези резервни копия се съхраняват на сигурно и

достатъчно отдалечено място, така че даден инцидент или природно бедствие да не могат да унищожат или повредят тези критични данни;

iii. решения за наблюдение за навременно откриване на инциденти с достъпа или непрекъсваемостта на ИКТ;

iv. процес на документирано управление на инцидентите и тяхната ескалация, който също така дава насоки относно различните роли и отговорности за управление и ескалация на инцидентите до членовете на кризисния(те) комитет(и) и на съответното управленско ниво в случай на извънредни ситуации;

v. физически мерки за защита на критичната инфраструктура на ИКТ на институцията (напр. центрове за данни) от рисковете, свързани с околната среда (напр. наводнения и други природни бедствия), както и за осигуряване на подходяща операционна среда за ИКТ системи (напр. климатична инсталация);

vi. процеси, роли и отговорности, които да гарантират, че изнесените към външни изпълнители системи и услуги в областта на ИКТ също са обхванати от подходящи решения и планове за бизнес устойчивост и непрекъсваемост;

vii. решения за планиране и наблюдение на производителността и капацитета на критични ИКТ системи и услуги с определени изисквания за достъпност, които да идентифицират своевременно важни ограничения в достъпността и капацитета;

viii. решения за защита на критични интернет дейности или услуги (напр. услуги за електронно банкиране), когато е необходимо и целесъобразно, срещу отказ на услугата и други видове кибератаки от интернет, насочени към предотвратяване или смущаване на достъпа до тези дейности и услуги;

в) тестване на решенията за достъп и непрекъсваемост на ИКТ спрямо редица реалистични сценарии, включително кибератаки, тестове за отказ поради повреда на отделни елементи и тестове за създаване на резервни копия на критичен софтуер и данни, които са:

i. планирани, формализирани и документирани, и резултатите от тестовете са използвани за повишаване на ефективността на достъпа и непрекъсваемостта на ИКТ решения;

ii. включват заинтересовани страни и функции в рамките на организацията, например управление на вид дейност, включително непрекъсваемост на дейността, екипи за реагиране при инциденти и кризи, както и съответните външни заинтересовани страни;

iii. ръководният орган и висшето ръководство са включени по подходящ начин (напр. като част от екипа за управление на кризи) и се информират за резултатите от тестовете.

Б) Контролни механизми за управление на съществените рискове за сигурността на ИКТ

55. Компетентните органи следва да оценят дали институцията има създадена ефективна рамка за идентифициране, разбиране, измерване и редуциране на риска за сигурността на ИКТ. За тази оценка компетентните органи следва по-специално да вземат предвид дали рамката включва:

а) ясно определени роли и отговорности по отношение на:

i. лицето(ата) и/или комитетите, които отговарят за ежедневното управление на сигурността на ИКТ и за разработването на общи политики за сигурност в областта на ИКТ, обръщайки внимание на независимостта, от която се нуждаят;
ii. проектирането, имплементиране, управлението и наблюдението на механизмите за контрол на сигурността в областта на ИКТ;
iii. защитата на критичните ИКТ системи и услуги, например чрез приемане на процес за оценка на уязвимостите, управление на софтуерните корекции, защита на крайните точки (напр. зловреден софтуер), инструменти за идентифициране и предотвратяване на проникване;
iv. наблюдението, класифицирането и обработката на външните или вътрешни инциденти със сигурността на ИКТ, включително реагиране на инциденти и възобновяването и възстановяването на ИКТ системите и услугите;
v. редовни и проактивни оценки на заплахите за поддържане на подходящи механизми за контрол на сигурността;

б) политика за сигурност в областта на ИКТ, която взема под внимание и, при необходимост, се придържа към международно признатите стандарти и принципи за сигурност в областта на ИКТ (напр. принципа за „най-малка привилегия“, т.е. ограничаване на достъпа до минималното ниво, което позволява нормалното функциониране за управление на правото на достъп, и принципа на „защита в дълбочина“, т.е. многопластовите механизми за сигурност увеличават сигурността на системата като цяло за проектиране на архитектура за сигурност);

в) процедура за идентифициране на ИКТ системи, услуги и съизмерими изисквания за сигурност, които отразяват потенциалния риск от измами и/или възможно неправилно използване и/или злоупотреба с поверителни данни, заедно с документирани очаквания за сигурност, които трябва да се спазват за тези идентифицирани ИКТ системи, услуги и данни, съгласувани с рисковия толеранс на институцията и следени за правилното им прилагане;

г) документирано управление на инцидентите, свързани със сигурността и на процеса на ескалация, който дава насоки за различните роли и отговорности за управление и ескалация на инцидентите, членовете на кризисния(те) комитет(и) и командната верига в случай на извънредна ситуации със сигурността;

д) регистриране на операциите на потребителите и администраторите, за да се даде възможност за ефективно наблюдение и навременно откриване и реакция при неразрешена дейност; за съдействие или за провеждане на съдебни разследвания на инциденти, свързани със сигурността. Институцията трябва да има създадени политики на регистрация,

определящи подходящите видове регистри, които трябва да се поддържат, както и техния срок на съхранение;

е) информационни кампании или инициативи за повишаване на осведомеността на всички нива в институцията относно безопасното използване и защита на ИКТ системите на институцията и основните рискове за сигурността на ИКТ, както и за (други) рискове, с които трябва да са запознати, по-специално по отношение на съществуващите и нововъзникващите кибер заплахи (напр. компютърни вируси, възможни вътрешни или външни злоупотреби или атаки, кибератаки) и тяхната роля за редуциране на нарушения на сигурността;

ж) адекватни мерки за физическа сигурност (напр. видеонаблюдение, алармена система срещу кражба, защитни врати), за да се предотврати неразрешен физически достъп до критични и чувствителни ИКТ системи (напр. центрове за данни);

з) мерки за защита на ИКТ системи от атаки от интернет (напр. кибератаки) или други външни мрежи (напр. традиционни телекомуникационни връзки или връзки с доверени партньори). Компетентните органи следва да прегледат дали рамката на институцията включва:

i. процес и решения за поддържане на пълен и актуален инвентарен опис на данните и преглед на всички насочени навън точки за мрежова връзка (напр. уебсайтове, интернет приложения, WIFI, отдалечен достъп), чрез които трети лица биха могли да проникнат във вътрешните ИКТ системи.

ii. детайлно управлявани и контролирани мерки за сигурност (напр. защитни стени, прокси сървъри, релейни сървъри за електронна поща, антивирусни програми и скенери на съдържание) за защитаване на входящия и изходящия мрежови трафик (напр. електронна поща) и насочените навън точки за мрежова връзка, чрез които трети лица биха могли да проникнат във вътрешните ИКТ системи;

iii. процеси и решения за защитаване на уебсайтове и приложения, които могат да бъдат директно атакувани от интернет и/или отвън, и които могат да служат като входяща точка във вътрешните ИКТ системи. Най-общо те включват комбинация от признатите практики за развитие на сигурността, практики за укрепване на ИКТ системите и сканиране за уязвимости и/или прилагане на допълнителни решения за сигурност, например прилагане на защитни стени и/или идентифициране на проникване (IDS) и/или системи за предотвратяване на проникванията (IPS);

iv. периодично тестване на проникването в системата за сигурност, за да се оцени ефективността на въведените кибер и вътрешни мерки и процеси за сигурност на ИКТ. Тези тестове трябва да се извършват от служители и/или външни експерти с необходимата експертиза, като документираните резултати от тестовете и заключенията се докладват на висшето ръководство и/или на управителния орган. Когато е необходимо и приложимо, институцията трябва да се обучава от тези тестове, както и да открива областите, където е необходимо подобрение в механизмите за контрол на сигурността и процесите и/или където може да се засили подсигуряването на тяхната ефективност.

В) Контролни механизми за управление на съществените рискове от промени на ИКТ

56. Компетентните органи следва да оценят дали институцията има създадена ефективна рамка за идентифициране, разбиране, измерване и редуциране на риска от промени на ИКТ, съответстваща на естеството, мащаба и сложността на дейностите на институцията и рисковия профил на ИКТ на институцията. Рамката на институцията трябва да обхваща рисковете, свързани с разработването, тестването и одобряването на промени в ИКТ системите, включително разработката или промяната на софтуера, преди да бъдат мигрирани към производствената среда, и да осигури адекватно управление на жизнения цикъл на ИКТ. За тази оценка компетентните органи следва по-специално да вземат предвид дали рамката включва:

а) документирани процедури за управление и контрол на промените в ИКТ системите (напр. конфигуриране и управление на софтуерните корекции) и данните (напр. отстраняване на грешки или корекции на данни), осигуряване на адекватно участие на управлението на рисковете за ИКТ при важни промени в ИКТ, които могат да окажат значително въздействие върху рисковия профил или експозиция на институцията;

б) спецификации по отношение на необходимото разпределение на отговорностите по време на различните етапи на процесите на промяна в областта на ИКТ (напр. проектиране и разработване на решения, тестване и одобрение на нов софтуер и/или промени, миграция и внедряване в производствената среда, както и коригиране на софтуерни дефекти), с акцент върху прилаганите решения и разпределение на отговорностите за управление и контрол на промените в системите за производство и данните за ИКТ от страна на персонала в областта на ИКТ (напр. разработчици, системни администратори на ИКТ, администратори на бази данни) или всяка друга страна (напр. бизнес потребители, доставчици на услуги);

в) тестови среди, които отразяват по подходящ начин производствените среди;

г) опис на активите, свързани със съществуващите приложения и ИКТ системи в производствената среда, както и средата за тестване и развитие, така че необходимите промени (напр. актуализиране или осъвременяване на версията, корекции на системи, промени в конфигурацията) да бъдат адекватно управлявани, прилагани и наблюдавани по отношение на включените ИКТ системи;

д) процес за наблюдение и управление на жизнения цикъл на използваните ИКТ системи, гарантиращ, че те продължават да отговарят на действителните изисквания на бизнеса и на управлението на риска, както и че използваните ИКТ решения и системи все още се поддържат от техните доставчици; и че това е придружено от адекватни процедури за разработване по време на жизнения цикъл на софтуера (SDLC);

е) система за контрол на изходния код на софтуера и подходящи процедури, които предотвратяват неразрешени промени в изходния код на софтуера, разработен в самата организация;

ж) процес за провеждане на скрининг на сигурността и уязвимостите на нови или съществено променени ИКТ системи и софтуер, преди да бъдат пуснати в производство и да бъдат изложени на евентуални кибератаки;

з) процес и решения за предотвратяване на неразрешено или непреднамерено разкриване на поверителни данни при замяна, архивиране, преустановяване на ползването или унищожаване на ИКТ системи;

и) независими процеси за преглед и валидиране за намаляване на рисковете от човешки грешки при извършване на промени в ИКТ системи, които могат да имат значителен неблагоприятен ефект върху достъпа, непрекъсваемостта или сигурността на институцията (напр. важни промени в конфигурацията на защитната стена), или в сигурността на институцията (напр. промени в защитните стени).

Г) Контролни механизми за управление на съществените рискове за целостта на ИКТ данните

57. Компетентните органи следва да оценят дали институцията има създадена ефективна рамка за идентифициране, разбиране, измерване и редуциране на рисковете за целостта на ИКТ данните в съответствие с естеството, мащаба и сложността на дейностите на институцията и рисковия профил на ИКТ на институцията. Рамката на институцията трябва да вземе предвид рисковете, свързани с опазване на целостта на данните, съхранявани и обработвани от ИКТ системите. За тази оценка компетентните органи следва по-специално да вземат предвид дали рамката включва:

а) политика, която определя ролите и отговорностите за управление на целостта на данните в ИКТ системите (напр. архитект на данни, отговорници за данни[6], попечители на данни[7], собственици/разпоредители с данни[8]) и дава насоки за това кои данни са от решаващо значение от гледна точка на целостта на данните и следва да подлежат на специфични мерки за контрол в областта на ИКТ (напр. автоматизирани механизми за контрол за валидиране на входящи данни, контрол на трансфера на данни, изравнявания и т.н.) или прегледи (напр. проверка на съвместимостта с архитектурата на данни) в различните етапи от жизнения цикъл на ИКТ данните;

б) документирана архитектура на данните, модел на данните и/или речник, който е потвърден от съответните заинтересовани лица от бизнеса и ИТ за поддържане на необходимата съгласуваност на данните в ИКТ системите и за гарантиране, че архитектурата на данни, моделът на данни и/или речникът продължават да изпълняват нуждите на бизнеса и управлението на рисковете;

в) политика по отношение на разрешеното използване и зависимост от компютърните системи на крайния потребител, по-специално по отношение на идентифицирането, регистрирането и документирането на важни за крайния потребител компютърни решения (напр. при

[6] Отговорникът за данните следи процеса за обработка на данните и тяхното използване.

[7] Попечителят на данни е отговорен за безопасното пазене, транспортиране и съхранение на данните.

[8] Собственикът/разпоредителят на данни е отговорен за управлението и годността на елементите на данните — както на съдържанието, така и на метаданните.

обработката на важни данни) и очакваните нива на сигурност за предотвратяване на неразрешени модификации, както в самите инструменти, така и в данните, съхранявани в тях;

г) документирани процеси за обработка на изключения за разрешаване на идентифицираните проблеми в целостта на ИКТ данните в съответствие с тяхната критичност и чувствителност.

58. За поднадзорни институции, които попадат в обхвата на принципите на BCBS 239 за ефективно агрегиране на данните за риска и отчитане на риска[9], компетентните органи трябва да прегледат анализа на риска на институцията за отчитането на риска от нейна страна и за възможностите за агрегиране на данните в сравнение с принципите и подготвената документация за тях, като се вземат предвид сроковете на изпълнение и преходните разпоредби на тези принципи.

Д) Контролни механизми за управление на съществените рискове, свързани с изнасяне на дейности, свързани с ИКТ

59. Компетентните органи следва да оценят дали стратегията за изнасяне на дейности на институцията, в съответствие с изискванията на насоките за изнасяне на дейности на Комитета на европейските банкови надзорници (CEBS) (2006 г.) и в допълнение към изискванията, посочени в параграф 85, буква г) на Насоките на ЕБО относно ПНПО, се отнася адекватно при изнасяне на дейности, свързани с ИКТ, включително за изнасянето на дейности в рамките на групата, предоставяща ИКТ услуги вътре в групата. При оценката на рисковете, свързани с изнасяне на дейности, свързани ИКТ, компетентните органи трябва да вземат предвид, че рисковете, свързани с изнасянето на дейности в областта на ИКТ, могат да бъдат обхванати и като част от оценката на присъщите операционни рискове съгласно параграф 240, буква й) от Насоките на ЕБО относно ПНПО, за да се избегне дублирането на дейности или двойно отчитане.

60. По-специално, компетентните органи следва да преценят дали институцията има създадена ефективна рамка за идентифициране, разбиране и измерване на риска, свързан с изнасяне на дейности в областта на ИКТ, и по-специално въведени контролни механизми и среда за контрол за редуциране на рисковете, свързани със съществени изнесени ИКТ услуги, които са съизмерими с размера, дейностите и рисковия профил на ИКТ на институцията и включват:

а) оценка на въздействието на изнасянето на дейности в областта на ИКТ за управлението на риска на институцията във връзка с използването на доставчици на услуги (напр. доставчици на облачни (“cloud”) услуги) и тяхното обслужване по време на процеса на възлагане на услуги, който е документиран и се взема под внимание от висшето ръководство или от ръководния орган за решението дали да се изнасяте тези дейности или не. Институцията следва да преразгледа политиките за управление на риска за ИКТ и контролните механизми на ИКТ и средата за контрол на доставчика на услуги, за да се гарантира, че те отговарят на вътрешните цели за управление на риска на институцията и на склонността към поемане на риск. Този преглед трябва да се актуализира периодично по време на периода на договора за изнасяне на дейности, като се вземат предвид характеристиките на изнесените услуги;

[9] Базелски комитет по банков надзор, Принципи за ефективно агрегиране на данните за риска и отчитане на риска, януари 2013 г., достъпен онлайн на: http://www.bis.org/publ/bcbs239.pdf.

б) наблюдение на рисковете за ИКТ на изнесените услуги по време на договора за изнасяне на дейности като част от управлението на риска на институцията, чиито данни постъпват в отчетността за управлението на риска за ИКТ на институцията (напр. отчитане на непрекъсваемостта на дейността, докладване, свързано със сигурността);

в) наблюдение и сравняване на получените нива на обслужване с договорените нива на обслужване, които следва да бъдат част от договора за изнасяне на дейности или от споразумение за нивото на обслужване (SLA); и

г) подходящи човешки и финансови ресурси и компетентности за наблюдение и управление на рисковете за ИКТ от изнесените услуги.

3.4 Резюме на констатациите и оценка

61. След извършване на посочената по-горе оценка компетентните органи следва да съставят становище за риска за ИКТ на институцията. Това становище следва да бъде отразено в резюме на констатациите, които компетентните органи трябва да вземат предвид при определяне на оценката на операционния риск в таблица 6 от Насоките на ЕБО относно ПНПО. Компетентните органи следва да основат своето становище върху съществените рискове за ИКТ, като вземат предвид следните съображения, които трябва да бъдат включени в оценката на операционния риск:

а) Съображения относно риска

i. рисковия профил на ИКТ и експозициите на институцията;
ii. идентифицирани критични системи и услуги в областта на ИКТ; и
iii. съществеността на риска за ИКТ по отношение на критични ИКТ системи.

б) Съображения относно управлението и контрола

i. дали има съгласуваност между политиката и стратегията за управление на риска в областта на ИКТ на институцията и нейната цялостната стратегия и склонност към поемане на риск;
ii. дали организационната рамка за управление на риска за ИКТ е стабилна, с ясни отговорности и ясно разделение на задачите между собствениците на риска и функциите за управление и контрол;
iii. дали измерването на риска за ИКТ, системите за наблюдение и отчетност са подходящи; и
iv. дали рамките за контрол на съществени рискове в областта на ИКТ са надеждни.

62. Ако компетентните органи считат, че рискът за ИКТ е съществен и компетентният орган реши да оцени и да измерва този риск като подкатегория на операционния риск, таблицата по-долу (Таблица 1) представя съображенията, свързани с оценките на риска за ИКТ.

Таблица 1: Надзорни съображения за определяне на оценки на риска, свързани с ИКТ

Оценка на риска	Становище на надзора	Съображения за присъщия риск	Съображения за адекватно управление и контрол
1	Не се наблюдава видим риск от съществено пруденциално въздействие върху институцията, като се има предвид нивото на присъщ риск и механизмите за управление и контрол.	• Източниците на информация, разгледани в съответствие с параграф 37, не са показали значими експозиции към риск, свързан с ИКТ. • Естеството на рисковия профил на ИКТ на институцията във връзка с прегледа на критичните ИКТ системи и съществените рискове за ИКТ за системи и услуги в областта на ИКТ не са показали съществени рискове в областта на ИКТ.	• Политиката и стратегията на институцията по отношение на риска за ИКТ са съизмерими с нейната цялостна стратегия и склонност към поемане на риск. • Рамката на организацията по отношение на риска за ИКТ е стабилна, с ясни отговорности и ясно разделение на задачите между собствениците на риска и функциите за управление и контрол на риска. • Системите за измерване на риска за ИКТ и за неговото наблюдение и отчетност са подходящи. • Рамката за контрол на риска за ИКТ е надеждна.
2	Наблюдава се нисък риск от съществено пруденциално въздействие върху институцията, като се има предвид нивото на присъщ риск и механизмите за управление и контрол.	• Източниците на информация, разгледани в съответствие с параграф 37, не са показали значими експозиции на риск, свързан с ИКТ. • Естеството на рисковия профил на ИКТ на институцията във връзка с прегледа на критичните ИКТ системи и съществените рискове за ИКТ за системи и услуги в областта на ИКТ са показали ограничена експозиция към риск, свързан с ИКТ (напр. не повече от 2 от 5 от предварително определените рискови категории за ИКТ).	
3	Налице е среден риск от значително пруденциално въздействие върху институцията, като се има предвид нивото на присъщ риск и механизмите за управление и контрол.	• Източниците на информация, разгледани в съответствие с параграф 37, са показали индикации за възможни значими експозиции към риск, свързан с ИКТ. • Естеството на рисковия профил на ИКТ на институцията във връзка с прегледа на критичните ИКТ системи и съществените рискове за ИКТ за системи и	

		услуги в областта на ИКТ са показали повишена експозиция на риска за ИКТ (напр. 3 или повече от 5 от предварително определените рискови риск за ИКТ).	
4	Наблюдава се висок риск от съществено пруденциално въздействие върху институцията, като се има предвид нивото на присъщ риск и управлението и механизмите за контрол.	• Източниците на информация, разгледани в съответствие с параграф 37, са показали множество индикации за значими експозиции на риск за ИКТ. • Естеството на рисковия профил на ИКТ на институцията във връзка с прегледа на критичните ИКТ системи и съществените рискове за ИКТ за системи и услуги в областта на ИКТ са показали висока експозиция към риска, свързан с ИКТ (напр. 4 или 5 от 5 от предварително определените рискови категории за ИКТ).	

Приложение — Таксономия на риска за ИКТ

Пет рискови категории за ИКТ с неизчерпателен списък на рисковете за ИКТ с потенциално висока тежест и/или въздействие във връзка с операциите, репутацията или финансите

Рискови категории за ИКТ	Рискове за ИКТ (неизчерпателен списък[10])	Описание на риска	Примери:
Рискове за достъпа и непрекъсваемостта на ИКТ;	Неадекватно управление на капацитета	Липсата на ресурси (напр. хардуер, софтуер, персонал, доставчици на услуги) може да доведе до невъзможност да се мащабира услугата, за да отговаря на нуждите на бизнеса, системни прекъсвания, влошаване на услугата и/или оперативни грешки.	• Недостигът на капацитет може да повлияе върху скоростите на предаване, както и на наличието на мрежа (интернет) за услуги като интернет банкиране. • Липсата на персонал (вътрешен или на трета страна) може да доведе до системни прекъсвания и/или оперативни грешки.
	Неизправности на ИКТ системата	Загуба на достъп поради неизправности с хардуера.	• Неизправност/повреда на съхранението (твърди дискове), сървър или друго ИТ оборудване, причинени например от липсата на поддръжка.
		Загубата на достъп поради неизправности или грешки със софтуера.	• Безкраен цикъл в софтуерно приложение не позволява изпълнение на операцията. • Прекъсвания поради продължителната употреба на остарели ИКТ системи и решения, които вече не отговарят на настоящите изисквания за достъп и устойчивост и/или вече не се поддържат от техните доставчици.
	Неадекватно планиране на непрекъсваемостта на ИКТ и възстановяването	Неизправност на планираните решения за достъп на ИКТ и/или решения за непрекъсваемостта и/или за възстановяване след бедствие (напр. резервен център за възстановяване на данни), когато се активира в отговор на инцидент.	• Разликите в конфигурацията между първичния и вторичния център за данни могат да доведат до невъзможност резервният център за данни да осигури планираната непрекъсваемост на услугата.

[10] Рисковете за ИКТ са изброени в рисковата категория, върху която оказват най-голямо-въздействие, но могат да окажат въздействие върху други рискови категории

Рискови категории за ИКТ	Рискове за ИКТ (неизчерпателен списък[10])	Описание на риска	Примери:
	о след бедствие		
	Неприемливи и разрушителни кибератаки	Атаки с различни цели (напр. активизъм, изнудване), които водят до претоварване на системите и мрежата, предотвратявайки достъп до онлайн компютърни услуги от страна на техните легитимни потребители.	• Разпространявани атаки от типа „отказ на услуги“ се извършват с помощта на множество компютърни системи в интернет, контролирани от хакер, изпращащ голямо количество видимо легитимни заявки за интернет услуги (напр. електронно банкиране).
Рискове за сигурността на ИКТ;	Кибер атаки и други външни атаки, базирани на ИКТ	Атаки, извършени от интернет или от външни мрежи с различни цели (напр. измама, шпионаж, активизъм/саботаж, кибертероризъм) с помощта на различни техники (напр. социално инженерство, опити за проникване чрез използване на уязвимости, внедряване на зловреден софтуер), което води до контрол върху вътрешни ИКТ системи.	Различни видове атаки: • APT (Разширена постоянна заплаха) за поемане на контрол върху вътрешни системи или за кражба на информация (напр. кражба на информация за самоличност, информация за кредитни карти). • Зловреден софтуер (напр. рансъмуер), който криптира данни с цел изнудване. • Инфекция на вътрешни ИКТ системи с троянски коне за извършване на злоумишлени действия на системата по прикрит начин. • Експлоатация на ИКТ система и/или на уязвимостите на (уеб) приложение (напр. „праSQL injection“ и т.н.) с цел получаване на достъп до вътрешната ИКТ система.
		Извършване на измамни финансови операции от хакери чрез разбиване или заобикаляне на сигурността на електронното банкиране и услуги за плащане и/или чрез атакуване и използване на уязвимости в сигурността във вътрешните системи за плащания на институцията.	• Атаки срещу електронно банкиране или платежни услуги, с цел да се извършат неразрешени операции. • Създаване и изпращане на измамни финансови операции от вътрешните системи за плащания на институцията (напр. измамни SWIFT съобщения).
		Сключване на сделки с ценни книжа с цел измама от хакери чрез разбиване или заобикаляне на	• Атаки от типа „дъмпингови схеми с акции“, при които нападателите получават достъп до сметки

Рискови категории за ИКТ	Рискове за ИКТ (неизчерпателен списък[10])	Описание на риска	Примери:
		сигурността на услугите за електронно банкиране, които също така предоставят достъп до сметки за ценните книжа на клиента.	за електронно банкиране на ценни книжа на клиенти и пускат измамни нареждания за покупка или продажба, целящи повлияване върху пазарната цена и/или реализиране на печалби на базата на предварително определени позиции на ценни книжа.
		Атаки върху комуникационни връзки и разговори от всякакъв вид или ИКТ системи с цел събиране на информация и/или извършване на измами.	• Подслушване/прихващане на незащитено предаване на данни за удостоверяване на автентичността в обикновен текст.
	Неадекватна вътрешна сигурност на ИКТ	Придобиване на неразрешен достъп до критични ИКТ системи в рамките на институцията с различни цели (напр. измама, извършване и скриване на нелоялни търговски дейности, кражба на данни, активизъм/саботаж) с разнообразни техники (напр. злоупотреба и/или ескалация на привилегии, кражба на самоличност, социален инженеринг, използване на уязвимости в областта на ИКТ системи, внедряване на зловреден софтуер).	• Инсталиране на устройства за регистриране на клавиши (кийлогъри) с цел кражба на потребителски имена и пароли за получаване на неразрешен достъп до поверителни данни и/или за извършване на измама. • Разбиване/отгатване на слаби пароли с цел сдобиване с нелегитимни или по-високи права за достъп. • Системен администратор използва операционни системи или бази данни (за директни модификации на бази данни) за извършване на измами.
		Неразрешени манипулации на ИКТ, дължащи се на неадекватни процедури и практики за управление на достъпа до ИКТ.	• Неуспешно деактивиране или изтриване на ненужни сметки, например на служители, които са променили функциите си и/или са напуснали институцията, включително външни лица или доставчици, които вече не се нуждаят от достъп, което от своя страна осигурява неупълномощен достъп до ИКТ системи. • Предоставяне на прекомерни права на достъп и привилегии, което позволява неразрешен достъп и/или прави възможно скриването на нелоялни

Рискови категории за ИКТ	Рискове за ИКТ (неизчерпателен списък[10])	Описание на риска	Примери:
			дейности.
		Заплахи за сигурността поради липса на информираност относно сигурността, при която служителите не разбират, проявяват небрежност или не успяват да спазват правилата и процедурите за сигурност в областта на ИКТ.	• Служители, които биват измамени за оказване на съдействие за атака (т.е. социално инженерство). • Лоши практики по отношение на пълномощията: споделяне на пароли, използване на „лесни за отгатване“ пароли, използване на една и съща парола за различни цели и т.н. • Съхранение на некриптирани поверителни данни на лаптопи и на преносими устройства за съхранение на данни (напр. USB ключове), които могат да бъдат изгубени или откраднати.
		Неправомерно съхранение или прехвърляне на поверителна информация извън институцията.	• Лица, които извършват кражба или умишлено изтичане или изнасяне на поверителна информация на неупълномощени лица или на обществеността.
	Неадекватна физическа сигурност в областта на ИКТ	Злоупотреба или кражба на активи в областта на ИКТ чрез физически достъп, причинявайки щети, загуба на активи или данни, или осигуряване на възможност за други заплахи.	• Физически взлом в офис сгради и/или центрове за данни с цел кражба на ИКТ оборудване (напр. компютри, лаптопи, решения за съхранение) и/или за копиране на данни чрез физически достъп до информационни и комуникационни системи.
		Умишлено или случайно увреждане на материалните активи в областта на ИКТ, причинено от терористични действия, аварии или случайни/погрешни манипулации от страна на персонала на институцията и/или трети страни (доставчици, техник).	• Физически тероризъм (т.е. терористични бомби) или саботаж на ИКТ активи. • Унищожаване на център за данни, причинено от пожар, изтичане на вода или други фактори.
		Недостатъчна физическа защита срещу природни бедствия в резултат от частично или пълно унищожаване на ИКТ системи/центрове за данни от	• Земетресения, екстремни температури, бури, тежки снежни бури, наводнения, пожар, мълния.

Рискови категории за ИКТ	Рискове за ИКТ (неизчерпателен списък[10])	Описание на риска	Примери:
		природни бедствия.	
Рискове в следствие от промени в ИКТ	Недостатъчен контрол на промените в областта на ИКТ системите и развитието на ИКТ	Инциденти, причинени от неоткрити грешки или уязвимости в резултат от промяна (напр. непредвидени последици от промяна или лошо управлявана промяна поради липса на тестване или неправилни практики за управление на промяната), напр. софтуер, ИКТ системи и данни.	• Въвеждане в производствения цикъл на недостатъчно тестван софтуер или промени в конфигурацията с неочаквани неблагоприятни ефекти върху данни (напр. увреждане, заличаване) и/или работа на ИКТ система (напр. повреда, влошаване на производителността). • Неконтролирани промени в ИКТ системи или данни в производствена среда. • Въвеждане в производствения цикъл на слабо осигурени ИКТ системи и интернет приложения, създаващи възможности хакерите да атакуват предоставяните интернет услуги и/или да нарушават вътрешните ИКТ системи. • Неконтролирани промени в изходния код на вътрешно разработен софтуер. • Недостатъчно тестване поради липса на подходящи условия за тестване.
	Неадекватна ИКТ архитектура	Слабото управление на ИКТ архитектурата при проектирането, изграждането и поддържането на ИКТ системи (напр. софтуер, хардуер, данни) може да доведе с течение на времето до сложни, трудни, скъпи за управление и трудни за промяна ИКТ системи, които не са достатъчно съобразени с нуждите на бизнеса и които не отговарят на реалните изисквания за управление на риска.	• Неадекватно управление на промените в областта на ИКТ системи, софтуер и/или данни за продължителен период от време, което води до сложни, разнородни и трудни за управление системи и архитектури в областта на ИКТ, причиняващи много неблагоприятни въздействия върху бизнеса и управлението на риска (напр. липса на гъвкавост и бързина, инциденти и неизправности в областта на ИКТ, високи операционни разходи, влошена сигурност и устойчивост на ИКТ, понижаване на качеството на данните и възможностите за отчитане).

Рискови категории за ИКТ	Рискове за ИКТ (неизчерпателен списък[10])	Описание на риска	Примери:
			• Прекомерното персонализиране и разширение на комерсиални софтуерни пакети с вътрешно разработен софтуер, което води до неспособност за изпълнение на бъдещи версии и подобрения на търговски софтуер и до риска, че вече не се поддържа от доставчика.
	Неадекватен жизнен цикъл и управление на корекциите	Невъзможност да се поддържа подходящ инвентар на всички ИКТ активи в подкрепа на, както и в комбинация със стабилен жизнен цикъл и практики за управление на корекциите. Това води до недостатъчно коригирани (и по този начин по-уязвими) и остарели ИКТ системи, които не могат да поддържат нуждите на управлението на бизнеса и риска.	• Некоригирани и остарели ИКТ системи, които могат да окажат неблагоприятно въздействие върху дейността и управлението на риска (напр. липса на гъвкавост и пъргавина, прекъсване на ИКТ, понижена сигурност и устойчивост на ИКТ).
Риск за целостта на ИКТ данните	Лошо функциониращa обработка или употреба на ИКТ данни	Поради грешките и неизправностите на системата, комуникацията и/или приложенията или поради процес на погрешно извличане, трансфер и натоварване (ETL) на данни, данните могат да бъдат повредени или изгубени.	• Грешка в ИТ системата при обработка на партида, която води до неправилни салда в банковите сметки на клиента. • Погрешно изпълнени запитвания. • Загуба на данни поради грешка в репликацията на данните (бекъп).
	Лошо проектирани механизми за контрол за проверка на данни в ИКТ системите	Грешки, свързани с липсващи или неефективни автоматизирани входни данни и контролни механизми за приемане (напр. за използвани данни на трети страни), трансфер на данни, обработка и контрол на изхода в ИКТ системи (напр. механизми за контрол на тяхната валидност на входа, съгласуване на данни).	• Недостатъчно или невалидно форматиране/валидиране на входящите данни в приложения и/или потребителски интерфейси. • Липса на механизми за контрол за съгласуване на данните за получените резултати • Липса на контрол за извършените процеси на извличане на данни (напр. заявки за базата данни), които водят до грешни данни. • Използване на некачествени външни данни.
	Лошо контролирани	Грешки във въведените данни поради липса на контролни механизми на коректността и	• Разработчици или администраторите на бази данни, имащи директен достъп, които

Рискови категории за ИКТ	Рискове за ИКТ (неизчерпателен списък[10])	Описание на риска	Примери:
	промени на данните в производствените ИКТ системи.	обосновано естество на манипулациите на данните, извършвани в производството на ИКТ системи.	извършват промяна на данните в производствените ИКТ системи по неконтролиран начин — например в случай на инцидент, свързан с ИКТ.
	Лошо проектирани и/или управлявани архитектура на данни, информационни потоци, модели на данни или речници на данни	Лошо управляваните архитектури на данни, модели на данни, пренос на данни или речници за данни могат да доведат до различни версии на едни и същи данни във всички ИКТ системи, които вече не са в съответствие поради прилаганите по различен начин модели на данните или определения на данните и/или различия в основните процеси за генериране и промяна на данните.	• Съществуването на различни клиентски бази данни за продукт или на бизнес единица с различни определения за данните и полетата, водещи до несъгласувани и трудни за сравнения интегрирани данни на клиентите на нивото на цялата финансова институция или група.
Рискове, свързани с изнасянето на дейности в областта на ИКТ.	Неадекватна устойчивост на услугите на трети страни или на друга структура от групата	Липса на критични изнесени услуги в областта на ИКТ, телекомуникационните услуги и съоръжения. Загуба или повреда на критични/чувствителни данни, поверени на доставчика на услуги	• Липса на основни услуги в резултат на неизправности на изнесени ИКТ системи или приложения на доставчици. • Прекъсване на телекомуникационни връзки. • Недостиг на захранване.
	Неадекватно управление на изнесените дейности	Значимо влошаване или неизправности на услуги, дължащи се на неефективна готовност или контролни процеси на външния доставчик на услуги. Неефективното управление на изнесените дейности може да доведе до липса на подходящи умения и способности за пълно идентифициране, оценяване, редуциране и наблюдение на рисковете за ИКТ и може да доведе до ограничаване на оперативните способности на институциите.	• Лоши процедури за справяне с инциденти, договорни механизми за контрол и гаранции, включени в договора с доставчик на услуги, които увеличават ключовата зависимост от трети страни и търговци. • Неподходящите механизми за управление на промяната по отношение на ИКТ средата на доставчик на услуги могат да доведат до значително влошаване или отказ на услуга.

Рискови категории за ИКТ	Рискове за ИКТ (неизчерпателен списък[10])	Описание на риска	Примери:
	Неадекватна сигурност на трета страна или на друга структура от групата.	Проникване в ИКТ системи на доставчиците на услуги на трети страни с пряко въздействие изнесените услуги или критични/поверителни данни, съхранявани от доставчика на услугата. Персоналът на доставчика на услуги получава неразрешен достъп до критични/чувствителни данни, съхранявани от доставчика на услугата.	• Проникване в системи на доставчиците на услуги от страна на престъпници или терористи като входна точка в ИКТ системи на институциите или с цел достъп/унищожаване на критични или чувствителни данни, съхранявани от доставчика на услугата. • Злонамерени „вътрешни лица“ от страна на доставчика на услуги, които се опитват да крадат и продават чувствителни данни.