проф. д-р ЕМИЛИЯ МИЛАНОВА – ЦОНЧЕВА
Дипломиран експерт-счетоводител
Регистриран одитор
Преподавател във Висшето училище по застраховане и финанси – София
Катедра „Счетоводство и одит“

Емилия Миланова е завършила ВИИ „Карл Маркс” (сега УНСС) в гр. София през 1974 г., магистър, специалност „Счетоводна отчетност”.

От 1990 г. е доктор по икономика, от м. януари 2012 г. е професор в катедра „Счетоводство и анализ” в УНСС, а от 2019 г. в катедра „Счетоводство и одит“ при ВУЗФ. Като професор изнася лекции по учебните дисциплини: „Основи на счетоводството”, „Регулации и управление на риска във финансовия сектор”, „Анализ на финансовите отчети“, „Вътрешен контрол и управление на риска в корпорацията“, „Счетоводство на застрахователите и осигурителите“, „Превенция на финансови измами и пране на пари“.

През 1997 г. е избрана за подуправител на БНБ и в продължение на 10 години ръководи Управление „Банков надзор”. За периода 1997 – 2001 г. е зам.-председател на Съвета на директорите на Банковата консолидационна компания.

От м. септември 2007 до м. април 2011 г. е председател на Съвета на директорите на „Юробанк България” АД (Пощенска банка). От м. май 2020 г. е член на Надзорния съвет и зам.-председател на Интернешънъл Асет Банк АД.

През 1993 г. е утвърдена като дипломиран експерт-счетоводител. Член е на ИДЕС, регистриран одитор. Одитирала е банки, застрахователни дружества, пенсионни дружества, инвестиционни посредници и финансови къщи, предприятия от нефинансовия сектор, в т.ч. извършващи дейност от обществен интерес.

Била е председател на Съвета по професионална етика на ИДЕС. От 2013 г. е председател на Редакционния съвет на списание ИДЕС.

Специализирала е счетоводство, анализ и банков надзор в Санкт Петербург, Вашингтон и Брюксел. Има монографии, студии, учебници и други публикации в научната област „Счетоводство, одит и финансов анализ”.

АНАЛИЗ И ОЦЕНКА НА ОПЕРАЦИОННИЯ РИСК ПРИ БАНКИТЕ. ОПЕРАТИВНА УСТОЙЧИВОСТ НА ИНФОРМАЦИОННИТЕ И КОМУНИКАЦИОННИ ТЕХНОЛОГИИ

Резюме

Студията обсъжда анализа и оценката на операционния риск в банките, като акцентира върху идентифициране, измерване и наблюдение на операционния риск; капиталовото изискване за операционен риск; оценката на подкатегориите операционен риск – риск, свързан с информационните и комуникационни технологии (ИКТ), риск от неправомерно поведение и риск, произтичащ от модела; върху стратегия за управление и рисков апетит за поемане на операционен риск. В контекста на анализа на операционния риск е представена оперативната устойчивост на ИКТ чрез актуалната нормативна регламентация и рамката за управление на риска в областта на ИКТ. Разсъждава се и върху стратегическите предизвикателства на оперативната устойчивост на цифровите технологии пред банките.

Prof. EMILIA MILANOVA, PhD
Certified Public Accountant
Registered Auditor
Lecturer at VUZF University – Sofia

ANALYSIS AND ASSESSMENT OF OPERATIONAL RISK IN BANKS. OPERATIONAL SUSTAINABILITY OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Summary

The study discusses the analysis and assessment of operational risk in banks, focusing on the identification, measurement and monitoring of operational risk; the capital requirement for operational risk; the assessment of the subcategories of operational risk - risk related to information and communication technologies (ICT), risk of misconduct and risk arising from the model; on the management strategy and risk appetite for taking operational risk.

In the context of the analysis of operational risk, the operational sustainability of ICT is presented through the current regulatory framework and the risk management framework in the field of ICT.

It also reflects on the strategic challenges of the operational sustainability of digital technologies for banks.

АНАЛИЗ И ОЦЕНКА НА ОПЕРАЦИОННИЯ РИСК ПРИ БАНКИТЕ. ОПЕРАТИВНА УСТОЙЧИВОСТ НА ИНФОРМАЦИОННИТЕ И КОМУНИКАЦИОННИ ТЕХНОЛОГИИ

ВЪВЕДЕНИЕ

Основните теми на 2024 г. за банковия сектор бяха:

1. БАЗЕЛ III – продължи въвеждането на окончателната рамка „Базел III“ и коректно въвеждане на оставащите елементи от реформата „Базел III“, договорена през 2017 г. (*Регламент (ЕС) 2024/1623 на Европейския парламент и на Съвета от 31 май 2024 г. за изменение на Регламент (ЕС) № 575/2013 по отношение на изискванията за кредитен риск, риск от корекция на кредитната оценка, операционен риск и пазарен риск, както и за долна граница на капиталовото изискване,* ще бъде обект на внимание в публикацията).

2. Развитие на рамката за екологични, социални и управленски рискове (ESG рискове и фактори)[1] – отново беше изведена напред с множество актове на ниво европейско законодателство, също така и национално – чрез промяна в *Закона за счетоводството* и *Закона за независимия финансов одит и изразяването на сигурност по устойчивостта*, включително редица актове на подзаконово ниво. В този контекст от банковия сектор се очаква да поеме водеща роля по пътя към устойчива икономика, като участва пряко в предизвикателствата и възможностите за ускоряване на зеления преход в Европа чрез устойчиво финансиране в подкрепа на бизнеса; да споделя целите на ЕС за ангажираност към опазването на околната среда и да продължава да надгражда и утвърждава интегрирането на екологичните, социални и управленски фактори в бизнес модела си.

3. Продължи въвеждането на ***единната правна рамка за повишаване стандартите на системите за дигитална устойчивост и поддържане на киберсигурността*** в 18 критични сектора в целия ЕС – DORA и МИС 2[2].

4. Развитие на рамката за платежни услуги на ниво европейско законодателство – *Регламент (ЕС) 2023/1113* на ЕП и на Съвета от 31 май 2023 г. *относно информацията, придружаваща преводите на средства и прехвърлянията на определени криптоактиви*, и за изменение на Директива (ЕС) 2015/84 и *Регламент (ЕС) 2024/886* на ЕП и на Съвета от

---

[1] Директива (ЕС) 2022/2464 на ЕП и на Съвета от 14 декември 2022 година за изменение на Регламент (ЕС) № 537/2014, Директива 2004/109/ЕО, Директива 2006/43/ЕО и Директива 2013/34/ЕС, *по отношение на отчитането на предприятията във връзка с устойчивостта.*

[2] Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14 декември 2022 година относно *оперативната устойчивост на цифровите технологии във финансовия сектор* – DORA.
Директива 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 година *относно мерки за високо общо ниво на киберсигурност* в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (Директива МИС 2).

13 март 2024 година *по отношение на незабавните кредитни преводи в евро*[3].

5. Консултации за управлението на лихвения риск, произтичащ от дейности извън търговския портфейл (IRRBB и CSRBB) – определяне на критерии за установяване, оценка, управление и редуциране на рисковете, произтичащи от потенциални промени в лихвени проценти, и за оценка и наблюдение на риска от кредитния спред на дейностите на институциите извън търговския портфейл (Насоки (EBA/GL/2022/14), както и Делегиран регламент (ЕС) 2024/857 на Комисията от 01.12.2023 година за допълнение на Директива 2013/36/ЕС на Европейския парламент и на Съвета по отношение на регулаторните технически стандарти за определяне на *стандартизирана методика и опростена стандартизирана методика* за оценка на рисковете, произтичащи от *потенциални промени в лихвените проценти, които засягат както икономическата стойност на собствения капитал, така и нетния доход от лихви от дейностите на институцията извън търговския портфейл.*

6. Възстановяване и преструктуриране.

7. Предотвратяване на изпирането на пари и финансирането на тероризма (AML/CTF) – ***нов пакет AML***, приет от ЕК: *6-а Директива AML* (Директива (ЕС) 2024/1640 на ЕП и на Съвета от 31 май 2024 г. относно механизмите, които да бъдат въведени от държавите членки за предотвратяване на използването на финансовата система за целите на изпирането на пари или финансирането на тероризма), *нов Регламент (ЕС) 2024/1624* на ЕП и на Съвета от 31 май 2024 г. *за предотвратяване на използването на финансовата система за целите* на изпирането на пари или финансирането на тероризма и *създаване на Орган за борба с изпирането на пари и финансирането на тероризма* (Регламент (ЕС) 2024/1620 на ЕП и на Съвета от 31 май 2024 г. за създаване на Орган за борба с изпирането на пари и финансирането на тероризма и за изменение на регламенти (ЕС) № 1093/2010, (ЕС) № 1094/2010 и (ЕС) № 1095/2010).

8. Развитие на Рамката за изискванията във връзка с инструментите на ***приемливите задължения*** като инструменти от капитала от първи ред.

Целта на настоящото изследване е да представи предизвикателствата пред банките при анализа и оценката на операционния риск, и най-вече подкатегорията на операционния риск – *рискът, свързан с информационните и комуникационни технологии (ИКТ) на съвременния етап.* За реализация на целта ще формулираме **следните задачи:**

- идентифициране, измерване и наблюдение на операционния риск като един от елементите за въвеждането на окончателната рамка „Базел III“;

[3] Добавяме и Регламент (ЕС) 2023/1114 на ЕП и на Съвета от 31 май 2023 г. *относно пазарите на криптоактиви* и за изменение на регламенти (ЕС) № 1093/2010 и (ЕС) № 1095/2010 и на Директиви (ЕС) 2013/36 и (ЕС) 2019/193.

- оценка на подкатегориите операционен риск – риск, свързан с информационните и комуникационни технологии (ИКТ), риск от неправомерно поведение и риск, произтичащ от модела;
- подробно представяне на оперативната устойчивост на ИКТ чрез актуалната нормативна регламентация и рамката за управление на риска в областта на ИКТ;
- стратегическите предизвикателства на оперативната устойчивост на цифровите технологии пред банките.

Акцентираме върху темата Базел III, тъй като останалите теми на 2024 година са пряко свързани с темата за коректното въвеждане на окончателната рамка „Базел III“ (*авторът на тази студия я нарече Базел IV*)[4]. В отговор на световната *финансова криза от 2008 – 2009 г.* Съюзът предприе широкообхватна реформа на пруденциалната рамка за кредитните институции, както е определена в Регламент (ЕС) № 575/2013 на ЕП и на Съвета[5], с цел повишаване на устойчивостта на банковия сектор на Съюза.

Рамката „Базел III“ е главен елемент от отговора на Базелския комитет за банков надзор (БКБН, Комитетът) по отношение на световната финансова криза от 2008 г. Комитетът разгледа недостатъците в регулаторната рамка, предшестваща кризата, за да осигури основа за устойчива банкова система, която ще помогне да се избегне натрупването на системни рискове[6]. При определяне на елементите на базелско споразумение за капитала (Базел III) се отдели силно внимание на въздействието, което то ще окаже върху банковата индустрия и националната икономика както по време на прехода, така и в дългосрочен план. Това означава да се очертае път към по-сигурна и по-силна финансова система, която поддържа растежа в правилната посока – *увеличавайки доходността в дългосрочен план, като в същото време минимизира икономическите разходи в краткосрочен план.*

Базелският комитет по банков надзор (БКБН) поиска да реформира съществуващите стандарти Basel III чрез серия от реформи, чиято цел е да затрудни банките да избягват по-високите капиталови изисквания, въведени след финансовата криза. Затова „новите правила“ (наречени

---

[4] За повече подробности вж. Миланова, Е. *Време ли е за Базел IV и какви са ефектите върху банките в България,* 2018, Икономически и социални алтернативи, УНСС, София, ISSN (print): 1314-6556, ISSN (online): 2534-8965, инд. в RePec, Google Scholar и EBSCO.

[5] Регламент (ЕС) № 575/2013 на ЕП и на Съвета от 26 юни 2013 г. относно пруденциалните изисквания за кредитните институции и за изменение на Регламент (ЕС) № 648/2012 (ОВ L 176, 27.6.2013 г. (*Регламент за капиталовите изисквания – РКИ*).

[6] дълбочината на кризата беше подсилена от една финансова система, която навлезе в кризата с твърде голяма задлъжнялост (ливъридж), недостатъчни капиталови нива и ликвидни буфери, и лоши стимули за поемане на рискове. Банковият сектор беше твърде уязвим за шокове без значение какъв е източникът. По време на най-жестокия епизод на кризата пазарът изгуби доверие в платежоспособността и ликвидността на много банкови институции. Слабостите в банковия сектор бяха пренесени в останалата част от финансовата система и реалната икономика, което предизвика като резултат внушително свиване на ликвидността и на възможността да се осигурят източници за кредитиране. Авторът е сигурен, че ако регулаторните стандарти бяха по-строги и разумни, кризата нямаше да е толкова дълбока и товарът върху публичния сектор толкова голям.

условно Basel IV) бяха разработени с цел да се предотврати поемането на твърде много рискове от страна на финансовите институции[7].

Американските и швейцарските регулатори настояваха за въвеждане на общо стандартизирано ниво на капитал, под което банката да не може да слиза въпреки вътрешните си изчисления на риска. Опасенията бяха свързани с това, че кредитните портфейли на европейските банки бяха оценени като по-рискови от американските. В такъв случай те се нуждаеха от повече капитал, отколкото банките в САЩ, които си осигуряваха повече финансиране чрез облигации и пакетирани ипотечни продукти.

В началото на м. декември 2017 г. органът за надзор на Базелския комитет, Групата на управителите на централните банки и ръководителите на надзорните органи (GHOS), *одобри програмата за реформи* за нерешените проблеми с регулаторната рамка на Базел III след кризата – наречен от автора *пакетът Базел IV*. Тази нова програма имаше за цел да допълва подобренията в глобалната регулаторна рамка, която направи Базел III, да възстановява надеждността при изчисляването на рисково претеглените активи (RWA) и да подобрява сравнимостта на капиталовите съотношения на банките чрез:

- ✓ *преработен стандартизиран подход за кредитен риск,* който да подобри устойчивостта и рисковата чувствителност на съществуващия подход (БКБН счита, че настоящият стандартизиран подход за оценяване на кредитния риск (стандартизиран подход за кредитен риск – СПКР) не е в достатъчна степен чувствителен към риска в редица области, което води до неточно или неподходящо – твърде високо или твърде ниско – измерване на кредитния риск и оттам – на капиталовите изисквания. Поради това разпоредбите относно СПКР следва да бъдат изменени, за да се повиши чувствителността към риска при този подход в няколко основни аспекта);
- ✓ *преразглеждане на подхода, базиран на вътрешните рейтинги за кредитен риск*, при който използването на подходите за вътрешни модели (IRB) за портфейли с ниска степен на неизпълнение да бъде ограничено;
- ✓ *промяна в рамката на риска от корекции на кредитната оценка (CVA)*, включително премахването на подхода на вътрешните модели и въвеждането на преработен стандартизиран подход;
- ✓ *преработен стандартизиран подход за операционен риск,* който да замести съществуващите стандартизирани подходи и напреднали подходи за измервания (AMA);

[7] Миланова, Е. Време ли е за Базел IV и какви са ефектите върху банките в България, 2018, Икономически и социални алтернативи, УНСС, София, инд. в RePec, Google Scholar и EBSCO.

- ✓ *промяна в измерването на съотношението на ливъридж* и в коефициента на ливъридж за глобално системно важни банки (G-SIBs);
- ✓ окончателната рамка на Базел 3 следва да отразява *значението на екологичните, социалните и управленските (ЕСУ) фактори* и цялостно разбиране на рисковете на експозициите към дейности, които са свързани с общата устойчивост или с ЕСУ целите, като за целите на сближаването в рамките на Съюза и на еднаквото разбиране на ЕСУ факторите и рисковете следва да бъдат въведени общи определения;
- ✓ *ревизиран капитал от първи стълб, който да гарантира, че рисковите активи на банките, генерирани от вътрешни модели, не са по-ниски от 72,5% от рисково-претеглените активи (RWA),* изчислени съгласно стандартизираните подходи на рамката на Базел III.

Благодарение на тази реформа предизвиканата от COVID-19 криза завари един устойчив банков сектор на Съюза. Все пак, въпреки че общото равнище на капитала в институциите в Съюза понастоящем като цяло е задоволително, някои от проблемите, установени в резултат на световната финансова криза, все още не са решени[8].

С цел да се намери решение на тези проблеми и *да се осигури правна сигурност* е изключително важно в правото на Съюза да бъдат *въведени коректно оставащите елементи от реформата „Базел III“,* договорена през 2017 г. (***окончателната рамка „Базел III“***). Същевременно при въвеждането е подходящо да се избегне значително увеличаване на общите капиталови изисквания за банковата система на Съюза като цяло и да се вземат предвид особеностите на икономиката на Съюза. Такова въвеждане следва да спомогне *да се избегнат неблагоприятни конкурентни последици за кредитните институции в Съюза*, най-вече при дейностите по търгуване, където те се конкурират пряко със своите международни партньори.

С въвеждането на *окончателната рамка „Базел III“* Съюзът приключва десетгодишен процес на реформи. Именно в този контекст Съюзът следва да извърши цялостна оценка на своята банкова система, като вземе предвид всички съответни измерения[9]. При прегледа следва да се вземе предвид въвеждането на долната граница на капиталовото изискване като част от пруденциалните правила за капитала и ликвидността, както и нейното

---

[8] Регламент (ЕС) 2024/1623 на Европейския парламент и на Съвета от 31 май 2024 г. за изменение на Регламент (ЕС) № 575/2013 по отношение на изискванията за кредитен риск, риск от корекция на кредитната оценка, операционен риск и пазарен риск, както и *за долна граница на капиталовото изискване.*

[9] Пак там: На Комисията следва да бъде възложено да извърши цялостен преглед на рамката за пруденциални и надзорни изисквания. При този преглед следва да се вземат предвид различните видове корпоративни форми, структури и бизнес модели в целия Съюз. При прегледа следва да се вземе предвид въвеждането на долната граница на капиталовото изискване като част от пруденциалните правила за капитала и ликвидността, както и нейното равнище на прилагане.

равнище на прилагане; да се прецени дали долната граница на капиталовото изискване и нейното равнище на прилагане осигуряват адекватно равнище на защита на вложителите и гарантират финансовата стабилност в Съюза, като се вземат предвид както развитието в целия Съюз като цяло, така и на банковия съюз във всичките му измерения.

Регламент (ЕС) № 575/2013 позволява на кредитните институции да изчисляват капиталовите си изисквания, като използват стандартизирани подходи или подходи на вътрешните модели. Стандартизираните подходи изискват от институциите да изчисляват капиталовите изисквания, като използват фиксирани параметри, които се основават на относително консервативни допускания и са указани в Регламент (ЕС) № 575/2013. Подходите на вътрешните модели, които трябва да бъдат одобрени от компетентните органи, позволяват на институциите сами да оценяват повечето или всички параметри, необходими за изчисляване на капиталовите изисквания. Въведената през декември 2017 г. от Базелския комитет по банков надзор (БКБН) *съвкупна долна граница на капиталово изискване* е взета въз основа на анализ, извършен след световната финансова криза от 2008 – 2009 г., от който стана ясно, че вътрешните модели обикновено подценяват рисковете, на които са изложени институциите, особено при някои видове експозиции и рискове, и следователно водят до недостатъчни капиталови изисквания.

Въвеждането на долна граница на капиталовото изискване е сред основните мерки на реформата „Базел III“. С нея се цели *да се ограничи неоправданата променливост на получените чрез вътрешни модели капиталови изисквания,* както и прекомерното намаляване на капитала, което може да получи институция, която използва вътрешните модели, спрямо институция, използваща стандартизираните подходи[10]. Добросъвестното въвеждане на долната граница на капиталовото изискване *би повишило съпоставимостта на съотношенията на капиталова адекватност* на банките, би възстановило доверието във вътрешните модели и *би било гарант за лоялна конкуренция сред кредитните институции*, които използват различни подходи за изчисляване на капиталовите си изисквания[11]. Още през м. юни 2023 г. Комисията поема ангажимент да извърши *цялостна, справедлива и балансирана оценка на състоянието на банковата система* и приложимите регулаторни и надзорни рамки на единния пазар (един от основните въпроси при анализа и оценката е *въвеждането на долна граница на капиталовото изискване*, включително нейното равнище на прилагане). Оценката е базирана на

[10] Като се определя долна граница на капиталовите изисквания, получени чрез вътрешните модели на дадена институция, на 72,5% от капиталовите изисквания, които биха се прилагали, ако същата институция беше използвала стандартизираните подходи, долната граница на капиталовото изискване ограничава риска от прекомерно намаляване на капитала.

[11] Регламент (ЕС) 2024/1623 на Европейския парламент и на Съвета от 31 май 2024 г. за изменение на Регламент (ЕС) № 575/2013 по отношение на изискванията за кредитен риск, риск от корекция на кредитната оценка, операционен риск и пазарен риск, както и *за долна граница на капиталовото изискване*.

информацията, предоставена от Европейския надзорен орган (Европейски банков орган) и от Европейската централна банка и единния надзорен механизъм, и ще се консултира със заинтересованите страни, за да гарантира, че различните гледни точки са взети предвид по подходящ начин.

През м. ноември 2024 г. Европейската централна банка (ЕЦБ) обсъди дали да публикува изследването, което показва, че капиталовите изисквания за големите кредитори от Европейския съюз трябва да нараснат *с двуцифрен процент*, ако за тях важат същите норми (наредби) за разумните, ограничаващи поемането на риск практики, както за конкурентите от Уолстрийт. Дори някои „стратези“ на ЕЦБ настояваха за огласяването на анализа или поне на някои от констатациите в него, за да оборят настойчивото лобиране от банковия сектор за редуциране на правилата за прилагане на базелското споразумение за глобалните капиталови изисквания за бранша.[12]

Целта на подготвения доклад е да оспори твърденията на играчите от европейския банков сектор, че те вече имат по-високи капиталови равнища от американските си конкуренти – част от усилията на бранша да редуцират новите правила, които, според тях, ще ги поставят в още по-неизгодно положение спрямо щатските играчи. Една от причините за тези по-високи капиталови коефициенти обаче е по-широкото използване на собствени модели, които могат да понижат степента на риск на активите им. Докато банките в Съединените щати нямат право да прилагат такива счетоводни модели. Европейските банки имат също и по-високи „буфери за управление“ над изисквания минимален капитал, отколкото щатските.

Регламент (ЕС) 2024/1623 *за приложение на окончателната рамка „Базел III“,* който беше приет окончателно през 2024 г., ще бъде въвеждан *постепенно през следващите осем години,* а Европейският банков орган е пресметнал, че този норматив ще повиши коефициентите за минимални капиталови равнища за големите банки с международна дейност на общността с 8.6% и няколкото най-едри, класифицирани като системно значими кредитори – с 12.2 процента[13]. Председателката на надзора на ЕЦБ Клаудия Бух дори е убедена, че Европа трябва да се придържа към плановете си да въведе наредбите на Базел независимо от действията на Съединените щати. Тя смята, че големите банки от Уолстрийт вече имат „значително по-високи капиталови изисквания“ от европейските си партньори.

---

[12] Натискът от кредиторите от ЕС вероятно ще се засили, ако Вашингтон „разводни“ или дори се откаже от плановете си да въведе наредбите на Базел за своите кредитни институции в условията на очакваната вълна от дерегулации след изборната победа на Доналд Тръмп на президентските избори.

[13] Преди няколко месеца Федералният резерв редуцира предложеното увеличение на капиталовите равнища на най-големите американски банки с повече от 50% – до 9%, след мощно недоволство от сектора и от политици срещу т. нар. „ендшпил на Базел“. Регулаторите обаче не успяха да се споразумеят за заложените наредби в „Базел III“ и в момента много кредитори отвъд Атлантика очакват новия екип на администрацията на Тръмп да отслаби изискванията или дори да ги отмени изцяло.

На 4 октомври 2024 г. ЕБО публикува *третия си задължителен мониторингов доклад „Базел III“ (Basel III monitoring Report),* в който се оценява въздействието, което прилагането на окончателната рамка „Базел III“ в ЕС ще окаже върху банките в ЕС на датата на пълното ѝ прилагане - 2033 г. В допълнителното въздействие се отчита прилагането на всички изисквания на ЕС, отразени в Регламента за капиталовите изисквания – Регламент (ЕС) № 575/2013-РКИ (изискванията на Стълб 2), и всички специфични за ЕС капиталови буфери. По отношение минимално изискуемия капитал въздействието е допълнително намалено спрямо предишната референтна дата – декември 2022 г. Въздействието е минимално по отношение на очаквания недостиг на капитал от първи ред, като общият недостиг на капитал се оценява на 5,1 млрд. евро. В този аспект си заслужава да отбележим публикуваното от Европейския банков орган (ЕВА) становище (Opinion on EC's amendments to draft ITS on Supervisory reporting and Pillar 3 disclosures – 14.11.2024 г.) за предложените от ЕК изменения на окончателния проект на Техническите стандарти за изпълнение (ТСИ) на ЕБО *относно публичното оповестяване от институциите и надзорното отчитане* съгласно преработения Регламент за капиталовите изисквания (CRR – Pillar 3). ЕБО отчита, че предложението на Комисията осигурява известна гъвкавост в сравнение с настоящата версия на ИТС и го приема като междинна стъпка, но счита, че образците и инструкциите трябва да бъдат достъпни чрез уебсайта на ЕБО, тъй като по този начин се осигурява по-голяма гъвкавост при разработването на такива ИТ решения[14].

В края на м. ноември 2024 г. *ЕБО публикува тримесечното си информационно табло за минималното изискване за собствен капитал и приемливи задължения (MREL)* за второто тримесечие на 2024 г. (MREL Dashboard Q1 and Q2 2024), в което се оповестява обобщена статистическа информация за 339 банки, предвидени за оздравяване в целия Европейски съюз, за които ЕБО е получил данни както за решението, така и за ресурсите. За първи път Информационното табло включва и списък на обхванатите субекти. Всички банки (с изключение на 21 банки, които все още са в *преходен период* и отчитат недостиг) изпълняват изискванията си за MREL в съответствие с крайния срок на Директивата за възстановяване и преструктуриране на банки – 1 януари 2024 г. Размерът на инструментите, които стават недопустими през следващата година за извадката, достигна 220 млрд. евро, което според нас изглежда управляемо.

[14] На 30.10.2024 г. европейските надзорни органи (ЕНО) публикуваха третия си годишен доклад *(Joint Committee Report on Principal Adverse Impact disclosures under SFDR*) относно *оповестяването на основните неблагоприятни въздействия* съгласно *Регламента за оповестяване на информация за устойчивото финансиране (SFDR).* Докладът оценява оповестяванията на основните неблагоприятни въздействия на ниво субект и продукт съгласно SFDR. Оповестяванията имат за цел да покажат отрицателното въздействие на инвестициите на финансовите институции върху околната среда и хората и действията, предприети от управителите на активи, застрахователи, инвестиционните посредници, банките и пенсионните фондове за неговото намаляване. Констатациите показват, че финансовите институции са подобрили достъпността на оповестяванията, вкл. положителен напредък е постигнат и по отношение на качеството на информацията, оповестявана за финансовите продукти.

Нещо, което според нас си заслужава да споделим, е публикуваното в края на м. ноември 2024 г. от ЕБО *есенно издание на доклада им за оценка на риска* (Risk Assessment Report – Autumn 2024), като същият е придружен *от доклад за прозрачността в целия ЕС за 2024 г.,* който предоставя подробна информация в сравним и достъпен формат за 123 банки от 26 държави в ЕС и ЕИП. Основни моменти от оценката на риска на ЕБО:

- Банките в ЕС/ЕИП продължават да работят в среда на бавен икономически растеж и рискове, свързани с геополитическия риск.
- Кредитирането се засилва бавно, докато качеството на активите на банките се влошава незначително.
- Преките експозиции на банковите сектори в ЕС към държави с геополитически риск са ограничени, но въпреки това вторичните рискове могат да бъдат съществени.
- Рисковете, свързани със сектора на кредитните институции и взаимовръзките с небанковите финансови посредници, остават значителни за банковия сектор в ЕС.
- Климатичните и физическите рискове не бива да се подценяват.
- Банките от ЕС/ЕИП запазиха силни капиталови позиции. Резервът на CET1 (базов капитал от първи ред) остава значително над общите капиталови изисквания (ОКР) и насоките по Стълб 2 (P2G).
- Рентабилността остава висока, но нейната устойчивост е предизвикателство, оценката на банките от ЕС/ЕИП изостава спрямо световните им колеги.
- Оперативните рискове, особено тези, свързани с киберзаплахи, се увеличават.
- Банките в ЕС/ЕИП прибягват до изкуствен интелект, за да насърчават ефективността, а изкуственият интелект с общо предназначение набира все по-голяма популярност, въпреки че по-широкото му използване не е лишено от рискове. Европейската централна банка (ЕЦБ) дори предупреди за „балон“ при акциите на компаниите, свързани с изкуствения интелект (AI), който може да се спука внезапно, ако „розовите очаквания“ на инвеститорите не се оправдаят. Предупреждението бе отправено като част от изготвяния два пъти годишно от ЕЦБ Преглед на финансовата стабилност (според Bloomberg).

Не искаме да пропуснем и публикуваното от ЕБО през м. декември 2024 г. *тримесечно информационно табло за риска* (Risk Dashboard Q3 2024) за *третото тримесечие на 2024 г.,* в което се оповестява обобщена статистическа информация за *най-големите институции в ЕС/ЕИП.*

▪ *Възвръщаемостта на собствения капитал (RoE)* на банките от ЕС/ЕИП леко се е повишила на тримесечна база с 20 bps до 11,1% (без промяна на годишна база). Увеличението се дължи на положителния принос на другите оперативни приходи и на спада на всички основни разходни компоненти. *Нетният лихвен доход и нетният доход от търговия* имат отрицателен принос за промяната в ROE.

▪ *Нетният лихвен марж* леко се понижава спрямо историческия връх през първото тримесечие с 3 bps до 1,66%. Цената на риска продължава да намалява и възлиза на 47 bps. След слабото възстановяване, наблюдавано през първата половина на годината, необслужваните кредити леко намаляват, което се дължи на по-ниските равнища при кредити за нефинансови предприятия (-1,6%), докато кредитите за домакинствата остават стабилни през тримесечието.

▪ *Качеството на активите остава стабилно*, като коефициентът на необслужваните кредити леко се повишава до 1,88%. Делът на кредитите във фаза 2 (обслужвани кредити с увеличен кредитен риск) възлиза на 9,2%, след като през тримесечието е слабо намаляло (9,3% през юни 2024 г.).

▪ На напълно натоварена база *коефициентът на базовия собствен капитал от първи ред* на банките от ЕС/ЕИП леко се понижава с 10 bps до 16,0% през последното тримесечие, оставайки значително над изискванията. Коефициентът на ликвидно покритие (LCR) и коефициентът на нетно стабилно финансиране (NSFR) намаляват съответно до 161,4% и 127,2%, но *остават значително над минималните изисквания.*

▪ ***За банките в България сравнителната информация е следната***:[15]

---

[15] ***Доходност:*** Възвръщаемостта на активите (ROA) на банковия сектор е 1.99% към края на септември 2024 г., а ***възвръщаемостта на собствения капитал (ROE) – на 16.40%*** (при съответно 2.18% и 18.64% към 30 септември 2023 г.). Приносът е основно на нарастването на нетния лихвен доход (10.9%) спрямо отчетения за деветте месеца на 2023 г.; повишава се също нетният доход от такси и комисиони, както и нетният доход от финансови инструменти, а другите нетни доходи отбелязват намаление.
Регулаторен капитал*:* Собственият капитал на банковата система в края на м. 09 2024 г. възлиза на 20.9 млрд. лв., като спрямо края на м. юни се увеличил с 1.5%; в края на декември 2024 г. възлиза на 23.2 млрд. лв. и спрямо края на септември се увеличава с 1.1 млрд. лв. (4.8%). Нарастването му се дължи главно на повишената печалба през периода, както и на растежа на натрупания друг всеобхватен доход и на другите резерви. Капиталовите съотношения се повишават и към 30.09. 2024 г***. съотношението на базовия собствен капитал от първи ред е 21.72%, на капитала от първи ред – 22.01%, а на общата капиталова адекватност – 23.44%.***
Качество на активите: Брутните необслужвани кредити и аванси в края на декември 2024 г. възлизат на 3.81 млрд. лв. (4.12 млрд. лв. в края на септември 2024 г.), а делът им в общата сума на брутните кредити и аванси се понижава до 3.16% (от 3.55% в края на септември). Нетната стойност на необслужваните кредити и аванси (след приспадане на присъщата им обезценка) в края на декември е 1.93 млрд. лв. (2.16 млрд. лв. в края на септември), а ***делът ѝ в общата нетна стойност на кредитите и авансите е 1.64% (1.91% в края на септември***).
Ликвидност: *Отношението на ликвидно покритие (LCR)* в края на декември 2024 г. е ***241.0%*** *(****244.1% в края на септември****).* Ликвидният буфер нараства до 56.9 млрд. лв., а нетните изходящи ликвидни потоци – до 23.6 млрд. лв. (от съответно 52.9 млрд. лв. и 21.7 млрд. лв. към 30 септември). Агрегираното за банковата система *отношение на нетно стабилно финансиране (NSFR)* към 30

1. ОЦЕНКА НА ОПЕРАЦИОННИЯ РИСК ЗА БАНКИТЕ В ОКОНЧАТЕЛНАТА РАМКА НА „БАЗЕЛ III“

БКБН измени международния стандарт за операционен риск, за да се преодолеят слабостите, появили се в резултат на световната финансова криза от 2008 – 2009 г. Освен липсата на чувствителност към риск при стандартизираните подходи, беше установена и липса на съпоставимост поради значителни различия в практиките на вътрешното моделиране съгласно усъвършенстваният подход за измерване (AMA). Поради това, а и за да се опрости уредбата за операционен риск, всички съществуващи подходи за оценка на капиталовите изисквания за операционен риск (включително базирания модел на усъвършенстван подход за измерване (AMA), са заменени с един-единствен метод, който не се основава на модел, а именно с *новия стандартизиран подход за оценка на операционен риск (SMA)*[16]. Новият, въведен от БКБН стандартизиран подход за оценка и измерване на операционен риск *съчетава показател, който се основава на размера на дейността на кредитната институция, с показател, който отчита историята на загубите на тази институция.* В окончателната рамка „Базел III“ е заложена известна свобода на преценка за начина, по който да се прилага показателят за историята на загубите на дадена институция[17].

Ето как новият Регламент (ЕС) 2024/1623 определя ***операционния риск (ОР)*** – рискът от загуба, произтичащ от неадекватни или недобре функциониращи вътрешни процеси (процедури), лица и системи, или поради външни събития, като тук спадат, без списъкът да е изчерпателен, *правният риск*, рискът, *свързан с модела,* или *рискът при информационните и комуникационните технологии (ИКТ),* но *не се включват стратегическият риск и рискът за репутацията.*

✓ *„**правен риск**“* е рискът от загуба, в т.ч. разноски, глоби, санкции или обезщетения с наказателен характер, които може да понесе дадена институция вследствие на събития, довели до съдебни производства, включително следното: а) надзорни действия и частни споразумения; б) бездействие, когато е необходимо действие с оглед на спазването на правно задължение; в) действие, предприето с цел да се избегне спазването на правно задължение; г) неправомерни действия с умисъл или небрежност, в т.ч. неподходящо предоставяне на финансови услуги или предоставяне на

септември 2024 г. е ***162.4%*** *(**при 159.2%*** в края на юни), като всички банки в България спазваха минималното регулаторно изискване от 100%.

Отношението на ливъридж (при напълно въведено определение за капитала от първи ред) към 30.09.2024 е *на ниво 10.45%* (при 10.62% в края на юни), като нивото продължава да показва високо капиталово покритие на общата експозиция.

[16] Вж. Регламент (ЕС) 2024/1623 на Европейския парламент и на Съвета от 31 май 2024 г. за изменение на Регламент (ЕС) № 575/2013 по отношение на изискванията за кредитен риск, риск от корекция на кредитната оценка, ***операционен риск*** и пазарен риск, както и за долна граница на капиталовото изискване.

[17] С цел да се осигурят равнопоставени условия в Съюза и да се опрости изчисляването на капиталовите изисквания за операционен риск, тази свобода на преценка следва да се упражнява еднакво за целите на минималните капиталови изисквания, като за нито една институция не се вземат предвид данните за минали загуби от събития, свързани с операционен риск.

неадекватна или подвеждаща информация за финансовия риск на продуктите, продавани от институцията; д) неспазване на изискване на национална или международна нормативна или законова разпоредба; е) неспазване на изискване, произтичащо от договорно споразумение или вътрешни правила и кодекси за поведение, установени съгласно националните или международните правила и практики; ж) неспазване на етичните правила.

✓ ***„риск, свързан с модела“***, е рискът от загуба вследствие на решения, които се основават предимно на резултатите от вътрешни модели, поради грешки в проектирането, разработването, оценката на параметрите, въвеждането, използването или наблюдението на тези модели, в т.ч. следното: а) неподходящо проектиране на избрания вътрешен модел и на неговите характеристики; б) неадекватно потвърждение на уместността на избрания вътрешен модел за дадения финансов инструмент, който ще бъде оценяван, за ценообразуването на дадения продукт или за приложимата пазарна конюнктура; в) грешки при въвеждането на избрания вътрешен модел; г) неточни пазарни оценки и измерване на риска в резултат на грешка при вписването на сделка в регистъра на сделките; д) използване на избрания вътрешен модел или на неговите резултати за цел, различна от целта, за която е бил предназначен или проектиран този модел, в т.ч. манипулиране на моделиращите параметри; е) ненавременно или неефективно наблюдение или утвърждаване на резултатите от модела или на прогностичната способност, за да се прецени дали избраният вътрешен модел продължава да е подходящ за целта.

✓ ***„риск при ИКТ“*** е рискът от загуба, свързан с всяко установимо и достоверно обстоятелство във връзка с използването на мрежи и информационни системи, което, ако се реализира, би могло да застраши сигурността на мрежите и информационните системи на всеки зависим от ИКТ инструмент или процес, на операциите и процесите или на предоставянето на услуги, като предизвика неблагоприятни последици за цифровата или физическата среда.

1.1. Идентифициране, измерване и наблюдение на операционния риск

Когато *оценяваме управлението на операционния риск в банката,* трябва да получим отговор на въпроса дали институцията разполага с подходяща рамка за идентифициране, оценяване, измерване и наблюдение на операционния риск в съответствие с размера и сложността на институцията (принципа на пропорционалност) и дали рамката отговаря на съответните минимални капиталови изисквания съгласно съответното европейско и национално транспониращо законодателство. За тази цел следва да се установи дали:

- институцията е въвела *ефективни процеси и процедури за цялостно идентифициране и оценка на експозицията към операционен риск* (в т.ч.

самооценки на риска и контрола (Risk and Control Self-Assessments RCSA) и за откриване и *точна категоризация на съответните събития* (т.е. събиране на данни за загубите, потенциални неблагоприятни събития без въздействие на загуба или дори събития, които генерират неочаквани печалби), включително гранични случаи с други рискове (например кредитни загуби, причинени или нараснали вследствие събитие, свързано с операционен риск); в тази връзка следва да се определи способността на институцията да установи ключовите фактори на съответните операционни загуби и да използва тази информация с цел управление на операционния риск;

- кредитната институция има *подходящи информационни системи и методологии* за количествено определяне или оценка на операционния риск, които отговарят на изискванията за определяне на съответния минимален капитал, каквито са изискванията в съответното европейско и националното приложимо законодателство;

- институцията е приложила *подходящи стрес тестове и сценариен анализ*, както е подходящо, за да се разбере въздействието на неблагоприятните операционни събития върху нейната доходност и собствен капитал, като вземат под внимание евентуалното неизпълнение на механизмите за вътрешен контрол и техниките за редуциране; където е уместно, следва да вземат под внимание съвместимостта на тези анализи с RCSA и с резултатите от анализа на сходните институции;

- ръководството с управленски и контролни функции на кредитната институция *разбира допусканията, лежащи в основата на системата за измерване,* и дали е информирано за степента на съответния риск, свързан с модела;

- банката е определила и прилага *непрекъснато и ефективно наблюдение на експозициите към операционен риск* в рамките на институцията, включително изнесени дейности и нови продукти и системи, като прилага и специфични ориентирани към бъдещето показатели (ключови рискови показатели и ключови контролни показатели) и съответните активатори за осигуряване на ефективни сигнали за ранно предупреждение;

- институцията е определила *подходящи действия в отговор на остатъчните рискове*, за да ги поддържа в рамките на лимитите, определени *в рисковия апетит*;

- институцията прилага *редовно отчитане на експозицията към операционен риск*, включително резултати от стрес тестове, пред ръководния орган с управленски и контролни функции и мениджърите на съответните дейности и процеси, както е уместно.

Капиталово изискване за операционен риск

За целите на тази част от публикацията се прилагат следните определения:

▪ *операционно събитие* е всяко събитие, свързано с операционен риск, което поражда загуба или множество загуби в рамките на една или няколко финансови години;

▪ *съвкупна брутна загуба* е сборът от всички брутни загуби, свързани с едно и също операционно събитие, в рамките на една или няколко финансови години;

▪ *съвкупна нетна загуба* е сборът от всички нетни загуби, свързани с едно и също операционно събитие, в рамките на една или няколко финансови години;

▪ *групирани загуби* са всички загуби, свързани с операционен риск, причинени от общи събития или първопричина, които биха могли да бъдат групирани в едно операционно събитие.

Новият стандартизиран подход за операционен риск определя капиталовите изисквания на банката за операционен риск, базирани на *два компонента*: (а) критерий/размер за доходите на банката; и (б) критерий/размер за историческите загуби на банката. От концептуална гледна точка се приема, че: а) операционният риск нараства с нарастващ темп с приходите на банката; и б) банките, които са имали исторически по-големи загуби от операционен риск, се предполага, че е по-вероятно да понесат загуби от операционен риск и в бъдеще.

Капиталовото изискване за операционен риск може да бъде обобщено по следния начин:

Капиталовото изискване за операционен риск е компонентът на бизнес индикатора.[18]

Кредитните институции изчисляват своя компонент на бизнес индикатора по следната формула:

$$BIC = \begin{cases} 0{,}12 \cdot BI, & \text{където } BI \leq 1 \\ 0{,}12 + 0{,}15 \cdot (BI - 1), & \text{където } 1 < BI \leq 30 \\ 4{,}47 + 0{,}18 \cdot (BI - 30) & \text{където } BI \leq 30 \end{cases}$$

където:

BIC = компонент на бизнес индикатора;

BI = бизнес индикатор, изчислен по следната формула:

$$BI = ILDC + SC + FC$$

където:

[18]Вж. Регламент (ЕС) 2024/1623 на Европейския парламент и на Съвета от 31 май 2024 г. за изменение на Регламент (ЕС) № 575/2013 по отношение на изискванията за кредитен риск, риск от корекция на кредитната оценка, ***операционен риск*** и пазарен риск, както и за долна граница на капиталовото изискване.

ILDC = *компонент на лихвите, лизинга и дивидентите*, изчислен по следната формула:

ILDC = min (IC, 0,0225 x AC) + DC

SC = компонента на услугите,

FC = финансов компонент,

IC = компонент на лихвите, който представлява приходите на институцията от лихви по всички финансови активи и други приходи от лихви, включително финансови приходи от финансов лизинг, приходи от оперативен лизинг и печалби от отдадените на лизинг активи, *минус* разходите на институцията за лихви по всички финансови пасиви и други разходи за лихви, включително разходи за лихви по финансов и оперативен лизинг, амортизация и загуби от оперирането на активи, предмет на лизинг, изчислен като средногодишната величина на абсолютните стойности на разликите за последните три финансови години;

AC = компонент на активите, който представлява сборът от общите брутни текущи заеми, аванси, лихвоносни ценни книжа, включително държавни облигации, и лизингови активи на институцията, изчислен като средна годишна стойност от сумите в края на всяка от съответните финансови години за последните три финансови години;

DC = компонент на дивидентите, който представлява приходите на институцията от дивиденти по инвестиции в акции и фондове, които не са консолидирани във финансовите отчети на институцията, включително приходите от дивиденти от неконсолидирани дъщерни предприятия, асоциирани и съвместни предприятия, изчислен като средна годишна стойност за последните три финансови години.

Компонентът на услугите се изчислява по следната формула:

SC = max (OI, OE) + max (FI, FE), където:

SC = компонент на услугите;

OI = другите оперативни приходи, които представляват средната годишна стойност за последните три финансови години на приходите на институцията от обичайни банкови операции, които не са включени в други елементи на бизнес индикатора, но са от сходно естество;

OE = другите оперативни разходи, които представляват средната годишна стойност за последните три финансови години на разходите и загубите на институцията от обичайни банкови операции, които не са включени в други елементи на бизнес индикатора, но са от сходно естество, и от операционни събития;

FI = компонент на доходите от такси и комисиони, който представлява средната годишна стойност за последните три финансови години на приходите на институцията, получени от предоставянето на консултации и

услуги, включително приходите, получени от институцията от предоставянето на финансови услуги на трети лица;

FE = компонент на разходите за такси и комисиони, който представлява средната годишна стойност за последните три финансови години на разходите на институцията, платени за получаването на консултации и услуги, включително таксите, платени от институцията за възлагане на финансови услуги на външни изпълнители, но без таксите, платени за възлагане на нефинансови услуги на външни изпълнители.

Финансовият компонент се изчислява по следната формула:

FC = TC + BC, където:

FC = финансовият компонент;

TC = компонент на търговския портфейл, който представлява средният годишен размер на абсолютните стойности за последните три финансови години на нетната печалба или загуба от търговския портфейл на институцията, според случая, определен по целесъобразност или съгласно счетоводните стандарти, включително от търгуеми активи и търгуеми пасиви, от отчитане на хеджиране и от курсови разлики;

BC = компонент на банковия портфейл, който представлява средния годишен размер на абсолютните стойности за последните три финансови години на нетната печалба или загуба от банковия портфейл на институцията, според случая, включително от финансовите активи и пасиви, оценявани по справедлива стойност през печалбата и загубата, от отчитане на хеджиране, от курсови разлики и от реализирани печалби и загуби от финансови активи и пасиви, които не се отчитат по справедлива стойност през печалбата и загубата.

Вече пояснихме, че за измерване на операционния риск *окончателната рамка Базел III* заменя всички съществуващи подходи с *новия стандартизиран подход на измерване* (SMA). По-точно подходът SMA заменя *усъвършенствания подход за измерване* (AMA – Advanced measurement approach), базиран на модел. Съгласно новата рамка за операционен риск банките могат да използват само SMA. Малките банки ще трябва да изчисляват MRC (Minimum Required Capital – Минимален изискуем капитал) въз основа *само на компонента на бизнес индикатора (BIC)*, докато големите банки ще трябва да изчисляват и така наречения компонент на загубата (LC). Изследването, направено от Европейския банков орган (EBA), показва, че промените на рамката генерират общо увеличение на MRC за операционен риск от 28,0% за банките от група 1 (големите банки, в т.ч. и Г-СЗИ – глобални, системно значими институции) и 5,2% за банките от група 2 (по-малките банки). Резултатите показват, че средно *засягат по-малко банките, които мигрират от AMA*, отколкото банките, които в момента използват други подходи (22,7% срещу 26,0%).

Таблица 1: Промени в T1 MRC, определени само за операционен риск (% от MRC T1, определени за операционен риск съгласно CRR 2/CRD 5)

Bank group	**AMA**	**Others**	**Total**
All banks	22.7	26.0	24.3
Group 1	23.5	34.3	28.0
Of which: G-SIIs	24.6	48.3	30.7
Group 2	-0.4	5.9	5.2

Източник: Данни на EBA QIS (декември 2022 г.), извадка от 158 банки

Банкова група	АМА	Други	Общо
Всички банки	22.7	26.0	24.3
1 група	23.5	34.3	28.0
От които: Г-СЗИ	24.6	48.3	30.7
2 група	- 0.4	5.9	5.2

Има няколко причини за по-голямото въздействие на операционния риск върху група 1, отколкото върху група 2. Първо, банките от група 1 са предимно големи банки с по-сложни и по-ориентирани на такси бизнес модели, докато банките от група 2 са склонни да предоставят универсална и диверсифицирана банкова услуга, които не разчитат значително на такси. За управляваните от такси бизнес модели новият индикатор е зададен на по-консервативно ниво за справяне с по-високите оперативни рискове, които обикновено се наблюдават при тези видове бизнес модели. Второ, големите банки като цяло са по-засегнати от високия бизнес показател.

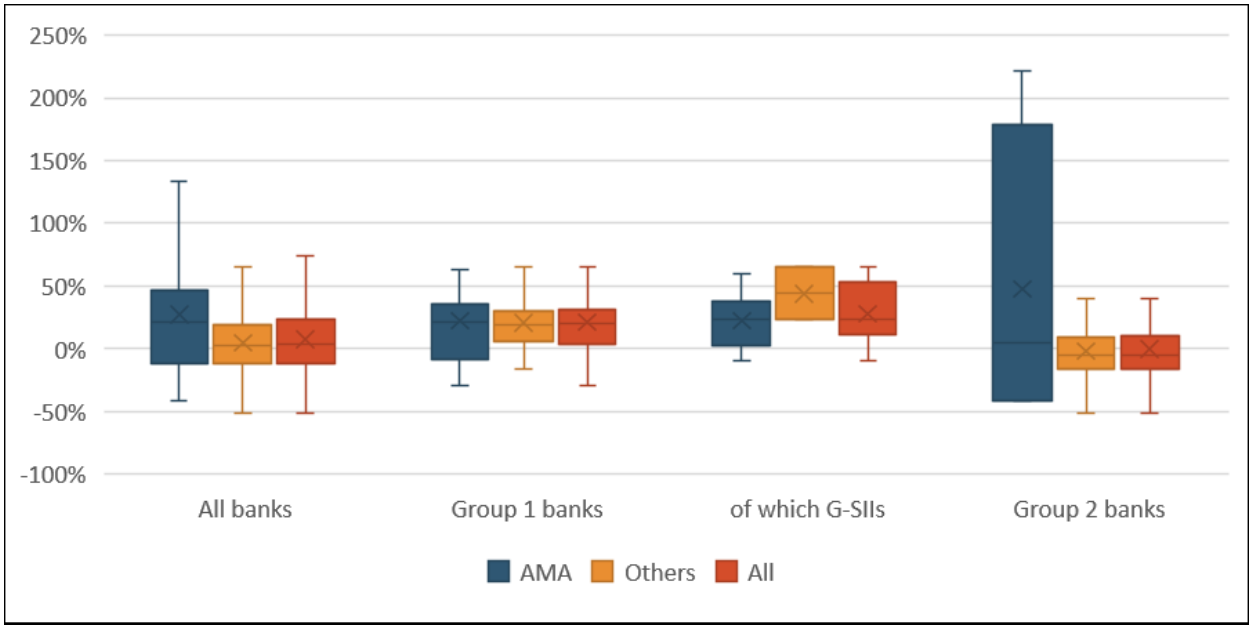
Данните също така показват, че за банките от група 1, и по-специално за G-SII, делът на MRC за операционен риск в общия MRC е по-висок, отколкото за банките от група 2. Това е така, защото бизнес моделите на банките от група 1 предлагат универсални услуги и следователно имат относително хомогенни характеристики на операционния риск, докато банките от група 2 следват различни бизнес модели, предлагащи специализирани или по-разнообразни видове услуги. Някои банки от група 2 са особено специализирани, като предлагат само услуги, базирани на такси, и никакви услуги, които биха били изложени на кредитен или пазарен риск. Това прави операционният риск най-доминиращата рискова категория за тях.

Извадката, на която се доверяваме, обхваща почти цялата съвкупност от големи АМА банки от Група 1, които са изправени пред по-значителни увеличения на капитала в сравнение с банките от Група 2, които или използват АМА за по-прости експозиции на оперативен риск, или използват прости стандартизирани подходи. Освен това някои от банките в момента може да бъдат обект на допълнителни капиталови изисквания по Стълб 2

поради слабости в тяхното управление на оперативния риск; тези допълнителни изисквания не са взети предвид в настоящия анализ. В резултат на това общото въздействие, показано в таблица 1, може да бъде надценено в сравнение с действителното въздействие.

Разпределението на капиталовите изисквания за операционен риск за банки, прилагащи АМА от група 2, е очевидно по-високо от съответната стойност за банки, прилагащи АМА от група 1 (Фигура 1).

Фигура 1: Разпределение на промените в T1 MRC (капиталово изискване за базов собствен капитал от първи ред - CET1 Common Equity Tier 1), определени само за операционен риск (в % от текущия MRC за операционен риск)



Източник: Данни на EBA QIS (декември 2022 г.), извадка от 158 банки

1.2. Оценка на операционния риск

Общи положения

Компетентните органи оценяват операционния риск във всички бизнес направления и операции на кредитната институция, като вземат предвид констатациите от оценката на системите за вътрешно управление и механизмите за контрол в рамките на институцията. Когато извършват тази оценка, те трябва да определят как може да се прояви операционният риск (икономически загуби, потенциално неблагоприятно събитие, загуба на бъдещи приходи, печалба) и също така да вземат предвид евентуалното въздействие по отношение на други свързани рискове (например кредитно-операционен риск, пазарно-операционен риск „гранични случаи“).

При оценката на операционния риск е особено важно да се оцени *риска, свързан с ИКТ*, тъй като ефективността и сигурността на ИКТ се считат за

първостепенни за извършването на дейността на банката; като оценят потенциалното въздействие на рисковете, свързани с ИКТ, върху критичните дейности на институцията и да разгледат потенциалното финансово, репутационно, регулаторно и стратегическо въздействие върху институцията, както и потенциала за прекъсване на дейността (по-подробното представяне на риска, свързан с ИКТ, ще изложим в т. 2 от настоящата студия).

Подходящо е органите за управление да оценяват и репутационния риск заедно с операционния риск поради силните връзки между тях (така например повечето събития, свързани с операционен риск, имат силно въздействие върху репутацията). Въпреки това резултатът от оценката на репутационния риск не трябва да се отразява в определянето на рейтинга за операционния риск, а трябва да се счита за част от анализа на бизнес модела (АБМ) и/или оценката на ликвидния риск, където е уместно, тъй като основните ефекти, които може да окаже, са редуциране на приходите и загуба на доверие в/или недоволство от институцията от страна на инвеститори, вложители или участници на междубанковия пазар.

Оценка на присъщия операционен риск

Компетентните органи (органите за управление и контрол) на кредитната институция следва да оценят естеството и степента на операционния риск, на който институцията е или може да бъде изложена. За тази цел те следва да изградят цялостно разбиране на бизнес модела на институцията, нейните операции, нейната култура по отношение на риска и средата, в която тя работи, тъй като всички тези фактори определят експозицията към операционен риск.

Оценката на *присъщия операционен риск* се състои от две стъпки:

а. предварителна оценка; и

б. оценка на естеството и значимостта на експозициите към операционен риск и подкатегориите на операционния риск, на които е изложена институцията.

Предварителна оценка

За да се определи обхватът на оценката на операционния риск на дадена кредитна институция, най-напред следва да се установят *източниците на операционния риск*, на който институцията е изложена, като се възползват от знанията, придобити от оценката на други елементи на Процеса на надзорен преглед и оценка (ПНПО), от сравнението на позицията на институцията спрямо сходните институции, включително информацията, предоставена от функциите по вътрешен одит и нормативно съответствие, както и надзорните органи в областта на борбата с изпирането на пари и финансирането на тероризма, и от други подходящи източници на информация.

Ето какво следва да се вземе под внимание:

(а) основната *стратегия за операционен риск* и рисковият апетит по отношение на операционния риск;

(б) *бизнес средата и външната среда* (включително географското местоположение на предприятието майка и неговите дружества, както и на операциите в областта на ИКТ и центровете за данни), в която институцията управлява, и използвани канали за разпространение;

(в) *капиталовото изискване за операционен риск* (разграничавано според използвания подход) в сравнение с общото капиталово изискване, а където е подходящо – вътрешният капитал за операционен риск в сравнение с общия вътрешен капитал, като се вземат предвид историческите тенденции и прогнози, ако има такива;

(г) *равнището и промяната в брутния доход, активите и загубите* от операционен риск през последните няколко години на агрегирано равнище, но също така и за съществените субекти и групите дейности;

(д) *скорошни значими корпоративни събития* (като сливания, придобивания, прехвърляния и преструктуриране), които може да доведат до промяна в профила на операционен риск на институцията в краткосрочен или в средносрочен до дългосрочен план (напр. тъй като системите, процесите и процедурите няма да бъдат напълно приравнени към политиките за управление на риска на предприятието майка в краткосрочен план);

(е) *промени в значими елементи на ИТ системите* и/или процесите, които могат да доведат до промяна в профила на операционен риск (напр. тъй като нова или променена ИТ система не е била правилно тествана или защото недостатъчното обучение по новите системи/процеси и процедури може да доведе до грешки);

(ж) *неспазвания на приложимо законодателство или на вътрешни разпоредби*, докладвани от надзорни органи (включително надзорни органи в областта на борбата с изпирането на пари и финансиране на тероризъм), външни одитори и функцията за вътрешен одит или които са изнесени при оповестяване на публична информация;

(з) *амбициозността на бизнес плановете и агресивните стимули и компенсационни схеми* (напр. по отношение на цели за продажба, включително приемане на клиенти, определени от институцията като имащи висок риск от ИП/ФТ, или разпростиране към юрисдикции с висок риск от ИП/ФТ, или разпространение на нови продукти/услуги, имащи високо ниво на присъщ риск от ИП/ФТ, намаляване на числеността на персонала и др.), което може да увеличи риска от несъответствие, човешка грешка и злоупотреби на служителите;[19]

[19] EBA/GL/2022/03, Revised GL on SREP, Насоки относно общите процедури и методологии за процеса на надзорен преглед и оценка (ПНПО) и надзорните стрес тестове.

(и) *процесите и процедурите, продуктите (продадени на клиенти или търгувани) и ИТ системите* (включително употребата на нови технологии) до степента, до която те може да доведат до злополуки, грешки, забавяния, грешна спецификация, нарушения на сигурността, повишена експозиция на измами, ИП/ФТ и други видове финансови престъпления и др.;

(к) *потенциалното въздействие на споразуменията за възлагане на дейности на външни изпълнители* върху операционния риск на институциите, както и надзора на институциите върху резултатите от дейността на доставчиците на услуги, включително степента на осведоменост за операционния риск, свързан с възложени на външни изпълнители дейности, и за цялостната рискова експозиция към доставчиците на услуги в съответствие с *Насоките на ЕБО за възлагане на дейности на външни изпълнители.*

Когато е уместно, тези аспекти трябва да се анализират по бизнес направления и географско местоположение, както и по категория на вида събитие, при условие че е налична подходяща информация, и да се сравни позицията на институцията с тази на сходните институции.

Оценка на подкатегориите операционен риск

Операционният риск следва да се установява и оценява *във всички подкатегории операционен риск* (и когато е уместно да включва тези, които са определени по видове събития и допълнителни разбивки на тези видове събития) и *свързаните фактори на риска*, като вниманието се съсредоточи върху онези подкатегории, които се считат за най-значими за институцията. Значимостта на дадена подкатегория следва да се оценява, като се използва количествената информация, събрана по време на предварителната оценка, включително равнището на загубите по подкатегории по отношение на капиталовите изисквания и брутния доход.

Подходът на оценката следва да включва специално внимание на някои специфични аспекти на операционния риск поради тяхното широко разпространение и тяхната релевантност за повечето институции, както и поради евентуалното им пруденциално въздействие. Аспектите, върху които оценката *винаги* следва да бъде съсредоточена, включват: а. риск, свързан с ИКТ; б. риск от неправомерно поведение; и в. риск, свързан с модела.

Риск, свързан с ИКТ

Компетентните органи следва да оценят дали информационните и комуникационните технологии на институцията са ефективни и надеждни, както и дали тези системи напълно подпомагат способностите за събиране на данни за риска в нормално време, както и по време на стрес, като вземат предвид това, че *рискът, свързан с ИКТ, е основен фактор за операционен риск;* да оценят дали институцията е установила ефективно управление на непрекъсваемостта на дейността с тествани планове за действие при непредвидени обстоятелства и за непрекъсваемост на дейността, както и

планове за възстановяване при бедствие, за всички свои критични функции, включително критични функции и ресурси, възложени на външни изпълнители, и дали тези планове могат надеждно да ги възстановят.

Риск от неправомерно поведение

При този риск се оценява уместността и значимостта на експозициите на институцията към риска от неправомерно поведение, като се вземат предвид няколко фактора:

- ✓ неправомерните продажби на продукти, включително принудителната кръстосана продажба на продукти на клиенти на дребно, като например пакетни банкови сметки или допълнителни продукти, от които клиентите не се нуждаят;
- ✓ конфликт на интереси при извършването на дейността;
- ✓ манипулиране на сравнителни лихвени проценти, обменни курсове или други финансови инструменти или индекси с цел повишаване на печалбите на институцията;
- ✓ бариери пред смяната на финансови продукти, докато съществуват, и/или пред смяната на доставчици на финансови услуги;
- ✓ лошо проектирани дистрибуторски канали, които може да доведат до конфликт на интереси с фалшиви стимули;
- ✓ автоматични подновявания на продукти или неустойки за прекратяване; и/или
- ✓ несправедливо обработване на клиентски рекламации.

Трябва да се има предвид и това, че рискът от неправомерно поведение *обхваща широк спектър от проблеми* и може да възникне от много бизнес процеси и продукти, затова при оценката следва да се използват резултатите от анализа на бизнес модела (АБМ) и да се проучат политики, пораждащи стимули, за да се разберат във висока степен в източниците на риск от неправомерно поведение. Известни са показатели, които сигнализират за съществуването на риск от неправомерно поведение: а. санкции, наложени от съответните органи на институцията за практики на неправомерно поведение; б. санкции, наложени на сходни институции за практики на неправомерно поведение; в. рекламации срещу институцията по отношение на изложени на риск цифри и суми. Подходящо е да се приложи *прогнозен подход,* като се вземе предвид вероятното въздействие на регулаторните развития и дейността на съответните органи по отношение на защитата на потребителя и предоставянето на финансови услуги като цяло.

Произтичащ от модела риск

В рамките на операционния риск компетентните органи следва да оценяват две отделни форми на риск, свързан с модела: (а). риск, *свързан с подценяването на капиталовите изисквания* чрез усъвършенствани

регулаторни подходи за измерване; и (б). риск от загуби, *свързани с разработването, прилагането или неправилното използване на други модели* от институцията за вземане на решения (напр. ценообразуване на продукт, оценка на финансови инструменти, наблюдение на рисковите лимити и др.), в които случаи следва да се направи преглед на тези модели, да се оцени тяхната значимост и да се оцени рамката за управление на риска, приета от институцията.

Когато се извършва оценка на риска, свързан с модела, следва да се вземе предвид резултатът от оценката на *други рискове за капитала и рисковете за ликвидността и финансирането*, по-специално по отношение на адекватността на методологиите, които се използват за измерване на риска, ценообразуване и оценка на активи и/или пасиви. Резултатите от тази оценка следва да послужат за основа на констатациите относно операционния риск.

В контекста на анализа на операционния риск е необходимо да се изследва и *относимостта и значимостта на експозициите на кредитната институция към риск от ИП/ФТ, от една страна, от пруденциална гледна точка* в обхвата на операционния риск, като се използва съответната информация, получена от надзорните органи в областта на борбата с изпирането на пари и финансирането на тероризма и на тази основа се прецени дали те пораждат опасения от пруденциален характер, свързани с риска от ИП/ФТ. *От друга страна,* следва да се има предвид, че всяка институция може да бъде изложена на риск от ИП/ФТ независимо от нейния размер или финансова стабилност. Ето защо следва да се обръща достатъчно внимание и на кредитни институции, които се възприемат като финансово стабилни и с добра репутация, но тези институции могат да бъдат специален обект за целите на ИП/ФТ: например банки, които много успешно привличат нови клиенти или разширяват пазарния си дял чрез използване на нетрадиционни канали за дистрибуция, тъй като това може да бъде свързано със слаб контрол на комплексната проверка на клиента на етапа, когато той става клиент на институцията за първи път, или имат недостатъци в информационната система или рамката за вътрешен контрол в областта на борбата с изпирането на пари и финансирането на тероризма (БИП/БФТ)[20].

[20] Вж. Регламент (ЕС) 2024/1624 на ЕП и на Съвета от 31 май 2024 г. за предотвратяване на използването на финансовата система за целите на изпирането на пари или финансирането на тероризма.
Насоки на ЕБО относно рисковите фактори, свързани с ИП/ФТ (EBA/GL/2021/02); EBA/GL/2023/03 и EBA/GL/2024/01, Насоки за изменение на Насоки EBA/2021/02 съгласно член 17 и член 18, параграф 4 от Директива (ЕС) 2015/849 относно комплексната проверка на клиента и факторите, които кредитните и финансовите институции следва да вземат предвид при оценката на риска от изпиране на пари и финансиране на тероризма, свързан с индивидуални делови взаимоотношения и случайни сделки („Насоките относно рисковите фактори, свързани с ИП/ФТ“).

Стратегия за управление и рисков апетит за поемане на операционен риск

Една добре формулирана *надеждна стратегия за управление и ниво на рисков апетит* за поемане на операционен риск трябва да включва следните елементи, които да бъдат обект на оценка от органите за управление на кредитната институция:

- ръководният орган изразява ли ясно стратегията за управление и нивото на рисковия апетит за поемане на операционен риск, както и процеса за техния преглед (напр. в случай на цялостен преглед на стратегията за риска, притеснения по отношение тенденцията на загубата и/или капиталовата адекватност и др.);

- *правилно ли се прилага и наблюдава стратегията за управление* на операционния риск, одобрена от ръководния орган от различните нива на управление, и дали това гарантира, че мерките за редуциране на операционния риск на институцията са съвместими с установената стратегия;

- тези стратегии *подходящи и ефикасни* ли са по отношение на естеството и съществеността на профила на операционния риск и дали институцията наблюдава тяхната ефективност през времето и тяхното съответствие с *нивото на толеранс към операционния риск;*

- стратегията за управление на операционния риск на институцията обхваща ли всички дейности, процеси и системи на институцията – включително на прогнозна база чрез стратегическия план, където операционният риск е или може да бъде значителен;

- институцията разполага ли с подходяща рамка, за да гарантира, че стратегията за управление на операционния риск се комуникира ефективно със съответните служители;

- институцията разпределила ли е достатъчно ресурси за прилагането на елементите на стратегията и дали съответните взети решения са независими от ползите от минималните капиталови изисквания, които може да се натрупат.

2. ОПЕРАТИВНА УСТОЙЧИВОСТ НА ИНФОРМАЦИОННИТЕ И КОМУНИКАЦИОННИ ТЕХНОЛОГИИ (ИКТ)

2.1. Регламенти и директиви за оперативната устойчивост на цифровите технологии във финансовия сектор

В т. 1.2. представихме риска, свързан с ИКТ като подкатегория на операционния риск. Защо ИКТ, като част от информационната система и системите за информационна сигурност, са важни за банките?

В цифровата ера информационните и комуникационните технологии (ИКТ) са в основата на сложни системи, използвани в ежедневните дейности.

ИКТ поддържат работата на икономиките ни в ключови сектори, включително финансовия сектор, и подобряват функционирането на вътрешния пазар.

Включването на цифрови технологии в работните процеси в банковия сектор поставя началото *на нова ера на оперативна ефективност*, реорганизирайки изпълнението, наблюдението и контрола върху финансовите процеси. Според обобщената дефиниция на корпорация IBM дигиталната трансформация в банкирането се отнася до интегрирането на цифрови технологии и иновативни стратегии в сектора на финансовите услуги за подобряване на оперативната ефективност, подобряване на преживяванията на клиентите и адаптиране към променящия се пазарен пейзаж[21]. Този процес включва модернизиране на традиционните банкови системи, процеси и бизнес модели и това позволява на банките да предоставят безпроблемни, удобни и сигурни услуги чрез различни цифрови канали.

Банковият сектор се намира в ключов момент, в който интегрирането на дигитални инструменти се превръща в модел за повишаване на оперативната ефективност и позициониране на институциите на челно място в трансформацията на индустрията. Ключовите аспекти на цифровата трансформация в банкирането включват:

(1) *Многоканално банкиране*: предоставяне на клиентите на интегрирано, безпроблемно изживяване през множество канали, като онлайн банкиране, мобилни приложения, банкомати и физически клонове.

(2) *Персонализиране*: използване на анализи на данни, изкуствен интелект (AI) и машинно обучение (ML) за адаптиране на продукти и услуги към индивидуалните потребности и предпочитания на клиентите.

(3) *Автоматизация и оптимизация на процеси*: внедряване на технологии като роботизирана автоматизация на процеси (RPA) и AI за рационализиране на вътрешните операции, намаляване на разходите и подобряване на ефективността. Според някои автори дигитализацията на банковия сектор чрез приложението на бизнес трансформацията и бизнес иновацията спомага за дългосрочното запазване на пазарните дялове на кредитните институти в световен мащаб.

(4) *Усъвършенствани мерки за сигурност*: приемане на иновативни решения и практики за киберсигурност за защита на клиентските данни, предотвратяване на измами и гарантиране на съответствие с нормативните разпоредби.

(5) *Вземане на решения, управлявани от данни*: използване на анализ на големи данни и усъвършенствани алгоритми за вземане на информирани

[21] Finn, T., A. Downie. (2024). What is digital transformation in banking and financial services? https://www.ibm.com/think/topics/digital-transformation-banking

стратегически решения, оптимизиране на управлението на риска и стимулиране на иновациите.

(б) *Сътрудничество с финтех компании и отворено банкиране*: партньорство с финтех стартиращи фирми и възприемане на отворени банкови инициативи за насърчаване на иновациите, подобряване на изживяването на клиентите и разширяване на предлаганите услуги.

Някои от ключовите технологии и решения, движещи финансовата цифрова трансформация, са:

√ *Облачните изчисления* стават съществени за инфраструктурата на цифровото банкиране, предоставяйки при необходимост изнесени ресурси за интегриране на софтуерни решения на различни локации. Чрез използването на *облачни технологии* банките могат бързо да разгръщат нови услуги, да осигурят непрекъсната връзка клиент – банка и да премахнат физическите ограничения в своята бизнес екосистема.

√ *Интерфейсите за приложно програмиране* (API) са софтуерни посредници, които определят правилата и протоколите за взаимодействието на различните софтуерни компоненти. Използвайки тази технология, банките могат да се интегрират с външни приложения, позволявайки нови цифрови услуги и функционалности за своите клиенти. API действат като защитени портали, позволявайки безпроблемно споделяне на данни между банки, финтех компании и други доставчици на трети страни.

√ *Изкуственият интелект (AI) и машинното обучение (ML)* тласкат банковата индустрия към бърза дигитализация, позволявайки реализацията на повече иновации и нови оперативни модели. Внедряването на способности на AI може да създаде нова добавена стойност за банките, възлизаща на $ 200 – $ 340 милиарда годишно, което означава 9 – 15% от оперативните печалби[22]. В отношенията си с клиентите банковият сектор използва тази трансформираща технология, за да рационализира процесите, да подобри сигурността и да предостави услуги с високо качество. *Някои AI приложения в банкирането включват:*

▪ *Чат ботове*: захранвани с изкуствен интелект чат ботове с обработка на естествен език осигуряват 24/7 поддръжка на клиенти, обработват запитвания, отварят нови акаунти и безпроблемно насочват оплаквания[23].

▪ *Откриване и предотвратяване на измами*: чрез анализиране на огромни масиви от данни AI може да идентифицира подозрителни модели, аномалии в данните и връзки между обекти, подобрявайки възможностите за предотвратяване на измами.

---

[22] Shkurdoda, A., A. Puczyk. (2024). Digital Transformation in Banking Industry: Revolutionizing Financial Services.https://neontri.com/blog/digital-banking-

[23] Вейсел, А. (2023). Влиянието на изкуствения интелект върху счетоводството, Списание ИДЕС, бр. 3/2023 г.

▪ *Подобряване на изживяването*: AI помага да се анализират предпочитанията на клиентите, да се извършва сегментиране и да се правят целеви маркетингови кампании, като се подобрява изживяването на потребителите.

▪ *Автоматизация на роботизирани процеси* променя ръчните операции като въвеждане на данни, комуникации за обслужване на клиенти и обработка на транзакции. Чрез прилагането му банките могат значително да намалят разходите за обработка, да подобрят производителността на служителите и да сведат до минимум човешките грешки, свързани с операционния риск.

▪ *Блокчейн технология*: благодарение на разпределеното си съхранение на данни в множество блокови точки, съхранявани в добре защитена децентрализирана мрежа, тази технология помага за укрепване на сигурността на банковите данни и сметки. За своите ползватели тя осигурява прозрачен, защитен и децентрализиран достъп за проследяване на записи на транзакции в мрежата, което позволява откриването на подозрителна дейност. Освен решения за борба с измамите блокчейн може да се използва и за активиране на интелигентни договори – сигурно, автоматизирано изпълнение на финансови споразумения.

▪ *Интернет на нещата (IoT) революционизира банкирането*, като позволява безпроблемна интеграция между финансови услуги и смарт устройства. Тази технология позволява на банките да вградят интелигентни софтуерни инструменти в своята инфраструктура и точки за контакт с клиенти, създавайки унифицирано, цифрово подобрено изживяване, управлявано от свързани устройства. Популярните приложения на IoT в банкирането включват: мобилни портфейли за безпроблемни плащания без дебитни/кредитни карти; функция за плащане с безконтактни транзакции; интелигентни банкомати, които наблюдават активността на клиентите, използвайки данни от околната среда като температура, осветление и сензори за движение; биометрично удостоверяване чрез пръстови отпечатъци, Face ID, сканиране на ретината или гласово разпознаване за сигурна проверка на потребителя.

В обобщение: като цяло *дигиталната трансформация в банкирането е продължаващ процес,* който се стреми да промени пейзажа на финансовите услуги чрез възприемане на нови технологии, иновативни бизнес модели и ориентирани към клиента подходи, за да отговори на променящите се изисквания на дигиталната ера. Цифровият проход[24] в Европа е водещ приоритет за ЕС през следващото десетилетие и приоритетна област за инвестиции според Плана за възстановяване и устойчивост (ПВУ). В съответствие с цифровата стратегия на ЕС развитието на цифровите финанси следва да се основава на европейските ценности и на строго регламентиране по отношение на рисковете. Използването на ИКТ придоби

[24] Цифровите финанси, често наричани финансови технологии, представляват прилагането на цифрови технологии към финансовите дейности.

до такава степен ключова роля в предоставянето на финансови услуги, че днес се е превърнало в критично важен елемент за осъществяването на обичайните ежедневни функции на всички финансови субекти. Цифровизацията понастоящем обхваща например плащанията, които все повече преминават от методи, базирани на плащане в брой и използване на хартиен носител, към използването на цифрови решения, както и клиринг и сетълмент на ценни книжа, електронна и алгоритмична търговия, операции по кредитиране и финансиране, партньорско финансиране, присъждане на кредитен рейтинг, уреждане на застрахователни претенции и вътрешни за дружествата операции. А цифровизацията доведе и до задълбочаване на взаимните връзки и зависимости както в рамките на самия финансов сектор, така и с доставчици на инфраструктура и услуги, които са трети страни.

От друга страна, засилената цифровизация и взаимосвързаност засилват риска в областта на ИКТ, което прави обществото като цяло и финансовата система в частност по-уязвими на киберзаплахи или смущения на ИКТ. Въпреки че повсеместното използване на системите на ИКТ и високата степен на цифровизация и свързаност са днес основни характеристики на дейностите на финансовите субекти на Съюза, предприемането на мерки по отношение на устойчивостта на използваните от тях цифрови технологии и интегрирането на тази устойчивост в по-широките им оперативни рамки все още не е завършена[25]. Този извод е направен през м. декември 2022 г., когато е приет Регламент (ЕС) 2022/2554 относно *оперативната устойчивост на цифровите технологии* във финансовия сектор (Регламентът), известен още като *Актът за цифрова оперативна устойчивост (DORA)* – The Digital Operational Resilience Act (или Акт за оперативната устойчивост на цифровите технологии).

В резултат на постоянно нарастващия риск от кибератаки с приемането на DORA (Регламент 2022/2554) ЕС укрепва информационната сигурност на финансови субекти като банките, застрахователните дружества и инвестиционните посредници. Приемайки акта за оперативната устойчивост на цифровите технологии (DORA), ще се гарантира способността на финансовия сектор в Европа да ***запази устойчивостта си в случай на сериозни оперативни смущения***. „Живеем в несигурни времена. Банките и другите дружества, които предоставят финансови услуги в Европа, вече имат планове за своята информационна сигурност, но трябва да направим още една крачка напред. Благодарение на хармонизираните правни изисквания, които приехме днес, нашият финансов сектор ще има по-голяма способност да продължи да функционира по всяко време. Ако бъде предприета широкомащабна атака срещу европейския финансов сектор, ние ще бъдем подготвени за това“[26].

---

[25] Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14.12.2022 г. относно *оперативната устойчивост на цифровите технологии във финансовия сектор* и за изменение на регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014, (ЕС) № 909/2014 и (ЕС) 2016/1011.
[26] Збинек Станюра, министър на финансите на Чехия.

Финансовият сектор на Съюза се регулира от единна нормативна уредба и се управлява от Европейска система за финансов надзор. Въпреки това разпоредбите относно оперативната устойчивост на цифровите технологии и сигурността на ИКТ все още не бяха хармонизирани изцяло или последователно независимо от факта, че оперативната устойчивост на цифровите технологии е от ключово значение за гарантиране на финансовата стабилност и интегритета на пазара в цифровата ера, като е не по-малко важна например от общите пруденциални стандарти или стандартите за пазарно поведение. Поради това единната нормативна уредба и надзорната система следваше да бъдат развити така, че да обхванат и оперативната устойчивост на цифровите технологии чрез укрепване на мандатите на компетентните органи, което да им позволи да упражняват надзор върху управлението на риска в областта на ИКТ във финансовия сектор с цел да се защитят интегритетът и ефикасността на вътрешния пазар и да се подпомогне безпроблемното му функциониране.

Единната нормативна уредба *не беше придружена от всеобхватна уредба на риска в областта на ИКТ или на операционния риск,* поради което беше необходимо *допълнително хармонизиране на ключовите изисквания* за всички финансови субекти във връзка с оперативната устойчивост на цифровите технологии.

Целта на Регламента (DORA) е да се к*онсолидират и подобрят изискванията във връзка с риска в областта на ИКТ, като част от изискванията за операционния риск,* които към момента на приемането се разглеждат отделно в различни правни актове на Съюза. Макар че тези актове обхващат основните категории финансов риск (напр. кредитен риск, пазарен риск, ликвиден риск, кредитен риск от контрагента, риск във връзка с пазарното поведение), към момента на приемането им в тях не са включени всеобхватно всички компоненти на оперативната устойчивост[27]. Недостатък при доразвиването на нормите за операционния риск в правните актове на Съюза често беше да се предпочита традиционният количествен подход по отношение на риска (определяне на капиталово изискване за покриване на риска в областта на ИКТ) *вместо целенасочени норми за качество във връзка с капацитета за защита, установяване, ограничаване, възстановяване на информацията и възобновяване на обичайното функциониране при инциденти, засягащи ИКТ, или за капацитета за докладване и цифрово тестване.*

Постижението е, че посредством *консолидирането и актуализирането* на различните правила за риска в областта на ИКТ всички разпоредби, посветени на цифровия риск във финансовия сектор, *за първи път са последователно обединени в един единствен законодателен акт. Като обобщение*: с Регламента (ЕС) 2022/2554 се запълват празнотите или се

[27] Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14.12.2022 г. относно оперативната устойчивост на цифровите технологии във финансовия сектор и за изменение на регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014, (ЕС) № 909/2014 и (ЕС) 2016/1011.

отстраняват несъответствията в някои от предходните правни актове, включително по отношение на използваната в тях терминология, и *изрично се прави позоваване на риска в областта на ИКТ чрез целенасочени правила за капацитета за управление на риска в областта на ИКТ, докладването на инциденти, тестването на оперативната устойчивост и наблюдението на риска в областта на ИКТ, пораждан от трети лица.* Очаква се Регламентът да *повиши осведомеността относно риска в областта на ИКТ* и да отчита факта, че инцидентите с ИКТ и липсата на оперативна устойчивост могат да застрашат стабилността на финансовите субекти.

В мерките си във връзка с риска в областта на ИКТ финансовите субекти следва да *спазват един и същ подход и принципни правила*, като отчитат размера и цялостния си рисков профил, както и естеството, мащабите и сложността на своите услуги, дейности и операции. *Съгласуваността допринася за засилване на доверието във финансовата система* и за съхраняване на нейната стабилност, особено във времена на голяма зависимост от системите, платформите и инфраструктурите на ИКТ, която повишава риска при цифровите технологии. Спазването на елементарна киберхигиена би следвало също така да оптимизира съотношението „разходи – ползи“, като спести необходимостта от налагане на значителни разходи върху икономиката.

По принцип приемането на регламент (за разлика от Директива) спомага за *намаляване на нормативната сложност, насърчава сближаването на надзорните практики, повишава правната сигурност,* като освен това допринася за ограничаване на разходите за спазване на изискванията – особено за финансовите субекти с трансгранична дейност, и за намаляване на нарушаването на конкуренцията. Авторът на това изследване също приема, че *изборът на регламент за създаване на обща рамка за оперативната устойчивост на цифровите технологии при финансовите субекти е най-добрият начин за осигуряване на еднообразно и съгласувано прилагане* от страна на финансовия сектор на Съюза на всички компоненти на управлението на риска в областта на ИКТ.

DORA (Регламентът) определя единни изисквания за сигурността на мрежите и информационните системи на дружествата и организациите, работещи във финансовия сектор, както и на възлови трети страни, които им предоставят услуги, свързани с ИКТ. Тези *изисквания са еднородни във всички държави – членки на ЕС,* като основната цел е предотвратяването и смекчаването на киберзаплахите.

Същевременно съответните европейски надзорни органи (ЕНО) – Европейският банков орган (ЕБО), Европейският орган за ценни книжа и пазари (ESMA) и Европейският орган за застраховане и професионално пенсионно осигуряване (EIOPA), разработиха ***технически стандарти,***

които да се спазват от всички институции за финансови услуги[28] – от банковото дело до застраховането и управлението на активи. Съответните национални компетентни органи следва да поемат надзора на съответствието и да прилагат Регламента според необходимостта.

Контекст

Комисията внесе предложението за DORA през м. септември 2020 г. То беше част от по-големия пакет за цифровите финансови услуги, който имаше за цел разработването на европейски подход, който да насърчава технологичното развитие и да гарантира финансова стабилност и защита на потребителите. Наред с предложението за оперативна устойчивост на цифровите технологии пакетът съдържаше стратегия за цифровизиране на финансовите услуги, предложение относно пазарите на криптоактиви (ПКА) и предложение относно технологията на разпределения децентрализиран регистър (ТРР)[29].

Този пакет трябваше да запълни празнина в съществуващото законодателство на ЕС, като гарантира, че действащата правна рамка не създава пречки за използването на нови цифрови финансови инструменти и същевременно дава гаранции, че тези нови технологии и продукти попадат в обхвата на финансовото регулиране и *договорености*те *за управление на операционния риск на дружествата,* осъществяващи дейност в ЕС. По този начин пакетът имаше за цел: •да стимулира конкурентоспособността и иновациите във финансовия сектор в Европа; •да предостави на потребителите и дружествата по-голям избор на финансови услуги и съвременни платежни решения; •да осигури защита на потребителите и финансова стабилност.

Едновременно с приемането на Регламент (ЕС) 2022/2554 Европейският съюз прие и Директива (ЕС) 2022/2555 ***относно мерки за високо общо ниво на киберсигурност*** в Съюза, за изменение на Регламент (ЕС) №

---

[28] *Делегиран регламент (ЕС) 2024/1772* на ЕК от 13.03.2024 за допълнение на Регламент (ЕС) 2022/2554 по отношение регулаторните технически стандарти, с които се определят подробно *критериите за класифициране на инциденти с ИКТ и киберзаплахи, праговете на същественост и информацията в докладите за съществени инциденти*

Делегиран регламент (ЕС) 2024/1773 за допълнение на Регламент (ЕС) 2022/2554 по отношение на регулаторните технически стандарти, с които се *доуточнява подробното съдържание на политиката по отношение на договорните споразумения за използването на услуги в областта на ИКТ, поддържащи критични или важни функции, предоставяни от трети страни доставчици на услуги в областта на ИКТ*

Делегиран регламент (ЕС) 2024/1774 за допълнение на Регламент (ЕС) 2022/2554 във връзка с регулаторните технически стандарти *за определяне на инструментите, методите, процесите и политиките за управление на риска в областта на ИКТ и опростената рамка за управление на риска в областта на ИКТ* от 25 юни 2024г

[29] През 2023г. бяха приети два регламента, като част от мерките за противодействие на ИП/ФТ (AML) – **Регламент (ЕС) 2023/1114** на ЕП и на Съвета от 31.05.2023 г. ***относно пазарите на криптоактиви*** и за изменение на регламенти (ЕС) № 1093/2010 и (ЕС) № 1095/2010 и на Директиви (ЕС) 2013/36 и (ЕС) 2019/193.

Регламент (ЕС) 2023/1113 на ЕП и на Съвета от 31.05.2023г. ***относно информацията, придружаваща преводите на средства и прехвърлянията на определени криптоактиви,*** и за изменение на Директива (ЕС) 2015/849, които са непосредствено свързани и с ИКТ.

910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (**т.нар. Директива МИС 2** – *Директива за мрежова и информационна сигурност 2*)[30]. Директивата МИС 2 засилва изискванията за киберсигурност и санкциите с цел хармонизиране и повишаване на нивата на сигурност в държавите членки. Тя въвежда по-строги изисквания към различни сектори, обхващащи аспекти като управление на киберрискове, контрол и мониторинг, реакция при инциденти и непрекъснатост на бизнеса. Освен това Директивата разширява обхвата си, за да включи повече организации, като въвежда по-строги правила за отговорност за техните ръководства.

Защо Директивата МИС 2 е важна за банките и останалите оператори на критична инфраструктура, както и за доставчиците на основни услуги за тях?

В днешната забързана дигитална ера, когато организациите са изправени пред сложни киберзаплахи, важността на стабилните мерки за киберсигурност е неоспорима. Следването на изискванията на Директивата МИС 2 позволява на организациите да намалят рисковете, да защитят чувствителните данни и да се възползват от подобрени защити срещу кибератаки. МИС 2 (NIS 2) определя *базовата линия за мерките за управление на риска за киберсигурността и задълженията за докладване* във всички сектори, обхванати от Директивата, в т.ч. финансов сектор, енергетика, транспорт, здравеопазване и цифрова инфраструктура (прилагането на *единен подход* към управлението на риска, докладването на инциденти, тестовете за устойчивост и технологиите с цел *усъвършенстване на общото ниво на сигурност и оперативна устойчивост*). За да премахне различията в изискванията за киберсигурност и в прилагането на мерките за киберсигурност в различните държави членки, тя определя минимални правила за регулаторна рамка и определя механизми за ефективно *сътрудничество между съответните органи във всяка държава членка.* Директивата официално създава *Европейската мрежа на организацията за връзка при киберкризи, EU-CyCLONe,* която ще подпомага координираното управление на широкомащабни инциденти в киберсигурността. От държавите – членки на ЕС, се изискваше да я транспонират в националното законодателство до октомври 2024 г.[31]

---

[30] Вж. и *Директива (ЕС) 2022/2556* на Европейския парламент и на Съвета от 14.12.2022 г. за изменение на директиви 2009/65/ЕО, 2009/138/ЕО, 2011/61/ЕС, 2013/36/ЕС, 2014/59/ЕС, 2014/65/ЕС, (ЕС) 2015/2366 и (ЕС) 2016/2341 *по отношение на оперативната устойчивост на цифровите технологии във финансовия сектор*;
Директива (ЕС) 2022/2557 на Европейския парламент и на Съвета от 14.12.2022 г. *за устойчивостта на критичните субекти* и за отмяна на Директива 2008/114/ЕО на Съвета.

[31] Европейската комисия открива наказателна процедура (05.12.2024) срещу България и още 22 държави от ЕС за това, че не са въвели изцяло европейските правила за киберсигурност. България има два месеца да отговори на какво се дължи забавянето. Министерският съвет е внесъл в Парламента на Р България одобрения с Решение № 843 от 11.12.2024 г. *проект на Закон за изменение и допълнение на Закона за киберсигурност (ЗИД на ЗКС).* На 06.02.2025 г. Комисията по електронно управление на НС е *приела на първо четене промените в Закона за киберсигурност.*

Авторът на настоящото изследване подкрепя изцяло очакваните резултати от предлаганите изменения в Закона за киберсигурност:

- създаване на условия за изграждане на ефективна система за превенция и борба с кибератаките;
- ограничаване на мащаба, честотата и въздействието на инцидентите;
- противодействие на инцидентите, които причиняват значителни финансови загуби, нарушават доверието на потребителите и причиняват сериозни вреди на икономиката на държавата;
- ограничаване на транснационалния характер на инцидентите;
- установяване на условия за равнопоставеност по отношение на контрола на съществените и важни субекти и административните органи;
- улесняване на достъпа до надлежна информация, касаеща услуга, която е от съществено значение за поддържането на особено важни обществени и/или стопански дейности;
- повишаване на сигурността чрез създаване и поддържане на непубличен регистър на определените субекти в кръга на ЗИД на ЗКС, както и на самите съществени услуги;
- въвеждане на ясна йерархична структура в управлението и организацията на националната система за киберсигурност;
- подобряване на надеждността, устойчивостта и ефективността на мрежите и информационните системи на всички субекти в обхвата на закона.

Очакванията ни са, че с транспонирането на Директивата МИС 2 и реализиране на поставените цели ще се опрости и ускори процесът по взаимодействието и разрешаването на трансгранични и национални инциденти в ЕС, като това ще става бързо и без никакви допълнителни формалности, което ще допринесе за своевременното преодоляване на атаките и намаляване на негативните последици от тях. Безспорно приемането на ЗИД на ЗКС ще има за резултат хармонизирането и привеждането в съответствие на националното с европейското законодателство.

2.2. Рамка за управление на риска в областта на ИКТ

(1). Всяка кредитна институция трябва да разполага с *надеждна, широкообхватна и добре документирана рамка за управление на риска в областта на ИКТ,* като част от цялостната ѝ система за управление на риска, която да ѝ позволява да се справя бързо и ефикасно с риска в областта на ИКТ и да поддържа високо равнище на оперативна устойчивост на цифровите технологии.

(2). *Рамката за управление на риска в областта на ИКТ включва*: стратегии, политики, процедури, протоколи за ИКТ и инструменти, основани на ИКТ, които са необходими за надлежната и подходяща защита на всички информационни активи и активи на ИКТ, включително компютърен софтуер, хардуер, сървъри, както и за защитата на всички относими физически компоненти и инфраструктури, като например помещения, центрове за данни и зони, определени като чувствителни, така че да се гарантира, че всички информационни активи и активи на ИКТ са подходящо защитени от рискове, включително от увреждане и непозволен достъп или използване.[32]

Тук е мястото, където трябва да представим *определенията за понятията и термините*, които ще използваме при характеристиката на Рамката за управление на риска в областта на ИКТ и при анализа на оперативна устойчивост на ИКТ[33]:

- ✓ *риск* е събитие, което ще повлияе върху постигане на целите на кредитната институция. Рискът се измерва с неговия ефект и с вероятността от настъпването му;
- ✓ *разумна увереност* – задоволително ниво на увереност, което изисква разходите за вътрешен контрол да не надхвърлят очакваните ползи от него. Концепцията за разумна увереност е признание, че не е възможно да се твърди абсолютно и със сигурност, че дадено неблагоприятно събитие няма да се случи въпреки взетите мерки и предприетите действия;
- ✓ *риск в областта на ИКТ* означава всяко установимо при обичайни условия обстоятелство във връзка с използването на мрежови и информационни системи, което, ако се реализира, може да застраши сигурността на мрежовите и информационните системи на зависим от технологиите инструмент или процес, на операциите или процесите или на предоставянето на услуги, като предизвика неблагоприятни последици в цифровата или физическата среда;
- ✓ *идентифициране на риска в областта на ИКТ* – идентифициране на вътрешни и външни събития, свързани с ИКТ, които могат да застрашат постигането на целите на кредитната институция и изпълнението на функциите ѝ;
- ✓ *оценка на риска* – процес, състоящ се от определяне на степен на вероятност от сбъдването на идентифицирания риск от ИКТ и определяне на степен на влияние (ефект) върху целите на кредитната институция при неговото настъпване;

---

[32] Вж и Делегиран регламент (ЕС) 2024/1774 за допълнение на Регламент (ЕС) 2022/2554 във връзка с регулаторните технически стандарти *за определяне на инструментите, методите, процесите и политиките за управление на риска в областта на ИКТ и опростената рамка за управление на риска в областта на ИКТ* от 25 юни 2024 г.

[33] Използваме основно определенията от Регламент (ЕС) 2022/2554 и Делегиран регламент (ЕС) 2024/1774.

- ✓ *присъщ риск* – рискът от ИКТ, свързан с естеството на дейността на институцията при липса на каквито и да е действия (контроли) за смекчаване на вероятността или на ефекта от неговото проявление;
- ✓ *остатъчен риск* – нивото на влияние и вероятност от риск, което остава след реакцията (контрола) на ръководството към ИКТ риска. След предприемане на конкретни действия (реакция на риска) продължава да съществува риск, който се нарича остатъчен риск и по същество изразява факта, че рискът не може да бъде премахнат изцяло. Отговорност на мениджмънта е да реши дали равнището на остатъчния риск е приемливо за банката или е необходимо да бъдат предприети допълнителни действия за неговото намаляване;
- ✓ *риск апетит* – нивото на риск, което банката е готова да поеме и поддържа в рамките на своя рисков капацитет в съответствие със своя бизнес модел за постигане на стратегическите си цели при извършване на обичайната дейност;
- ✓ *риск толерантност* – максимално приемливото ниво риск, свързано с всяко измерение и класификация на ИКТ риска, определени от кредитната институция: установена чрез методология за определяне на риск лимити; насърчаване на среда, в която участниците са наясно с взаимовръзката между риск и печалба; осигурява институцията да остане в *границите на риск апетита*;
- ✓ *рисковият капацитет* е максималната степен на ИКТ риск, която банката е способна да поеме преди да наруши или увреди функциите си, показателите си за добро финансово състояние (капиталовата база, ликвидността, кредитоспособността), репутацията си и регулаторните изисквания в условията на нормално развитие и на криза;
- ✓ *оперативна устойчивост на цифровите технологии* е способността на банковата институция да изгражда, осигурява и преглежда своята оперативна цялост и надеждност, като осигурява пряко или непряко – чрез ползване на услуги, предоставяни от трети страни, доставчици на услуги в областта на ИКТ, пълния набор от свързан с ИКТ капацитет, необходим за сигурността на използваните от него мрежови и информационни системи, и който поддържа непрекъснатото предоставяне на финансови услуги и тяхното качество, включително при смущения;
- ✓ *информационен актив* означава материална или нематериална съвкупност от информация, която си струва да се защитава;
- ✓ *актив на ИКТ* е софтуерен или хардуерен актив в мрежовите и информационните системи, използвани от кредитната институция;
- ✓ *инцидент с ИКТ* означава единично събитие или поредица от свързани събития, които не са планирани от финансовата

институция, застрашават сигурността на мрежовите и информационните системи и имат неблагоприятно въздействие върху наличността, автентичността, цялостността или поверителността на данните или върху предоставяните от банката услуги;

- ✓ *съществен инцидент с ИКТ* означава инцидент с ИКТ, който има силно неблагоприятно въздействие върху мрежовите и информационните системи, поддържащи критични или важни функции на кредитната институция;
- ✓ *съществен операционен или свързан със сигурността инцидент, свързан с плащания,* означава операционен или свързан със сигурността инцидент, свързан с плащания, който има силно неблагоприятно въздействие върху предоставяните услуги, свързани с плащания;
- ✓ *киберзаплаха* е всяко потенциално обстоятелство, събитие или действие, което може да навреди, наруши или по друг начин да окаже неблагоприятно въздействие върху мрежите и информационните системи, ползвателите на такива мрежи и системи и други лица;[34]
- ✓ *значителна киберзаплаха* е киберзаплаха, чиито технически характеристики показват, че би могла да доведе до съществен инцидент с ИКТ или до съществен операционен или свързан със сигурността инцидент, свързан с плащания;
- ✓ *кибератака* означава инцидент с ИКТ в резултат на злонамерен акт, причинен от опит на източник на заплаха с цел унищожаване, разкриване, промяна, деактивиране, откradване или получаване на непозволен достъп или непозволено използване на актив;
- ✓ *уязвимо място* означава слабост, тенденция или недостатък на актив, система, процес или контролна функция, която може да бъде използвана;
- ✓ *тестване за проникване (TLPT)* е симулиране на тактиката, техниките и процедурите на реални източници на заплаха, за които се счита, че представляват истинска киберзаплаха; тази симулация представлява контролиран, специално разработен и опиращ се на разузнавателни сведения (червен екип) тест на критичните оперативни производствени системи на финансовия субект;
- ✓ *риск в областта на ИКТ, пораждан от трета страна,* означава риск в областта на ИКТ, който може да възникне за финансовата институция във връзка с използваните от нея услуги в областта на ИКТ, предоставяни от трета страна – доставчик на такива услуги, или

[34] *Регламент (ЕС) 2019/881* от 17 април 2019 г. относно ENISA (Агенцията на ЕС за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии, както и за отмяна на Регламент (ЕС) № 526/2013 (*Акт за киберсигурността*).

от нейни поддоставчици, включително чрез споразумения за възлагане на дейности на външни изпълнители;

- ✓ *трета страна доставчик на услуги в областта на ИКТ* е предприятие, което предоставя услуги в областта на ИКТ;
- ✓ *вътрешногрупов доставчик на услуги в областта на ИКТ* е предприятие, което е част от финансова група и предоставя предимно услуги в областта на ИКТ на финансови институции от същата група или на финансови институции, които са част от една и съща институционална защитна схема, включително на техните предприятия майки, дъщерни предприятия, клонове или други субекти, намиращи се в обща собственост или под общ контрол;
- ✓ *услуги в областта на ИКТ* са цифрови услуги и услуги за данни, предоставяни непрекъснато чрез системите на ИКТ на един или повече вътрешни или външни ползватели, включително хардуер като услуга и хардуерни услуги, което включва техническа поддръжка чрез актуализации на софтуер или фърмуер от доставчика на хардуер и изключва традиционните аналогови телефонни услуги;
- ✓ *критична или важна функция* е функция, чието смущение би намалило съществено финансовите резултати на даден финансов субект или стабилността или непрекъснатостта на неговите услуги и дейности, или функция, чието прекъсване, неизправност или срив би намалил съществено възможността на дадена кредитна институция да продължи да изпълнява условията и задълженията, свързани с нейния лиценз, или останалите си задължения, съгласно приложимото право в областта на банковите услуги;
- ✓ *трета страна критичен доставчик на услуги в областта на ИКТ* е трета страна, която е доставчик на услуги в областта на ИКТ, определен като имащ критично значение в съответствие с изискванията на Регламент (ЕС) 2022/2554 (член 31);
- ✓ *риск от концентрация при ИКТ* означава експозиция към дадена трета страна критичен доставчик на услуги в областта на ИКТ или към множество свързани такива доставчици, *която поражда известна степен на зависимост от такива доставчици*, така че ако съответният доставчик не бъде достъпен, престане да предоставя услугите си или понесе друг вид неизправност, това потенциално може да застраши способността на банката да изпълнява критични или важни функции или да ѝ причини други видове неблагоприятни последици, включително големи загуби, или да застраши финансовата стабилност на Съюза като цяло.

Подходящо е политиките и процедурите за управление на риска в областта на ИКТ да съдържат следните елементи:

а) указание за *одобрението на нивото на толерантност* към риска в областта на ИКТ според склонността на институцията за поемане на риск и чрез проучване допустимата степен на въздействие при смущения на ИКТ;

б) *процедура и методика за провеждане на оценка на риска* в областта на ИКТ, при която се установяват: уязвимите места и заплахите, които засягат или може да засегнат поддържаните работни функции, системите на ИКТ и активите на ИКТ, поддържащи тези функции; количествените или качествените показатели за измерване на въздействието и вероятността от наличието на уязвимите места и заплахите;

в) *процедура за идентифициране*, прилагане и документиране на *мерките за третиране (намаление) на риска в областта на ИКТ* във връзка с идентифицираните и оценените рискове, включително определянето на мерките за третиране на риска в областта на ИКТ, необходими за привеждане на рисковете в рамките на нивото на толерантност към риска;

г) за *остатъчните рискове в областта на ИКТ*, които все още съществуват след прилагането на мерките за третиране на риска в областта на ИКТ, посочени в буква в): подхода за установяването на тези остатъчни рискове в областта на ИКТ; разпределянето на ролите и отговорностите относно поемането на остатъчните рискове, които надвишават нивото на толерантност към риска на кредитната институция и процеса на преглед; основанието за тяхното поемане; разпоредбите относно извършвания поне веднъж годишно преглед на поетите остатъчни рискове в областта на ИКТ (вкл. установяването на всички промени в остатъчните рискове в областта на ИКТ; оценката на наличните мерки за намаляване на риска; оценката на това дали причините, обосноваващи поемането на остатъчни рискове в областта на ИКТ, са все още валидни и приложими към датата на прегледа);

д) *процедури относно наблюдението на:* всички промени в рисковете в областта на ИКТ и обстановката по отношение на киберзаплахите; вътрешни и външни уязвими места и заплахи; риск в областта на ИКТ за банката, който позволява своевременно откриване на промени, които биха могли да повлияят на рисковия ѝ профил в областта на ИКТ.

(3). Кредитната институция възлага на съответна *контролна функция отговорността за управление и надзор на риска в областта на ИКТ* и осигурява подходящо ниво на независимост на тази контролна функция *(напр. Комитет по ИКТ и устойчивост*, чиято дейност се подпомага от Комисии по киберсигурност и непрекъсваемост на дейността), за да се избегнат конфликти на интереси, като се гарантират *подходящо разделяне и независимост* на функциите за управление на риска в областта на ИКТ,

контролните функции и функциите за вътрешен одит, според модела на трите защитни слоя или друг (свой) модел за управление и контрол на риска.

(4). Рамката за управление на риска в областта на ИКТ се документира и *се преразглежда поне веднъж годишно, както и при съществени инциденти с ИКТ,* като това се прави съобразно инструкциите на надзорните органи или заключенията, направени в резултат от съответните *тестове на оперативната устойчивост* на цифровите технологии или от одитните процеси. Рамката се усъвършенства непрекъснато въз основа на натрупания при нейното прилагане и наблюдаване опит[35].

(5). Рамката за управление на риска в областта на ИКТ на банките подлежи на редовен вътрешен одит от одитори в съответствие с годишния одитен план. Тези одитори притежават достатъчно знания, умения и експертен опит във връзка с риска в областта на ИКТ, както и подходящо ниво на независимост, като честотата и насочеността на одитите на ИКТ са съобразени с риска в областта на ИКТ на банката. Като добра практика, въз основа на заключенията от вътрешния одитен преглед, банките въвеждат официален процес на последващи действия, включително правила за своевременна проверка и отстраняване на *критично важните проблеми*, посочени в заключенията от одита на ИКТ.

(6). Рамката за управление на риска в областта на ИКТ включва *стратегия за оперативна устойчивост на цифровите технологии,* която представяме в т. 3 от настоящата публикация.

(7). В контекста на стратегията за оперативна устойчивост на цифровите технологии кредитните институции могат да определят *цялостна стратегия* за използване на множество доставчици на ИКТ, на равнище група или отделна институция, в която се посочват ключовите зависимости от третите страни доставчици на услуги в областта на ИКТ и се обяснява логиката зад избора на съответните трети страни доставчици[36].

Европейските надзорни органи напредват в прилагането на общоевропейската рамка за надзор на *критични ИКТ доставчици на трети страни* (CTPP – Critical Third-Party Providers) с цел да определят CTPP и да започнат ангажимента за надзор тази година[37].

За да определят CTPP през 2025 г., ESA ще извършат следните стъпки:

---

[35] Вж. и Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14.12.2022 г. относно оперативната устойчивост на цифровите технологии във финансовия сектор и за изменение на регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014, (ЕС) № 909/2014 и (ЕС) 2016/1011.
[36] Вж Делегиран регламент (ЕС) 2024/1773 за допълнение на Регламент (ЕС) 2022/2554 по отношение на регулаторните технически стандарти, с които се *доуточнява подробното съдържание на политиката по отношение на договорните споразумения за използването на услуги в областта на ИКТ, поддържащи критични или важни функции, предоставяни от трети страни, доставчици на услуги в областта на ИКТ.*
[37] В началото на м. февруари 2025 г. Европейските надзорни органи – ЕНО (EBA, EIOPA и ESMA – ESAs) предоставят пътна карта за определяне на критични доставчици трети страни (Critical Third-Party Providers – CTPP).

Събиране на регистри на информация: Компетентните органи са длъжни да предоставят на ЕНО до *30 април 2025 г.* регистрите на информация относно споразумения с трети страни в ИКТ, които са получили от финансовите институции.

Оценки на критичност: ESA ще извършат оценките на критичността, възложени от DORA, и ще уведомят доставчиците на ИКТ услуги от трети страни за тяхната класификация като критични до юли 2025 г. Това уведомление ще обхване шестседмичен период, през който доставчиците на ИКТ услуги от трети страни могат да възразят срещу оценката с мотивирано изявление и подходяща подкрепяща информация.

Окончателно определяне: След шестседмичния период ESA ще определят СТРР и ще започнат надзорни ангажименти с тях[38].

Рамката за управление на риска в областта на ИКТ, като част от действията по осигуряване и поддържане на оперативната устойчивост, има за цел да подпомогне изпълнението на бизнес стратегията и целите на банката, което се постига чрез пълното и точно идентифициране, оценка, контрол и управление на рисковете, застрашаващи тяхното изпълнение. За целта е подходящо да бъде въведен *стандартизиран подход за управление на риска,* позволяващ навременното предприемане на адекватни действия спрямо идентифицирани рискове, застрашаващи постигането на конкретните цели. *Управлението на риска, разглеждано като процес, е предназначено да даде разумна увереност, че целите на организацията в областта на оперативната устойчивост ще бъдат постигнати.* Рамката за управление на риска в областта на ИКТ в банката трябва *да съдържа и матрица,* в която е определено нивото на толерантност към риска в областта на ИКТ, според склонността ѝ за поемане на риск, и е определена допустимата степен на въздействие при смущения на ИКТ.

В контекста на представената обща рамка за управление на риска в областта на ИКТ управлението на ИКТ рисковете, включително тези за оперативната устойчивост и в частност за информационната сигурност, включва конкретно: идентификация на ИКТ активите и заплахите към тях (определянето на активите и собствениците на риска, идентификация на заплахите за ИКТ активите); оценка на бизнес критичността на актива; оценка на риска; идентификацията на остатъчни рискове; наблюдение, преглед и преоценка на риска. Към списъка с активите се включват всички ИКТ и информационни активи – тези, които са свързани със създаване, обработка, пренос или съхранение на информация.

[38] *Трети доставчици на ИКТ услуги*, които *не са определени като критични*, могат *доброволно* да поискат да бъдат определени като критични, след като списъкът на СТРР бъде публикуван.

ЗАКЛЮЧЕНИЕ

При анализа и оценката на рамката за управление на операционния риск, риска, свързан с ИКТ и оперативната устойчивост на цифровите технологии органите за управление следва да подходят към този преглед с оглед на *ключовите фактори на операционния риск* (т.е. хора, процеси, външни фактори, системи), които може да действат като редуциращи фактори, и трябва да вземат предвид: а. стратегията за управление на операционния риск и рисковия апетит към операционен риск; б. организационната рамка; в. политики и процедури; г. идентифициране, измерване, наблюдение и отчитане на операционния риск; д. плановете за устойчивост и непрекъсваемост на дейността; и е. рамката за вътрешен контрол, така както се прилага към управлението на операционния риск.

Като изводи от изследването е важно да се определи дали кредитната институция е изградила планове за непрекъсваемост на дейността, съизмерими с естеството, размера и сложността на нейните дейности и бизнес модел. Тези планове следва да вземат под внимание различните видове вероятни или допустими сценарии, при които институцията може да прояви слабост. В този ред е необходимо да се оценят качеството и ефективността на процеса на *планиране на управлението на непрекъсваемостта* на кредитната институция; дали процесът на планиране на управлението на непрекъсваемостта на дейността на банката включва: анализ на въздействието върху бизнеса; подходящи стратегии за възстановяване, включващи вътрешни и външни зависимости и ясно определени приоритети за възстановяване; изработване на цялостни и гъвкави планове за справяне с възможни сценарии; ефективно изпитване на проектирането и оперативната ефективност на плановете; програми за информираност и обучение по признати процеси на управление на непрекъсваемостта на дейността (Business Continuity Management – BCM) и документация и обучение по комуникации и управление на кризи.

Какви са очакванията ни за 2025 година? Да погледнем в публикуваната работна програма – Joint Committee Annual Work Programme 2025 (през м. октомври 2024 г.) на съвместния комитет на европейските надзорни органи ЕНО, в която се поставя *специален акцент* върху продължаващото сътрудничество за справяне с междусекторните рискове, насърчаване на устойчивостта на финансовата система на ЕС и укрепване на цифровата устойчивост на финансовите институции. По-конкретно, в допълнение към насърчаването на регулаторната съгласуваност, адекватната оценка на риска, финансовата стабилност, както и защитата на потребителите и инвеститорите, *ЕНО ще предприемат съвместна работа през 2025 г. за:* предоставяне на допълнителни насоки относно оповестяването на информация за устойчивостта; *постигнат напредък по отношение на цифровата оперативна устойчивост на финансовите институции* чрез стартиране на надзора на критични доставчици на информационни и комуникационни технологии (ИКТ) от трети страни и прилагане на рамката

за координиране на големи инциденти, свързани с ИКТ, в съответствие с DORA; насърчаване координацията и сътрудничеството между националните координатори на иновациите с оглед улесняване на разширяването на обхвата на иновативните решения във финансовия сектор; разглеждане на други междусекторни въпроси, като например финансовите услуги на дребно, инвестиционните продукти и секюритизацията.

Библиографска справка:

1. *Вейсел, А. (2023). Влиянието на изкуствения интелект върху счетоводството, Списание ИДЕС, бр. 3/2023 г., инд. в RePec, Google Scholar и EBSCO.*
2. *Делегиран регламент (ЕС) 2018/389 от 27 ноември 2017 година за допълнение на Директива (ЕС) 2015/2366 на Европейския парламент и на Съвета по отношение на регулаторните технически стандарти за задълбоченото установяване на идентичността на клиента и общите и сигурни отворени стандарти на комуникация.*
3. *Делегиран регламент (ЕС) 2024/1772 на ЕК от 13.03.2024 за допълнение на Регламент (ЕС) 2022/2554 по отношение регулаторните технически стандарти, с които се определят подробно критериите за класифициране на инциденти с ИКТ и киберзаплахи, праговете на същественост и информацията в докладите за съществени инциденти.*
4. *Делегиран регламент (ЕС) 2024/1773 за допълнение на Регламент (ЕС) 2022/2554 по отношение на регулаторните технически стандарти, с които се доуточнява подробното съдържание на политиката по отношение на договорните споразумения за използването на услуги в областта на ИКТ, поддържащи критични или важни функции, предоставяни от трети страни доставчици на услуги в областта на ИКТ.*
5. *Делегиран регламент (ЕС) 2024/1774 за допълнение на Регламент (ЕС) 2022/2554 във връзка с регулаторните технически стандарти за определяне на инструментите, методите, процесите и политиките за управление на риска в областта на ИКТ и опростената рамка за управление на риска в областта на ИКТ от 25 юни 2024 г.*
6. *Директива 2013/36/ЕС на ЕП 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 (Директива за капиталовите изисквания) с последни изменения.*
7. *Директива (ЕС) 2022/2464 на ЕП и на Съвета от 14 декември 2022 година за изменение на Регламент (ЕС) № 537/2014, Директива 2004/109/ЕО, Директива 2006/43/ЕО и Директива 2013/34/ЕС по отношение на отчитането на предприятията във връзка с устойчивостта.*
8. *Директива 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 година относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) №*

910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (Директива МИС 2).

9. *Директива (ЕС) 2022/2556 на Европейския парламент и на Съвета от 14.12.2022 г. за изменение на директиви 2009/65/ЕО, 2009/138/ЕО, 2011/61/ЕС, 2013/36/ЕС, 2014/59/ЕС, 2014/65/ЕС, (ЕС) 2015/2366 и (ЕС) 2016/2341 по отношение на оперативната устойчивост на цифровите технологии във финансовия сектор.*
10. *Директива (ЕС) 2022/2557 на Европейския парламент и на Съвета от 14.12.2022 г. за устойчивостта на критичните субекти и за отмяна на Директива 2008/114/ЕО на Съвета.*
11. *Директива (ЕС) 2015/2366 на Европейския парламент и на Съвета от 25 ноември 2015 година за платежните услуги във вътрешния пазар, за изменение на Директиви 2002/65/ЕО, 2009/110/ЕО и 2013/36/ЕС и Регламент (ЕС) № 1093/2010 и за отмяна на Директива 2007/64/ЕО.*
12. *Закон за киберсигурност, обн., ДВ, бр. 94 от 13.11.2018 г., посл. изм. и доп., ДВ, бр. 15 от 22.02.2022 г.*
13. *Закон за защита на личните данни, обн., ДВ, бр. 1 от 4 януари 2002 г., изм., ДВ, бр. 84 от 06.10.2023 г., посл. изм., ДВ, бр. 70 от 20.08.2024 г.*
14. *Миланова, Е. (2018). Време ли е за Базел IV и какви са ефектите върху банките в България, Икономически и социални алтернативи, УНСС, София, инд. в RePec, Google Scholar и EBSCO.*
15. *Миланова, Е. (2020). Оценка на вътрешното управление и механизмите за контрол при банките в рамките на процеса на надзорен преглед и оценка (ПНПО), (студия), Годишник на ИДЕС, София, ISSN 1313-2148, инд. в RePec, Google Scholar и EBSCO.*
16. *Миланова, Е. (2022). Оценка на бизнес модела на банките в процеса на надзорен преглед и оценка (ПНПО) и икономиката на страха (предизвикателствата на икономическата криза), Сборник с научни доклади „Икономика на страха“, ВУЗФ, Издателство „Св. Григорий Богослов“, 2022.*
17. *Насоки на ЕБО относно рисковите фактори, свързани с ИП/ФТ (EBA/GL/2021/02); EBA/GL/2023/03 и EBA/GL/2024/01.*
18. *Насоки EBA/GL/2022/03 относно общите процедури и методологии за процеса на надзорен преглед и оценка (ПНПО) и надзорните стрес тестове.*
19. *Регламент (ЕС) № 575/2013 на ЕП и на Съвета от 26 юни 2013 г. относно пруденциалните изисквания за кредитните институции и за изменение на Регламент (ЕС) № 648/2012 (ОВ L 176, 27.6.2013 г. (Регламент за капиталовите изисквания – РКИ).*

20. *Регламент за изпълнение (ЕС) 2022/2453 на Комисията от 30 ноември 2022 година за изменение на техническите стандарти за изпълнение, определени в Регламент за изпълнение (ЕС) 2021/637, по отношение на оповестяването на екологичните, социалните и управленските рискове.*
21. *Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14 декември 2022 г. относно оперативната устойчивост на цифровите технологии във финансовия сектор и за изменение на регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014, (ЕС) № 909/2014 и (ЕС) 2016/1011 – DORA.*
22. *Регламент (ЕС) 2023/1114 на ЕП и на Съвета от 31.05.2023 г. относно пазарите на криптоактиви и за изменение на регламенти (ЕС) № 1093/2010 и (ЕС) № 1095/2010.*
23. *Регламент (ЕС) 2023/1113 на ЕП и на Съвета от 31.05.2023 г. относно информацията, придружаваща преводите на средства и прехвърлянията на определени криптоактиви, и за изменение на Директива (ЕС) 2015/849.*
24. *Регламент (ЕС) 2024/1623 на Европейския парламент и на Съвета от 31 май 2024 г. за изменение на Регламент (ЕС) № 575/2013 по отношение на изискванията за кредитен риск, риск от корекция на кредитната оценка, операционен риск и пазарен риск, както и за долна граница на капиталовото изискване.*
25. *Регламент (ЕС) 2024/2847 на ЕП и на Съвета от 31 май 2024 г. за предотвратяване на използването на финансовата система за целите на изпирането на пари или финансирането на тероризма.*
26. *Регламент (ЕС) 2024/1623 на Европейския парламент и на Съвета от 23 октомври 2024 г. относно хоризонтални изисквания за киберсигурност за продукти с цифрови елементи и за изменение на регламенти (ЕС) № 168/2013 и (ЕС) 2019/1020 и Директива (ЕС) 2020/1828 (Акт за киберустойчивост).*
27. *EBA/GL/2019/04 от 28.11.2019 г. Насоки на ЕБО относно управление на риска в областта на ИКТ.*
28. *EBA/GL/2017/05 11/09/2017. Насоки за оценка на риска в областта на информационните и комуникационните технологии (ИКТ) в рамките на процеса на надзорен преглед и оценка (ПНПО).*
29. *Finn, T., A. Downie. (2024). What is digital transformation in banking and financial services?. https://www.ibm.com/think/topics/digital-transformation-banking*
30. *Shkurdoda, A., A. Puczyk. (2024). Digital Transformation in Banking Industry: Revolutionizing Financial Services. https://neontri.com/blog/digital-banking*