

Зміни

до Положення про організацію системи управління ризиками в банках України  
та банківських групах

1. У розділі I:

1) у пункті 3 глави 1:

підпункти 5<sup>2</sup>, 5<sup>3</sup> замінити трьома новими підпунктами 5<sup>2</sup>–5<sup>4</sup> такого змісту:

“5<sup>2</sup>) внутрішньогруповий TPSP-постачальник (англійською мовою intragroup TPSP – intragroup Third-Party Service Provider) – постачальник, який є учасником банківської групи згідно зі статтею 2 Закону України “Про банки і банківську діяльність” та надає послуги іншим учасникам цієї банківської групи;

5<sup>3</sup>) головний ризик-менеджер (CRO) – головна посадова особа банку, відповідальна за управління ризиками;

5<sup>4</sup>) головний комплаєнс-менеджер (CCO) – головна посадова особа банку, відповідальна за здійснення контролю за дотриманням норм (комплаєнс);”;

пункт після підпункту 7 доповнити новим підпунктом 7<sup>1</sup> такого змісту:

“7<sup>1</sup>) договір з TPSP-постачальником – укладений в письмовій формі договір між банком / учасником банківської групи та TPSP-постачальником про надання банку / учаснику банківської групи однієї або кількох послуг, а саме:

включає договір з аутсорсером, договір з надання послуг внутрішньогруповим TPSP-постачальником, договір про надання послуг з підтримки діяльності банку / учасника банківської групи та договір про виконання функцій технологічного оператора платіжних послуг відповідно до Закону України “Про платіжні послуги”;

не включає:

операцій з надання банківських послуг / фінансових послуг / платіжних послуг / здійснення іншої діяльності, що здійснюється банком / учасником банківської групи на підставі ліцензії / дозволу, наданого органом, який здійснює державне регулювання ринків фінансових послуг;

операцій, які здійснюються між банками, іншими учасниками ринку фінансових послуг, банками / учасниками банківської групи з їх працівниками, банками / учасниками банківської групи за дорученням їх клієнтів або контрагентів, включаючи страхування, надання / отримання послуг інфраструктури фінансового ринку, зокрема клірингові послуги, послуги розрахунків, послуги центрального депозитарію цінних паперів;

договори між TPSP-постачальником і будь-якою стороною в ланцюгу постачання (п-ю стороною для банку / учасника банківської групи);”;

пункт після підпункту 12 доповнити двома новими підпунктами 12<sup>1</sup>, 12<sup>2</sup> такого змісту:

“12<sup>1</sup>) інфраструктура фінансового ринку – багатостороння система взаємодії учасників фінансового ринку, організаторів торгівлі, центрального депозитарію цінних паперів, платіжних, клірингових, розрахункових і депозитарних установ, а також інформаційних та технологічних систем, діяльність яких спрямована на забезпечення функціонування фінансового ринку шляхом укладання договорів, обліку, виконання розрахунків за фінансовими операціями та фінансовими інструментами;

12<sup>2</sup>) карта взаємозв’язків і взаємозалежностей між TPSP-постачальниками – внутрішньобанківський / внутрішньогруповий документ, що містить інформацію про ділові відносини між TPSP-постачальниками, спільних власників TPSP-постачальників, ключові п-і сторони TPSP-постачальників та іншу інформацію, що свідчить про наявність / відсутність взаємозв’язків і взаємозалежностей між TPSP-постачальниками;”;

пункт після підпункту 13 доповнити новим підпунктом 13<sup>1</sup> такого змісту:

“13<sup>1</sup>) ключова п-на сторона – п-на сторона в ланцюгу постачання, яка має опосередкований вплив на підтримання / надання критичної послуги TPSP-постачальником банку / учаснику банківської групи;”;

пункт після підпункту 16 доповнити чотирма новими підпунктами 16<sup>1</sup>–16<sup>4</sup> такого змісту:

“16<sup>1</sup>) критична послуга – послуга, що надається банку / учаснику банківської групи одним критичним TPSP-постачальником або кількома TPSP-постачальниками, які не є критичними та мають спільного кінцевого бенефіціарного власника або керівником яких є одна й та сама фізична особа, відмова або збій / переривання у наданні якої/яких може мати суттєвий вплив на його бізнес-модель, здатність забезпечувати безперервну діяльність, виконувати критичні функції, дотримуватися вимог законодавства України;

16<sup>2</sup>) критична функція – вид діяльності / процес / персонал / допоміжні активи, включаючи технології, інформацію та обладнання, необхідні для виконання такої функції банком / учасником банківської групи, порушення / зупинення / припинення яких матиме суттєвий негативний вплив на фінансовий стан, безперервність діяльності, дотримання банком / учасником банківської групи вимог законодавства України, та/або може загрожувати фінансовій стабільності, та/або мати суттєвий негативний вплив на економіку або на окремі галузеві / регіональні сегменти економіки України через розмір або частку банку / учасника банківської групи на ринку / у регіоні, складність / унікальність / обсяги здійснюваних ним операцій, ступінь фінансових взаємозв’язків, включаючи транскордонну діяльність банку / учасника банківської групи;

16<sup>3</sup>) критичний договір з TPSP-постачальником – договір, на підставі якого критичний TPSP-постачальник надає одну чи більше критичних послуг банку / учаснику банківської групи;

16<sup>4</sup>) критичний TPSP-постачальник – TPSP-постачальник, який надає банку / учаснику банківської групи критичну послугу;”;

пункт після підпункту 17 доповнити новим підпунктом 17<sup>1</sup> такого змісту:

“17<sup>1</sup>) ланцюг постачання – сукупність суб’єктів господарювання, включаючи TPSP-постачальника, що здійснюють діяльність з надання послуг, постачання матеріальних / нематеріальних активів, інших ресурсів, діяльність яких прямо чи опосередковано використовуються TPSP-постачальником для надання послуг банку / учаснику банківської групи;”;

пункт після підпункту 33<sup>2</sup> доповнити новим підпунктом 33<sup>3</sup> такого змісту:

“33<sup>3</sup>) ризик концентрації послуг – імовірність виникнення збитків або додаткових втрат або недоотримання доходів унаслідок залежності банку / учасника банківської групи / банківської групи (у випадках, коли це релевантно) від однієї або кількох послуг, що надаються одним критичним TPSP-постачальником або кількома TPSP-постачальниками, які не є критичними (прямо або опосередковано через співпрацю з однією і тією самою п-ю стороною), збій / переривання у наданні яких можуть мати негативний вплив на виконання банком / учасником банківської групи критичних функцій;”;

пункт після підпункту 37 доповнити новим підпунктом 37<sup>1</sup> такого змісту:

“37<sup>1</sup>) ризик третіх сторін (складова операційного ризику) – імовірність виникнення збитків або додаткових втрат, або недоотримання запланованих доходів унаслідок неналежного надання послуг TPSP-постачальником (включаючи аутсорсинг) та/або п-ю стороною;”;

пункт після підпункту 42<sup>1</sup> доповнити новим підпунктом 42<sup>2</sup> такого змісту:

“42<sup>2</sup>) толерантність до збоїв – максимальний рівень наслідків від збоїв, який банк / учасник банківської групи в змозі прийняти під час своєї діяльності без втрати здатності забезпечувати безперервну діяльність, діяльність без порушення вимог законодавства України, без створення загрози фінансовій стійкості, інтересам клієнтів, вкладників та інших кредиторів унаслідок настання будь-якого типу подій операційного ризику в разі реалізації екстремальних, однак реалістичних сценаріїв;”;

пункт після підпункту 44<sup>2</sup> доповнити новим підпунктом 44<sup>3</sup> такого змісту:

“44<sup>3</sup>) угода про рівень сервісу / обслуговування (англійською мовою SLA – Service Level Agreement) – договір / умови договору з TPSP-постачальником, що визначає / визначають рівень якості, доступності та ефективності послуг / обслуговування, їх характеристики, які банк / учасник банківської групи очікує отримати від TPSP-постачальника, включаючи вимоги до строків та обсягів надання послуг / обслуговування, контрольні показники якості, які щонайменше мають включати допустимі середній час між збоями, середній час ремонту,

середній час відновлення надання послуг / обслуговування, оперативність вирішення проблем за першим викликом та час виконання робіт / усунення проблем, а також відповідальність сторін за неналежне виконання умов договору;”;

пункт після підпункту 49 доповнити двома новими підпунктами такого змісту:

“50) п-на сторона – постачальник послуг, який є частиною ланцюга постачання TPSP-постачальника, включаючи, але не обмежуючись особами, на яких покладено виконання послуг TPSP-постачальника (субпідрядниками);

51) TPSP-постачальник (англійською мовою TPSP – Third-Party Service Provider) – юридична або фізична особа, яка є суб’єктом господарювання, включаючи внутрішньогрупового TPSP-постачальника, що надає послуги безпосередньо банку / учаснику банківської групи.”;

пункт після абзацу дев’ятого шостого доповнити новим абзацом дев’ятого сьомим такого змісту:

«Термін “кінцевий бенефіціарний власник” уживається в цьому Положенні в значенні, визначеному в Законі України “Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення”».

У зв’язку з цим абзац дев’ятого сьомий уважати абзацом дев’ятого восьмим;

2) пункт 36 глави 6 після підпункту 7 доповнити новим підпунктом такого змісту:

“8) розробляє та впроваджує процеси та процедури, визначає функції, обов’язки, повноваження та відповідальність працівників щодо управління відносинами за договорами з TPSP-постачальниками на кожному з етапів життєвого циклу відносин банку з TPSP-постачальником.”;

3) друге речення пункту 65 глави 10 замінити двома новими реченнями другим та третім такого змісту: “Рада банку під час визначення стратегії та складання бізнес-плану банку враховує величину ризик-апетиту, зазначену в декларації схильності до ризиків. Рада банку також ураховує визначений рівень ризик-апетиту та рівень толерантності до збоїв у разі прийняття рішення щодо збільшення обсягів активів у результаті розширення діючих видів діяльності, запровадження нових продуктів та значних змін у діяльності банку, укладення нових / унесення суттєвих змін до діючих критичних договорів із TPSP-постачальниками.”;

4) пункт 78 глави 11 після підпункту 4<sup>1</sup> доповнити новим підпунктом 4<sup>2</sup> такого змісту:

“4<sup>2</sup>) укладення / припинення (розірвання) / унесення суттєвих змін до критичного договору з TPSP-постачальником;”.

2. У розділі VI:

1) у главі 44:

пункт 277 викласти в такій редакції:

“277. Банк самостійно визначає перелік кількісних показників ризик-апетиту до операційного ризику, які обов'язково повинні включати показники ризик-апетиту до ризику третіх сторін. Такий перелік повинен обов'язково включати показник максимального обсягу втрат від подій операційного ризику протягом наступних 12 місяців у цілому та в розрізі ризиків, які є складовими операційного ризику.”;

главу після пункту 277 доповнити новим пунктом 277<sup>1</sup> такого змісту:

“277<sup>1</sup>. Банк визначає ризик-апетит з урахуванням ризиків, пов'язаних з послугами, які банк отримує від TPSP-постачальників, та рівня толерантності до збоїв.

Оцінка ризиків, пов'язаних з послугами, які банк отримує від TPSP-постачальників, має бути орієнтованою на перспективу та враховувати стрес-тестування таких ризиків включно з використанням методу сценарного аналізу.”;

2) главу 45 після пункту 282 доповнити новим пунктом 282<sup>1</sup> такого змісту:

“282<sup>1</sup>. Банк створює ефективні механізми управління ризиком третіх сторін, які є частиною системи управління операційним ризиком банку, з урахуванням впливу ризику третіх сторін на інші ризики, що притаманні його діяльності.”;

3) розділ після глави 45<sup>1</sup> доповнити сімома новими главами 45<sup>2</sup>–45<sup>8</sup> такого змісту:

“45<sup>2</sup>. Загальні підходи до управління ризиком третіх сторін

290<sup>10</sup>. Банк забезпечує управління ризиком третіх сторін дотримуючись моделі трьох ліній захисту:

1) на першій лінії захисту – приймає ризик третіх сторін, несе відповідальність за нього, здійснює поточне управління ризиком третіх сторін, включаючи управління відносинами за договорами з TPSP-постачальниками, подає звіти щодо поточного управління таким ризиком;

2) на другій лінії захисту – здійснює управління та контроль за ризиком третіх сторін з урахуванням ризиків, пов'язаних із послугами, які банк отримує від TPSP-постачальників;

3) на третій лінії захисту – здійснює перевірку та оцінку ефективності стратегії / стратегій, політики, процесів, процедур управління ризиком третіх сторін.

290<sup>11</sup>. Банк для цілей управління ризиком третіх сторін відповідно до цього Положення має право не враховувати таких послуг, що надаються TPSP-постачальниками:

1) послуги, отримання яких вимагається законодавством України, включаючи послуги зовнішнього аудитора;

2) послуги глобальної карткової мережевої інфраструктури;

3) клірингові послуги, виконання функцій центрального контрагента, послуги центрального депозитарію цінних паперів та послуги розрахунків, що надаються кліринговими установами, центральними контрагентами, центральним депозитарієм цінних паперів та розрахунковими установами, включаючи надання таких послуг у державних платіжних системах;

4) послуги міжнародних міжбанківських систем передавання інформації та здійснення платежів;

5) послуги банків-кореспондентів;

6) послуги, які не мають впливу на профіль ризику банку та операційну діяльність (включаючи: послуги архітектора; юридичні, медичні, туристичні послуги; послуги з прибирання, озеленення та обслуговування приміщень, службових автомобілів банку; послуги з громадського харчування; послуги торгових автоматів, пошти, секретарів та операторів розподільних щитів, комутаторів; канцелярські послуги).

Банк за послугами, що отримуються від TPSP-постачальників, визначеними в пункті 290<sup>11</sup> глави 45<sup>2</sup> розділу VI цього Положення, зобов'язаний здійснювати управління ризиками, пов'язаними з отриманням таких послуг.

290<sup>12</sup>. Банк за послугами, що отримуються від TPSP-постачальника, регулювання та нагляд за діяльністю якого здійснюється державним органом, уповноваженим відповідно до законодавства України встановлювати обов'язкові до виконання правила діяльності у визначеній сфері, а також здійснювати контроль за дотриманням такого законодавства та застосовувати заходи впливу, включаючи такі сфери, як електропостачання, газопостачання, постачання теплової енергії, водопостачання та водовідведення, телефонний зв'язок і передача даних (далі – регульований TPSP-постачальник / регульована послуга TPSP-постачальника), здійснює оцінку ризику третіх сторін з

урахуванням судження щодо співставності вимог, установлених уповноваженим державним органом щодо діяльності такого TPSP-постачальника, з вимогами, установленими в цьому Положенні, з урахуванням специфіки діяльності TPSP-постачальника.

290<sup>13</sup>. Банк формує та супроводжує перелік договорів, укладених з TPSP-постачальниками, включаючи угоди про рівень сервісу / обслуговування (SLA) (далі – Перелік договорів).

Банк уносить до Переліку договорів інформацію, яка щонайменше має містити дані, які вносяться до переліку договорів, укладених з TPSP-постачальниками, включаючи угоди про рівень сервісу / обслуговування (SLA), що наведені в додатку 7 до цього Положення.

Банк оновлює інформацію в Переліку договорів не пізніше 90 календарного дня від дня:

- 1) укладення договору з новим TPSP-постачальником, нового договору з наявним TPSP-постачальником;
- 2) унесення суттєвих змін до умов договору з TPSP-постачальником;
- 3) припинення договору з TPSP-постачальником;
- 4) визначення банком суттєвої зміни рівня ризиків за послугами, що надаються TPSP-постачальником;
- 5) зміни визначеного банком рівня критичності послуги, що надається TPSP-постачальником;
- 6) зміни юрисдикції та/або географічного місця розташування, з якого відбувається надання послуги TPSP-постачальником;
- 7) реорганізації TPSP-постачальника;
- 8) зміни ключової n-ї сторони в ланцюгу постачання TPSP-постачальника.

290<sup>14</sup>. Банк несе відповідальність за ризики, пов'язані з укладенням договору з TPSP-постачальником та відносинами, що виникають на підставі такого договору.

Укладення банком договору з TPSP-постачальником не звільняє банк від відповідальності за недотримання вимог законодавства України, поточних зобов'язань перед вкладниками та кредиторами внаслідок реалізації / нереалізації такого договору.

Договір банку з TPSP-постачальником не повинен ускладнювати / унеможлилювати оцінку уповноваженими працівниками Національного банку системи управління ризиками банку.

290<sup>15</sup>. Банк під час встановлення відносин із TPSP-постачальником, укладання нових / унесення змін до діючих договорів, продовження або поновлення дії договорів та/або угод про рівень сервісу (SLA) і протягом терміну дії таких договорів / угод зобов'язаний враховувати вимоги, обмеження та заборони, установлені законодавством України, нормативно-правовими актами Національного банку та інших державних органів України, вимоги яких застосовуються до TPSP-постачальників у відповідній сфері, включаючи, але не обмежуючись таким:

1) наявності в TPSP-постачальника та/або його кінцевих бенефіціарних власників громадянства чи податкового резидентства держави-агресора та/або постійного проживання на території держави-агресора;

2) застосування до TPSP-постачальника, його кінцевих бенефіціарних власників Україною, іноземними державами (крім держав, які здійснюють збройну агресію проти України), міждержавними об'єднаннями або міжнародними організаціями санкцій (застосовується протягом строку дії санкцій і протягом трьох років після їх скасування або закінчення строку, на який їх було введено);

3) включення TPSP-постачальника, його кінцевих бенефіціарних власників до переліку осіб, пов'язаних із провадженням терористичної діяльності або стосовно яких застосовано міжнародні санкції (застосовується протягом строку перебування особи в переліку та протягом 10 років після виключення з нього);

4) перевірки TPSP-постачальника, його кінцевих бенефіціарних власників щодо належності до осіб, пов'язаних із державою-агресором, що зазначені в абзацах другому – п'ятому підпункту 1 пункту 1 постанови Кабінету Міністрів України від 03 березня 2022 року №187 “Про забезпечення захисту національних інтересів за майбутніми позовами держави Україна у зв'язку з військовою агресією Російської Федерації” (зі змінами).

45<sup>3</sup>. Політика залучення TPSP-постачальників, політика, порядок та процедури управління ризиком третіх сторін

290<sup>16</sup>. Банк розробляє та періодично (не рідше одного разу на рік) переглядає політику залучення TPSP-постачальників, політику, порядок та процедури управління ризиком третіх сторін, включаючи обрані банком для виконання на умовах аутсорсингу окремі функції банку.

290<sup>17</sup>. Політика залучення TPSP-постачальників може бути складовою стратегії / стратегій управління ризиками або окремим документом.

290<sup>18</sup>. Політика залучення TPSP-постачальників повинна обов'язково містити:

- 1) цілі банку щодо отримання послуг від TPSP-постачальників;
- 2) критерії, за якими банк визначає доцільність / необхідність отримання послуг від TPSP-постачальників;
- 3) перелік послуг, які банк визначив потенційно прийнятними для отримання від TPSP-постачальників;
- 4) види операцій / послуг банку, щодо здійснення / надання яких банк визначив неприйнятним залучення TPSP-постачальників;
- 5) критерії / вимоги до критичних TPSP-постачальників, включаючи вимоги до організації системи корпоративного управління, ділової репутації, кваліфікації персоналу, наявності активів, достатніх для здійснення таким TPSP-постачальником операційної діяльності, надання послуг банку;
- 6) принципи та підходи до визначення прийнятного співвідношення ризиків та переваг банку, пов'язаних із залежністю від одного або кількох TPSP-постачальників;
- 7) підходи до аналізу ризиків та переваг банку у зв'язку з використанням TPSP-постачальниками нових технологій;
- 8) умови, наслідком яких є прийняття банком рішення про припинення договору / відмову від укладення договору з критичним TPSP-постачальником, включаючи встановлення ознак невідповідності ділової репутації такого TPSP-постачальника, його кінцевих бенефіціарних власників та керівників, ознакам, визначеним у пункті 65 глави 6 розділу II, пункті 69 глави 7 розділу II Положення про ліцензування банків, затвердженого постановою Правління Національного банку України від 22 грудня 2018 року № 149 (зі змінами) (далі – Положення № 149), та іншим ознакам, установленим у внутрішньобанківських документах щодо управління ризиком третіх сторін;
- 9) вимоги до договорів з TPSP-постачальниками.

Банк не включає до політики залучення TPSP-постачальників послуги, визначені в пункті 290<sup>11</sup> глави 45<sup>2</sup> розділу VI цього Положення.

290<sup>19</sup>. Політика, порядок та процедури управління ризиком третіх сторін повинні відповідати стратегії / стратегіям управління ризиками та політиці залучення TPSP-постачальників.

290<sup>20</sup>. Політика, порядок та процедури управління ризиком третіх сторін можуть бути складовими політики, порядку та процедур управління операційним ризиком або окремими документами.

290<sup>21</sup>. Політика управління ризиком третіх сторін повинна обов'язково містити:

- 1) мету, завдання та принципи управління ризиком третіх сторін;
- 2) організаційну структуру процесу управління ризиком третіх сторін з урахуванням розподілу функціональних обов'язків між учасниками процесу, їх повноваження, відповідальність та порядок взаємодії;
- 3) перелік лімітів для контролю за рівнем ризику третіх сторін та порядок їх установлення;
- 4) підходи щодо виявлення, вимірювання, моніторингу, контролю, звітування та пом'якшення ризику третіх сторін, включаючи підходи до оцінки та моніторингу:
  - відсутності щодо критичного TPSP-постачальника, його кінцевих бенефіціарних власників та керівників ознак небездоганної ділової репутації, визначених у пункті 65 глави 6 розділу II, пункті 69 глави 7 розділу II Положення № 149, та інших ознак, установлених у внутрішньобанківських документах щодо управління ризиком третіх сторін;
  - відповідності критичного TPSP-постачальника критеріям операційної та фінансової спроможності, визначеним у пунктах 290<sup>40</sup>, 290<sup>41</sup> глави 45<sup>5</sup> розділу VI цього Положення;
  - відповідності укладених договорів умовам, визначеним у пунктах 290<sup>49</sup>, 290<sup>50</sup> глави 45<sup>6</sup> розділу VI цього Положення, та/або дотримання TPSP-постачальником / критичним TPSP-постачальником таких умов під час виконання договору;
- 5) підходи до здійснення стрес-тестування ризику третіх сторін за базовим та несприятливим сценаріями;
- 6) перелік та формат (інформаційне наповнення) форм управлінської звітності щодо ризику третіх сторін, порядок і періодичність / терміни їх подання суб'єктам системи управління ризиками.

290<sup>22</sup>. Банк з метою дотримання встановлених лімітів ризику третіх сторін, ризик-апетиту щодо операційного ризику, ризик-апетиту щодо ризику третіх сторін, рівня толерантності до збоїв уживає таких заходів:

- 1) визначає альтернативних TPSP-постачальників; та / або
- 2) поєднує використання власної інфраструктури з послугами TPSP-постачальника; та/або
- 3) забезпечує / зберігає можливість використання виключно власної інфраструктури для виконання робіт самостійно за послугами, що надаються TPSP-постачальником.

290<sup>23</sup>. Порядок та процедури управління ризиком третіх сторін повинні обов'язково містити:

1) процедури щодо виявлення, вимірювання, моніторингу, контролю, звітування та пом'якшення ризику третіх сторін, включаючи процедури оцінки та моніторингу:

відсутності щодо критичного TPSP-постачальника, його кінцевих бенефіціарних власників та керівників ознак небездоганної ділової репутації, визначених у пункті 65 глави 6 розділу II, пункті 69 глави 7 розділу II Положення № 149, та інших ознак, установлених у внутрішньобанківських документах щодо управління ризиком третіх сторін;

відповідності критичного TPSP-постачальника критеріям операційної та фінансової спроможності, визначеним у пунктах 290<sup>40</sup>, 290<sup>41</sup> глави 45<sup>5</sup> розділу VI цього Положення;

відповідності укладених договорів умовам, визначеним у пунктах 290<sup>49</sup>, 290<sup>50</sup> глави 45<sup>6</sup> розділу VI цього Положення, та/або дотримання TPSP-постачальником / критичним TPSP-постачальником таких умов під час виконання договору;

2) процедури ескалації інформації та звітування про встановлені факти невідповідності ділової репутації критичного TPSP-постачальника, його кінцевих бенефіціарних власників та керівників ознакам щодо ділової репутації, критеріям операційної та фінансової спроможності, умовам критичного договору згідно зі встановленими внутрішньобанківськими документами, включаючи форму та порядок інформування про такі порушення ради банку, комітету з управління ризиками, правління банку та його комітетів;

3) порядок обміну інформацією між учасниками процесу управління ризиком третіх сторін, включаючи види, форми і строки надання інформації;

4) програму проведення стрес-тестування ризику третіх сторін за базовим та несприятливим сценаріями;

5) процедури управління ризиком ланцюга постачання;

6) підхід до вимірювання та контролю ризику третіх сторін на рівні окремого договору з TPSP-постачальником;

7) критерії визначення критичних послуг, які надаються TPSP-постачальником;

8) критерії визначення критичних функцій, які підтримуються послугами TPSP-постачальників;

9) підхід до моніторингу інцидентів у діяльності TPSP-постачальників, звітування та реагування на них;

10) порядок формування судження щодо співставності встановлених уповноваженим державним органом вимог до діяльності TPSP-постачальників з вимогами, установленими цим Положенням, з урахуванням специфіки діяльності TPSP-постачальників;

11) порядок формування судження про неспроможність TPSP-постачальника забезпечувати надання послуги банку, яка відповідає визначеному в договорі рівню якості, доступності та ефективності, підхід до вимірювання та контролю ризику третіх сторін на рівні окремого договору з TPSP-постачальником.

290<sup>24</sup>. Порядок та процедури управління ризиком третіх сторін повинні охоплювати всі етапи життєвого циклу відносин банку з TPSP-постачальником.

Етапами життєвого циклу відносин банку з TPSP-постачальником є:

1) оцінка ризику третіх сторін та вразливості банку до такого ризику;

2) здійснення комплексної перевірки критичного TPSP-постачальника перед установам договорних відносин;

3) укладення договору з TPSP-постачальником;

4) початок договірних відносин із TPSP-постачальником і моніторинг виконання умов договору;

5) припинення договірних відносин із TPSP-постачальником.

Кожний етап життєвого циклу відносин із TPSP-постачальником має відповідати стратегії банку, політиці залучення TPSP-постачальників, політиці, порядкам та процедурам управління ризиком третіх сторін.

290<sup>25</sup>. Банк здійснює управління ризиком третіх сторін та оцінку вразливості банку до такого ризику на всіх етапах життєвого циклу відносин із TPSP-постачальником з урахуванням:

1) критичності TPSP-постачальника, послуги, що надається TPSP-постачальником, та договору / договорів, укладеного / укладених із таким TPSP-постачальником;

2) оцінки ризику концентрації послуг за договорами з TPSP-постачальником, ураховуючи, що кілька некритичних договорів із TPSP-постачальником можуть становити для банку вищий ризик, ніж один критичний договір із таким TPSP-постачальником;

3) адекватності механізмів управління ризиком третіх сторін розміру банку, його бізнес-моделі, масштабу діяльності, видам, складності операцій, профілю ризиків, діяльності банку, що здійснюється за кордоном, рівню ризиків та критичності договорів з TPSP-постачальниками;

4) оцінки ризику третіх сторін за договорами з внутрішньогруповим TPSP-постачальником.

Банк здійснює управління ризиком третіх сторін за договорами з внутрішньогруповим TPSP-постачальником, який включений до системи управління ризиками в банківській групі, у межах системи управління ризиками в банківській групі, організованої відповідальною особою банківської групи згідно з вимогами цього Положення.

Банк, якщо відповідальною особою банківської групи згідно з пунктом 18<sup>1</sup> глави 2 розділу I цього Положення система управління ризиками в банківській групі організована без урахування учасника банківської групи, який є TPSP-постачальником, здійснює управління ризиком третіх сторін за договорами з таким TPSP-постачальником згідно з вимогами цього Положення, установленими для TPSP-постачальника, який не є внутрішньогруповим TPSP-постачальником;

5) оцінки здатності TPSP-постачальника забезпечити належне виконання своїх зобов'язань за всіма договорами перед банком, включаючи оцінку залежності виконання таких зобов'язань від виконання умов договорів n-ми сторонами в ланцюгу постачання послуги для банку TPSP-постачальником та здатності такого TPSP-постачальника управляти ризиком ланцюга постачання.

Процедури управління ризиком ланцюга постачання повинні бути адекватними рівням ризиків та критичності послуг, що надаються.

Банк здійснює аналіз ланцюга постачання за:

TPSP-постачальниками;

n-ми сторонами, які є другою та третьою сторонами в ланцюгу постачання. Першою стороною в ланцюгу постачання є сам TPSP-постачальник, другою та третьою сторонами – є відповідно наступні сторони, які є постачальниками послуг для TPSP-постачальника в ланцюгу постачання.

Банк має право не здійснювати аналізу ланцюга постачання за n-ми сторонами, які є наступними сторонами після третьої сторони в ланцюгу постачання послуг для TPSP-постачальника, якщо банк на підставі судження довів відсутність впливу такої n-ї сторони на здатність TPSP-постачальника забезпечувати належне виконання своїх зобов'язань перед банком за всіма договорами.

Банк визначає ключові n-ні сторони в ланцюгу постачання критичних TPSP-постачальників.

Банк включає інформацію про ключові n-ні сторони до карти взаємозв'язків і взаємозалежностей між TPSP-постачальниками та враховує її під час оцінки ризику третіх сторін, включаючи оцінку ризику концентрації послуг;

6) впливу розвитку нових технологій на підвищення залежності банку від TPSP-постачальника.

Банк забезпечує наявність кваліфікованих і досвідчених працівників, здатних забезпечити належне управління ризиком третіх сторін, пов'язаним із розвитком нових технологій, створенням нових / зміною діючих продуктів / сервісів із використанням таких технологій;

7) іншої інформації (за наявності), яка забезпечує додаткову впевненість банку щодо рівня організації системи внутрішнього контролю в діяльності критичного TPSP-постачальника / його ключової n-ї сторони на належному рівні, включаючи:

результати перевірки зовнішнім аудитором або іншим незалежним суб'єктом, який проводить незалежну професійну діяльність, критичного TPSP-постачальника / його ключової n-ї сторони;

відповідність діяльності критичного TPSP-постачальника / його ключової n-ї сторони вимогам національних стандартів України (ДСТУ) та міжнародних стандартів (ISO).

290<sup>26</sup>. Банк оновлює (за потреби) порядок та процедури управління ризиком третіх сторін на кожному з етапів життєвого циклу відносин із TPSP-постачальником з урахуванням інформації, отриманої на інших етапах життєвого циклу відносин із таким TPSP-постачальником.

45<sup>4</sup>. Оцінка ризику третіх сторін та вразливості банку до такого ризику

290<sup>27</sup>. Банк під час оцінки ризику третіх сторін здійснює оцінку:

- 1) внутрішніх та зовнішніх факторів ризику третіх сторін;
- 2) ризиків, на які наражатиметься / наражається банк унаслідок укладення договору з TPSP-постачальником;
- 3) критичності послуги, яка надаватиметься / надається банку TPSP-постачальником.

290<sup>28</sup>. Банк під час оцінки ризиків, на які наражатиметься / наражається банк унаслідок укладення договору з TPSP-постачальником, ураховує:

- 1) ризик концентрації послуг;
- 2) ризик, пов'язаний з довгими ланцюгами постачання;
- 3) ризик, пов'язаний з розвитком нових технологій;
- 4) вплив ризику третіх сторін на інші ризики, притаманні діяльності банку, та безперервність його діяльності.

Довгим ланцюгом постачання для цілей управління ризиком третіх сторін є ланцюг постачання, який містить три та більше сторін.

Ланцюг постачання обмежується послугами, що надаються банку / учаснику банківської групи в межах договору з TPSP-постачальником.

290<sup>29</sup>. Банк під час оцінки критичності послуги, яка надаватиметься / надається банку TPSP-постачальником, ураховує:

- 1) потенційний вплив (позитивний та негативний) від укладення нового / унесення змін до діючого договору з TPSP-постачальником на операції банку, системи, дані, безперервність його діяльності;
- 2) рівень толерантності банку до збоїв;
- 3) характер даних та інформації, якими обмінюватиметься / обмінюється банк із TPSP-постачальником;
- 4) можливість та складність заміни TPSP-постачальника.

290<sup>30</sup>. Банк з урахуванням результатів оцінки ризику третіх сторін:

1) оцінює адекватність процедур внутрішнього контролю щодо своєчасності та якості отримання банком послуг за укладеними договорами з TPSP-постачальниками;

2) визначає механізми моніторингу, звітування та ескалації інформації про ризик третіх сторін;

3) визначає заходи щодо пом'якшення ризику третіх сторін;

4) запроваджує процедури інформування ради, правління, відповідних підрозділів, включаючи підрозділ з управління ризиками, з урахуванням розподілу обов'язків та повноважень, щодо очікуваного впливу від укладання нових договорів, унесення змін до діючих договорів із TPSP-постачальниками на процеси та діяльність банку;

5) розробляє процедури визначення умов договорів із TPSP-постачальниками з урахуванням специфіки послуг, що надаються TPSP-постачальниками, та їх впливу на процеси та діяльність банку.

290<sup>31</sup>. Банк забезпечує належний рівень документування процесу і результатів оцінки ризиків за договорами з TPSP-постачальниками.

45<sup>5</sup>. Здійснення комплексної перевірки критичного TPSP-постачальника перед установами договірних відносин

290<sup>32</sup>. Банк перед укладенням критичного договору з TPSP-постачальником здійснює комплексну перевірку критичного TPSP-постачальника.

290<sup>33</sup>. Банк з метою комплексної перевірки критичного TPSP-постачальника здійснює:

1) збір та аналіз інформації, необхідної для визначення відповідності критичного TPSP-постачальника політиці залучення TPSP-постачальників;

2) оцінку відповідності критичного TPSP-постачальника вимогам, визначеним у пункті 290<sup>15</sup> глави 45<sup>2</sup> розділу VI цього Положення;

3) оцінку ділової репутації критичного TPSP-постачальника, його кінцевих бенефіціарних власників та керівників з урахуванням ознак небездоганної ділової репутації, визначених у пункті 65 глави 6 розділу II, пункті 69 глави 7 розділу II Положення № 149, та інших ознак, установлених у внутрішньобанківських документах щодо управління ризиком третіх сторін;

4) оцінку відповідності критичного TPSP-постачальника критеріям операційної та фінансової спроможності, визначеним у пунктах 290<sup>40</sup>, 290<sup>41</sup> глави 45<sup>5</sup> розділу VI цього Положення;

5) аналіз ризиків, на які може наражатися банк у разі укладення договору з критичним TPSP-постачальником;

6) оцінку спроможності банку належно управляти ризиком третіх сторін, пов'язаним з укладенням договору з критичним TPSP-постачальником;

7) обґрунтування фінансової та операційної доцільності укладення договору з критичним TPSP-постачальником.

290<sup>34</sup>. Банк з метою визначення відповідності критичного TPSP-постачальника політиці залучення TPSP-постачальників здійснює аналіз отриманої від критичного TPSP-постачальника інформації про:

1) проведену критичним TPSP-постачальником власну оцінку ефективності системи внутрішнього контролю та управління ризиками, включаючи управління ризиком ICT, кіберризиком та іншими операційними ризиками за критеріями, визначеними для регульованих TPSP-постачальників / регульованої послуги TPSP-постачальника – уповноваженим державним органом, для інших критичних TPSP-постачальників – банком з урахуванням вимог цього Положення;

2) наявність у критичного TPSP-постачальника достатньої кількості кваліфікованих і досвідчених працівників для забезпечення безперервного надання послуг банку, включаючи доступність таких послуг під час збоїв у роботі критичного TPSP-постачальника;

3) спроможність критичного TPSP-постачальника управляти ризиком ланцюга постачання, включаючи спроможність виявляти ключові n-ні сторони;

4) операційну та технічну спроможність критичного TPSP-постачальника забезпечувати власну безперебійну діяльність;

5) спроможність критичного TPSP-постачальника надавати банку послуги, що забезпечують:

дотримання банком політики залучення TPSP-постачальників;

досягнення банком стратегічних цілей щодо розширення діяльності із застосуванням сучасних технологій;

дотримання банком вимог законодавства України та встановлених обмежень (за наявності);

здійснення банком безперервної діяльності з урахуванням визначеного рівня толерантності до збоїв, включаючи реалізацію заходів із відновлення систем та сервісів ІСТ після збоїв;

б) готовність оперативно надавати банку на його запит необхідну інформацію.

290<sup>35</sup>. Банк здійснює оцінку ділової репутації критичного TPSP-постачальника, його кінцевих бенефіціарних власників та керівників з урахуванням ознак небездоганної ділової репутації, визначених у пункті 65 глави 6 розділу II, пункті 69 глави 7 розділу II Положення № 149, та інших ознак, установлених у внутрішньобанківських документах щодо управління ризиком третіх сторін.

290<sup>36</sup>. Банк включає до ознак небездоганної ділової репутації критичного TPSP-постачальника, його кінцевих бенефіціарних власників та керівників щонайменше такі ознаки:

1) щодо фізичної особи – ознаки, установлені в пункті 65 глави 6 розділу II Положення № 149;

2) щодо юридичної особи – ознаки, установлені в пункті 69 глави 7 розділу II Положення № 149.

290<sup>37</sup>. Банк додатково до ознак, установлених у пункті 65 глави 6 розділу II, пункті 69 глави 7 розділу II Положення № 149, установлює у внутрішньобанківських документах щодо управління ризиком третіх сторін ознаки небездоганної ділової репутації критичного TPSP-постачальника, його кінцевих бенефіціарних власників та керівників, включаючи відсутність підтверджених фактів вчинення кримінальних правопорушень проти власності, корупційних кримінальних правопорушень / кримінальних правопорушень, пов'язаних із корупцією, кримінальних правопорушень у сфері господарської діяльності, з метою комплексної, своєчасної та адекватної оцінки ризиків, на які може наражатися банк унаслідок установлення / підтримання відносин із критичним TPSP-постачальником.

290<sup>38</sup>. Банк з метою здійснення оцінки ділової репутації критичного TPSP-постачальника, його кінцевих бенефіціарних власників та керівників надсилає критичному TPSP-постачальнику запит про отримання документів та/або інформації, необхідних / необхідної для підтвердження їх ділової репутації.

Банк здійснює оцінку ділової репутації критичного TPSP-постачальника, його кінцевих бенефіціарних власників та керівників шляхом:

1) перевірки достовірності поданих / наданої критичним TPSP-постачальником документів та/або інформації;

2) перевірки відсутності в критичного TPSP-постачальника, його кінцевих бенефіціарних власників та керівників ознак небездоганної ділової репутації, визначених у пункті 65 глави 6 розділу II, пункті 69 глави 7 розділу II Положення № 149, та інших ознак, установлених у внутрішньобанківських документах щодо управління ризиком третіх сторін.

290<sup>39</sup>. Банк визначає наявність ознак небездоганної ділової репутації критичного TPSP-постачальника, його кінцевих бенефіціарних власників та керівників на підставі судження, сформованого з урахуванням інформації, отриманої від критичного TPSP-постачальника, а також інформації, що є в державних реєстрах, інформаційних системах органів державної влади, медіа, інших відкритих джерелах.

290<sup>40</sup>. Банк здійснює аналіз операційної спроможності критичного TPSP-постачальника надавати послуги відповідно до умов договору на відповідність щонайменше таким критеріям:

1) наявність щодо критичного TPSP-постачальника документального підтвердження:

належного (релевантного) досвіду протягом не менше 12 місяців поспіль, що передують такому аналізу, виконання ним укладених договорів / угод про рівень сервісу / обслуговування (SLA);

спроможності забезпечувати виконання зобов'язань, включаючи наявність кваліфікованих і досвідчених працівників, необхідних для виконання таким TPSP-постачальником умов договору / договорів із банком;

2) наявність у критичного TPSP-постачальника у власності або довгостроковій оренді / лізингу активів, достатніх для здійснення операційної діяльності, надання послуг, належного та своєчасного виконання умов договору / договорів із банком;

3) немає судових спорів щодо невиконання / неналежного виконання критичним TPSP-постачальником умов договору / договорів / угод про рівень сервісу / обслуговування (SLA), які за обґрунтованим судженням банку можуть негативно вплинути на належне виконання критичним TPSP-постачальником договору з банком.

Банк під час здійснення аналізу операційної спроможності критичного TPSP-постачальника на відповідність критеріям, визначеним у пункті 290<sup>40</sup> глави 45<sup>5</sup> розділу VI цього Положення, має право враховувати результати перевірки критичного TPSP-постачальника зовнішнім аудитором або іншим незалежним суб'єктом, який проводить незалежну професійну діяльність, а також відповідність критичного TPSP-постачальника вимогам національних стандартів України (ДСТУ), міжнародних стандартів (ISO) за відповідними напрямками діяльності критичного TPSP-постачальника, підтверджену діючими станом на дату здійснення аналізу сертифікатами.

290<sup>41</sup>. Банк здійснює аналіз фінансової спроможності критичного TPSP-постачальника надавати послуги відповідно до умов договору на відповідність щонайменше таким критеріям:

1) відповідність значень показників фінансового стану критичного TPSP-постачальника, визначених банком у внутрішньобанківських документах щодо управління ризиком третіх сторін;

2) немає негативного розміру власного капіталу критичного TPSP-постачальника, що підтверджується фінансовою звітністю за останній звітний період;

3) немає невиконаних критичним TPSP-постачальником понад 180 календарних днів фінансових зобов'язань перед кредиторами / контрагентами та/або органами державної влади на суму, що перевищує 50 тисяч гривень, або 10% від сукупної суми зобов'язань за договором, укладеним з таким TPSP-постачальником. Банк у разі наявності факту щодо невиконаних критичним TPSP-постачальником фінансових зобов'язань на підставі сформованого судження має право прийняти рішення про те, що такий факт не має негативного впливу на належне виконання критичним TPSP-постачальником договору з банком.

290<sup>42</sup>. Аналіз ризиків, на які може наражатися банк у разі укладення договору з критичним TPSP-постачальником, повинен включати щонайменше оцінку:

1) розподілу відповідальності між банком і критичним TPSP-постачальником згідно з умовами договору щодо забезпечення безпеки, включаючи інформаційну безпеку та кіберзахист, а також стабільності під час надання послуг;

2) прозорості структури власності критичного TPSP-постачальника. Структура власності TPSP-постачальника є непрозорою, якщо неможливо

визначити всіх кінцевих бенефіціарних власників TPSP-постачальника через, але не виключно, наявність ознак номінального володіння, використання трастів або інших подібних правових утворень, офшорних зон, неповне розкриття або відмову в розкритті, або надання TPSP-постачальником недостовірної / неповної інформації, або інші обставини, що унеможливають встановлення кінцевих бенефіціарних власників;

3) ризику концентрації послуг;

4) ризиків, пов'язаних з географічним регіоном фактичного розташування критичного TPSP-постачальника, які, серед іншого, пов'язані зі стихійними лихами, економічною, соціальною, політичною сферами, правовим та регуляторним середовищем країни, з території якої надаватиметься відповідна послуга;

5) наявності потенційного конфлікту інтересів між банком та критичним TPSP-постачальником, включаючи ключові п-ні сторони;

6) усієї доступної інформації щодо діяльності критичного TPSP-постачальника, його кінцевих бенефіціарних власників та керівників, включаючи наявність або відсутність поточних, нещодавно завершених чи незавершених процесів чи обставин, що можуть свідчити про підвищений операційний, включаючи юридичний / репутаційний ризик або комплаєнс-ризик критичного TPSP-постачальника, включаючи, але не обмежуючись результатами нещодавно завершених регуляторних перевірок, застосованих заходів впливу [штрафів, приписів, зупинення повністю або частково (тимчасове призупинення) або припинення (анулювання) ліцензій, обмеження діяльності], результатами внутрішніх розслідувань, адміністративних, цивільних або кримінальних проваджень;

7) доступності альтернативних критичних TPSP-постачальників;

8) інших фактів, подій, обставин, що можуть свідчити про наявність ризиків, на які може наражатися банк у разі укладення договору з критичним TPSP-постачальником.

290<sup>43</sup>. Банк оцінює ризик концентрації послуг під час здійснення комплексного аналізу критичного TPSP-постачальника та протягом усього життєвого циклу відносин з ним.

Ризик концентрації послуг є щонайменше в разі наявності одного або кількох із таких випадків:

1) надання одним TPSP-постачальником кількох критичних послуг або кількох некритичних послуг, які в сукупності є критичними для безперервності діяльності банку;

2) надання послуг критичним TPSP-постачальником, який є єдиним на ринку, якщо немає альтернативних критичних TPSP-постачальників;

3) наявність концентрації критичних послуг або кількох некритичних послуг, що надаються одним або кількома TPSP-постачальниками та/або в одному географічному регіоні, які в сукупності є критичними для безперервності діяльності банку;

4) наявність залежності від однієї ключової п-ї сторони кількох критичних TPSP-постачальників, що надають критичні послуги, або кілька некритичних послуг, які в сукупності є критичними для безперервності діяльності банку.

Банк здійснює оцінку ризику концентрації послуг з урахуванням інформації, яка міститься в Переліку договорів та в карті взаємозв'язків і взаємозалежностей між TPSP-постачальниками.

290<sup>44</sup>. Банк з метою обґрунтування фінансової та операційної доцільності укладення договору з критичним TPSP-постачальником здійснює щонайменше оцінку:

1) переваг та недоліків для банку від укладення договору;

2) витрат, які банку необхідно здійснити відповідно до умов договору;

3) потенційних ризиків, на які може наражатися банк унаслідок укладення / неукладення договору, включаючи ризик несвоєчасної заміни застарілих систем та сервісів, необхідності найму та утримання кваліфікованих та досвідчених працівників;

4) спроможності банку достроково розірвати критичний договір з критичним TPSP-постачальником (включаючи одностороннє припинення договірних відносин за ініціативою банку), ураховуючи фінансові, юридичні та репутаційні наслідки такого розірвання, а також ураховуючи вартість, строки та можливість укладення договору з аналогічним предметом регулювання з іншим альтернативним критичним TPSP-постачальником або можливість здійснення такої діяльності без залучення TPSP-постачальника, або із застосуванням іншого визначеного банком варіанта;

5) спроможності банку запроваджувати нові технології, а також потенційних ризиків банку, пов'язаних із використанням / застосуванням таких технологій.

290<sup>45</sup>. Банк у разі виявлення невідповідності критичного TPSP-постачальника вимогам пункту 290<sup>15</sup> глави 45<sup>2</sup> розділу VI цього Положення приймає рішення про відмову від встановлення договірних відносин із таким TPSP-постачальником.

290<sup>46</sup>. Банк у разі виявлення щодо критичного TPSP-постачальника ознак небездоганної ділової репутації, установлених у пункті 65 глави 6 розділу II, пункті 69 глави 7 розділу II Положення № 149, та інших ознак небездоганної ділової репутації, установлених у внутрішньобанківських документах щодо управління ризиком третіх сторін, та/або невідповідності критеріям операційної та фінансової спроможності, визначеним у пунктах 290<sup>40</sup>, 290<sup>41</sup> глави 45<sup>5</sup> розділу VI цього Положення, приймає рішення про доцільність встановлення або відмову від встановлення договірних відносин із таким TPSP-постачальником.

Банк у разі прийняття рішення про встановлення договірних відносин із критичним TPSP-постачальником починаючи з дня укладення договору та до дня забезпечення критичним TPSP-постачальником усунення ознак небездоганної ділової репутації, забезпечення відповідності критеріям операційної та фінансової спроможності:

1) визначає рівень ризику третіх сторін за договором із таким TPSP-постачальником як високий;

2) ураховує такий ризик під час здійснення стрес-тестування ризику третіх сторін за базовим сценарієм;

3) здійснює оцінку потенційного впливу повного припинення надання таким TPSP-постачальником послуг банку на безперервність діяльності та профіль ризику банку.

#### 45<sup>6</sup>. Укладення договору з TPSP-постачальником

290<sup>47</sup>. Банк укладає договір з TPSP-постачальником у письмовій (електронній) формі з накладанням електронного підпису або підпису, прирівняного до власноручного підпису відповідно до Закону України “Про електронну ідентифікацію та електронні довірчі послуги”, та з урахуванням вимог, визначених цим Положенням.

290<sup>48</sup>. Умови договору з TPSP-постачальником повинні:

1) узгоджуватися з політикою залучення TPSP-постачальників, політикою, порядками та процедурами банку щодо управління ризиком третіх сторін;

2) урахувувати критичність послуги, а також вимоги законодавства країн, в яких банк і TPSP-постачальник здійснюють свою діяльність.

290<sup>49</sup>. Банк у договорі з TPSP-постачальником визначає щонайменше:

1) ключові умови щодо рівня сервісу / обслуговування (SLA), якщо не укладено окрему угоду про рівень сервісу / обслуговування (SLA);

2) обов'язок TPSP-постачальника надавати банку точну, повну та своєчасну інформацію про наявність вимог, обмежень та заборон, зазначених у пункті 290<sup>15</sup> глави 45<sup>2</sup> розділу VI цього Положення, а в разі ненадання такої інформації та/або встановлення невідповідності TPSP-постачальника вимогам пункту 290<sup>15</sup> глави 45<sup>2</sup> розділу VI цього Положення – право банку розірвати договір в односторонньому порядку;

3) обов'язок TPSP-постачальника надавати банку точну, повну та своєчасну інформацію, яка впливає на виконання та/або пов'язана з виконанням умов договору, включаючи інформацію про управління TPSP-постачальником ризиком третіх сторін, інциденти TPSP-постачальника;

4) права TPSP-постачальника щодо отримання від банку необхідної інформації / даних згідно з угодою про рівень сервісу / обслуговування (SLA), дотримання банком встановлених технічних вимог та забезпечення банком доступу TPSP-постачальнику до об'єктів, пов'язаних із наданням послуг, у встановленому банком порядку (за потреби);

5) зобов'язання TPSP-постачальника щодо забезпечення безперервності діяльності щодо надання послуг банку та відповідальність за невиконання таких зобов'язань;

6) вартість послуг, включаючи можливість / умови диференціації їх вартості залежно від обсягу використання послуги банком;

7) права власності, доступу та використання логічних активів, включаючи дані, додатки, інтерфейси прикладного програмування (API), моделі, права інтелектуальної власності, та фізичних активів, включаючи обладнання, документацію, приміщення, а також особливості передавання таких активів (необхідний час та формат), включаючи в разі припинення діяльності;

8) зобов'язання та відповідальність, пов'язані з безпекою, включаючи інформаційну безпеку та кіберзахист, стабільність / надійність надання послуг;

9) місце (регіон, країна), з якого надаватимуться послуги TPSP-постачальником, та місцезнаходження (регіон, країна) центрів обробки та збереження даних TPSP-постачальником;

10) уникнення ризику змішування TPSP-постачальником інформації банку з інформацією інших його клієнтів;

11) право банку на отримання відшкодування від TPSP-постачальника, обставини, умови та порядок отримання банком такого відшкодування;

12) порядок розгляду скарг клієнтів банку, пов'язаних з отриманням послуг від TPSP-постачальника, та вирішення спорів;

13) дії сторін у разі дострокового розірвання договору з TPSP-постачальником через невиконання / неналежне виконання сторонами зобов'язань за договором, включаючи вимоги щодо попереднього повідомлення про наміри дострокового розірвання договору та мінімальні строки для такого повідомлення;

14) положення про вибір права та підсудності в разі виникнення спорів між банком і TPSP-постачальником, за винятком виключної підсудності (з наданням переваги застосуванню права України та підсудності справам судам України);

15) умови щодо підтримки TPSP-постачальником виходу банку з відносин у разі дострокового розірвання договору з таким TPSP-постачальником;

16) наявність зобов'язань TPSP-постачальника про нерозголошення інформації (англійською мовою NDA – Non-disclosure Agreement), публічне розкриття якої матиме суттєвий негативний вплив на конкурентну ринкову позицію банку та/або його клієнтів / контрагентів на ринку;

17) згоду TPSP-постачальника на надання банком Національному банку на його запит інформації (за винятком інформації щодо вартості послуг та порядку її визначення), отриманої банком під час укладення та виконання договору;

18) підстави, порядок перегляду умов договору, унесення до нього змін, включаючи зміни, пов'язані зі змінами в законодавстві України, та припинення його дії, включаючи розірвання.

290<sup>50</sup>. Банк у договорі з критичним TPSP-постачальником визначає щонайменше умови, визначені в пункті 290<sup>49</sup> глави 45<sup>6</sup> розділу VI цього Положення, а також:

1) обов'язок критичного TPSP-постачальника надавати банку точну, повну та своєчасну інформацію про:

ключових n-х сторін, включаючи повідомлення про використання / зміну ключової n-ї сторони;

суттєві зміни в послугах, що надаються критичним TPSP-постачальником; повідомлення про інциденти в ключової n-ї сторони, що впливають / можуть мати вплив на надання критичним TPSP-постачальником послуг банку;

2) обов'язок критичного TPSP-постачальника передбачати в договорах, які укладаються з ключовими n-ми сторонами, згоду ключових n-х сторін на надання банку на його запит інформації щодо ключової n-ї сторони (за винятком інформації щодо вартості послуг ключової n-ї сторони та порядку її визначення), яка впливає на виконання та/або пов'язана з виконанням такою стороною умов договору;

3) обов'язок критичного TPSP-постачальника надавати банку інформацію про діяльність ключової n-ї сторони, визначену в підпункті 7 пункту 290<sup>25</sup> глави 45<sup>3</sup> розділу VI цього Положення;

4) зобов'язання критичного TPSP-постачальника щодо забезпечення безперервності діяльності щодо надання послуг банку, а також його участі в тестуванні плану забезпечення безперервної діяльності банку та відповідальність за невиконання таких зобов'язань;

5) установлення додаткових показників ефективності виконання критичним TPSP-постачальником умов договору, включаючи інформацію про результати проведених критичним TPSP-постачальником тестування власного плану забезпечення безперервної діяльності, оцінку ефективності внутрішнього контролю, наявність скарг від його клієнтів;

6) право банку на доступ до приміщень критичного TPSP-постачальника, проведення перевірок діяльності критичного TPSP-постачальника, включаючи незалежними сторонами, та отримання інформації про діяльність критичного TPSP-постачальника, визначеної в підпункті 7 пункту 290<sup>25</sup> глави 45<sup>3</sup> розділу VI цього Положення;

7) зобов'язання критичного TPSP-постачальника щодо визначення ним у плані забезпечення безперервної діяльності:

мінімального часу безперервної роботи та максимального часу простою в наданні послуг;

максимального часового інтервалу, протягом якого втрата даних банку в разі значного інциденту / збою / відмови систем та сервісів до моменту їх відновлення вважаються допустимими для критичних бізнес-процесів та функцій банку, не перевищуючи критичного рівня втрат (англійською мовою *recovery point objective*) (далі – RPO);

цільового часового інтервалу на відновлення процесів і систем, що обслуговують цей бізнес-процес, після інциденту / збою / переривання діяльності (англійською мовою *recovery time objective*) (далі – RTO);

8) зобов'язання критичного TPSP-постачальника щодо своєчасного надання банку інформації / повідомлення про інциденти в його діяльності та/або діяльності ключової n-ї сторони, які впливають на спроможність виконувати зобов'язання, визначені в договорі, включаючи вимоги до мінімального змісту інформації, яку необхідно повідомляти, та строку її надання;

9) запровадження критичним TPSP-постачальником процесів виявлення, розслідування та усунення інцидентів, пов'язаних із послугами, що надаються банку.

290<sup>51</sup>. Банк у разі укладення договору з TPSP-постачальником, що є надавачем хмарних послуг, керується умовами та вимогами, що визначені в главі IV Положення про порядок застосування технології хмарних обчислень, затвердженого постановою Правління Національного банку України від 25 серпня 2025 року № 99.

290<sup>52</sup>. Банк у разі укладення нового договору / унесення змін до діючого договору з TPSP-постачальником оновлює карту взаємозв'язків і взаємозалежностей між TPSP-постачальниками.

45<sup>7</sup>. Початок договірних відносин з TPSP-постачальником та моніторинг виконання умов договору

290<sup>53</sup>. Банк для виконання умов договору з TPSP-постачальником забезпечує належну комунікацію з TPSP-постачальником та надає йому необхідну інформацію з дотриманням вимог законодавства України та внутрішньобанківських документів з метою розуміння TPSP-постачальником особливостей діяльності та бізнес-процесів банку, пов'язаних із послугами, що надаватимуться таким постачальником.

Така інформація може включати політику банку, вимоги внутрішньобанківських документів до ділової репутації критичного TPSP-

постачальника, його кінцевих бенефіціарних власників і керівників, інформацію про процеси, технології та обладнання банку.

290<sup>54</sup>. Банк після укладення договору з TPSP-постачальником з метою прийняття своєчасних та адекватних управлінських рішень щодо пом'якшення ризику третіх сторін і зменшення пов'язаних із таким ризиком втрат (збитків) здійснює:

1) на постійній основі моніторинг:  
дотримання вимог пункту 290<sup>15</sup> глави 45<sup>2</sup> розділу VI цього Положення;  
відсутності ознак небездоганної ділової репутації критичного TPSP-постачальника, його кінцевих бенефіціарних власників та керівників, визначених у пункті 65 глави 6 розділу II, пункті 69 глави 7 розділу II Положення № 149, та інших ознак, установлених у внутрішньобанківських документах щодо управління ризиком третіх сторін;  
можливості отримання послуг від іншого альтернативного TPSP-постачальника;  
оцінки критичності послуг, що надаються TPSP-постачальником;

2) не рідше одного разу на рік моніторинг:  
відповідності критичного TPSP-постачальника критеріям операційної та фінансової спроможності, визначеним у пунктах 290<sup>40</sup>, 290<sup>41</sup> глави 45<sup>5</sup> розділу VI цього Положення;  
відповідності укладеного договору умовам, визначеним у пунктах 290<sup>49</sup>, 290<sup>50</sup> глави 45<sup>6</sup> розділу VI цього Положення, та дотримання TPSP-постачальником / критичним TPSP-постачальником таких умов під час виконання договору.

290<sup>55</sup>. Банк під час здійснення моніторингу виконання критичним TPSP-постачальником умов договору та його діяльності:

1) перевіряє наявність у критичного TPSP-постачальника процедур внутрішнього контролю та оцінює його спроможність виконувати договірні зобов'язання;

2) здійснює моніторинг системи внутрішнього контролю критичного TPSP-постачальника, якщо укладений з таким TPSP-постачальником договір передбачає розподіл відповідальності за надання банку послуг з іншими TPSP-постачальниками, ключовими п-ми сторонами;

3) розробляє заходи реагування на проблеми, пов'язані з неналежним виконанням критичним TPSP-постачальником умов договору;

4) здійснює аналіз відповідності діяльності критичного TPSP-постачальника політиці управління безперервною діяльністю банку;

5) здійснює моніторинг інцидентів у діяльності критичного TPSP-постачальника;

6) здійснює аналіз розроблених критичним TPSP-постачальником заходів реагування на такі інциденти та результати усунення їх наслідків;

7) здійснює моніторинг переліку ключових п-х сторін критичного TPSP-постачальника, які мають опосередкований вплив на підтримання / надання критичної послуги TPSP-постачальником банку;

8) здійснює оцінку діяльності критичного TPSP-постачальника, включаючи аналіз планових та фактичних показників діяльності, які є релевантними для врахування під час оцінки ризику третіх сторін;

9) перевіряє відповідність умов договору вимогам законодавства України та країни, з території якої надаватиметься відповідна послуга TPSP-постачальником.

290<sup>56</sup>. Моніторинг виконання TPSP-постачальником умов договору повинен узгоджуватися із:

1) системою управління ризиками банку;

2) ризиками, які були оцінені та враховані банком під час укладення договору з TPSP-постачальником;

3) новими ризиками, які виникли після укладення договору з TPSP-постачальником;

4) зобов'язаннями TPSP-постачальника згідно з укладеним з банком договором;

5) рівнем залежності критичного TPSP-постачальника від ключових п-х сторін під час надання послуг банку.

290<sup>57</sup>. Банк здійснює моніторинг виконання TPSP-постачальником умов договору, оцінку стану виконання умов договору, перегляд умов договору (за потреби) на регулярній основі, але не рідше одного разу на рік та в разі значних змін:

1) у внутрішньому операційному середовищі банку, включаючи організаційні зміни, наявність конфлікту інтересів;

2) у внутрішньому операційному середовищі критичного TPSP-постачальника, включаючи організаційні зміни, зміни місця (регіону, країни), з якого надаються послуги, упровадження нових технологій;

3) у зовнішньому середовищі, включаючи політичну, економічну, соціальну, правову та фінансову сфери, перешкоди щодо здійснення діяльності банком та критичним TPSP-постачальником.

290<sup>58</sup>. Банк у разі встановлення за результатами моніторингу невідповідності TPSP-постачальника вимогам пункту 290<sup>15</sup> глави 45<sup>2</sup> розділу VI цього Положення приймає рішення про припинення у найкоротший строк договірних відносин із таким TPSP-постачальником.

290<sup>59</sup>. Банк у разі встановлення за результатами моніторингу щодо критичного TPSP-постачальника ознак небездоганної ділової репутації, установлених у пункті 65 глави 6, пункті 69 глави 7 розділу II Положення № 149, та інших ознак небездоганної ділової репутації, установлених у внутрішньобанківських документах щодо управління ризиком третіх сторін, та/або невідповідності критеріям операційної та фінансової спроможності, визначеним у пунктах 290<sup>40</sup>, 290<sup>41</sup> глави 45<sup>5</sup> розділу VI цього Положення, та/або невідповідності укладених договорів умовам, визначеним у пунктах 290<sup>49</sup>, 290<sup>50</sup> глави 45<sup>6</sup> розділу VI цього Положення, та/або порушення критичним TPSP-постачальником таких умов під час виконання договору приймає одне з таких рішень про:

1) продовження договірних відносин із таким TPSP-постачальником;

2) розроблення плану поетапного скорочення обсягу отримуваних послуг від такого TPSP-постачальника та припинення договірних відносин із ним. Такий план повинен затверджуватися радою банку.

290<sup>60</sup>. Банк із дня встановлення за результатами моніторингу фактів, визначених в абзаці першому пункту 290<sup>59</sup> глави 45<sup>6</sup> розділу VI цього Положення, до дня їх виправлення (усунення) / припинення договірних відносин із критичним TPSP-постачальником:

1) визначає рівень ризику третіх сторін за договором із таким TPSP-постачальником як високий;

2) ураховує такий ризик під час здійснення стрес-тестування ризику третіх сторін за базовим сценарієм;

3) здійснює оцінку потенційного впливу повного припинення надання таким TPSP-постачальником послуг банку на безперервність діяльності та профіль ризику банку.

290<sup>61</sup>. Банк у разі встановлення фактів, що можуть свідчити про підвищення ризику концентрації послуг критичних TPSP-постачальників та ключових п-х сторін, збільшує частоту (періодичність) здійснення моніторингу виконання TPSP-постачальниками умов договорів.

290<sup>62</sup>. Банк для отримання впевненості у відповідності послуг, що надаються TPSP-постачальником, умовам договору має право враховувати результати зовнішніх перевірок діяльності TPSP-постачальника.

Банк для отримання впевненості у відповідності послуг, що надаються критичним TPSP-постачальником, умовам договору враховує результати перевірок (за наявності) критичного TPSP-постачальника зовнішнім аудитором або іншим незалежним суб'єктом, який проводить незалежну професійну діяльність, а також відповідність критичного TPSP-постачальника вимогам національних стандартів України (ДСТУ), міжнародних стандартів (ISO) за відповідними напрямками діяльності критичного TPSP-постачальника, підтверджену діючими станом на дату здійснення аналізу сертифікатами.

290<sup>63</sup>. Банк під час прийняття рішення про продовження / поновлення / припинення дії договору з TPSP-постачальником ураховує інформацію про виконання TPSP-постачальником умов попереднього договору.

#### 45<sup>8</sup>. Припинення договірних відносин з TPSP-постачальником

290<sup>64</sup>. Банк здійснює управління процесом припинення договірних відносин з TPSP-постачальником з урахуванням:

- 1) закінчення строку дії договору з TPSP-постачальником;
- 2) наявних фактів порушення умов договору TPSP-постачальником;
- 3) наявних фактів невиконання / порушення TPSP-постачальником вимог законодавства України;
- 4) наміру банку замінити TPSP-постачальника на альтернативного TPSP-постачальника;

5) наміру банку виконувати роботи самостійно за послугами, що надаються TPSP-постачальником, використовуючи власну інфраструктуру;

6) припинення банком здійснення діяльності, для якої залучався TPSP-постачальник;

7) установлення ознак небездоганної ділової репутації критичного TPSP-постачальника, його кінцевих бенефіціарних власників та керівників;

8) установлення невідповідності операційної та фінансової спроможності критичного TPSP-постачальника.

Банк у межах припинення договірних відносин із критичним TPSP-постачальником уживає заходів для забезпечення безперервності своєї діяльності.

290<sup>65</sup>. Банк щодо кожного критичного TPSP-постачальника розробляє та періодично (не рідше одного разу на рік) оновлює:

1) план очікуваного (запланованого) припинення отримання критичної послуги від критичного TPSP-постачальника;

2) оперативний план неочікуваного (незапланованого) припинення отримання критичної послуги від критичного TPSP-постачальника.

290<sup>66</sup>. План очікуваного (запланованого) припинення отримання критичної послуги від критичного TPSP-постачальника повинен урахувати:

1) можливість заміни критичного TPSP-постачальника, який надає банку критичну послугу;

2) наявні можливості / ресурси в банку для припинення отримання критичної послуги від критичного TPSP-постачальника, включаючи наявність та доступність фінансових ресурсів (бюджету) і технічної інфраструктури.

290<sup>67</sup>. План очікуваного (запланованого) припинення отримання критичної послуги від критичного TPSP-постачальника повинен визначати:

1) часовий проміжок для повного припинення отримання послуг і поетапний графік такого припинення;

2) заходи, спрямовані на забезпечення дотримання прав, визначених у договорі з критичним TPSP-постачальником, включаючи збереження та

доступність результатів перевірок, обробки конфіденційних даних, архівування, збереження або знищення даних, відкликання доступу до систем;

3) розподіл обов'язків і повноважень щодо управління виходом з відносин із критичним TPSP-постачальником;

4) процеси для своєчасного передавання до банку / нового TPSP-постачальника логічних активів у відповідному форматі, фізичних активів і персоналу (консультантів, працівників за контрактом);

5) заходи, необхідні для забезпечення узгодженості у взаємодії між підрозділами банку [включаючи підрозділ з управління персоналом, юридичний підрозділ, підрозділ контролю за дотриманням норм (комплаєнс), підрозділ інформаційних технологій] та зовнішніми зацікавленими сторонами, включаючи нового критичного TPSP-постачальника (за наявності).

290<sup>68</sup>. Оперативний план неочікуваного (незапланованого) припинення отримання критичної послуги від критичного TPSP-постачальника повинен урахувати залучення такого TPSP-постачальника до надання критичних послуг та заміність таких послуг.

Оперативний план неочікуваного (незапланованого) припинення отримання критичної послуги від критичного TPSP-постачальника повинен ґрунтуватися на реалістичних сценаріях та обґрунтованих припущеннях.

290<sup>69</sup>. Оперативний план неочікуваного (незапланованого) припинення отримання критичної послуги від критичного TPSP-постачальника повинен містити:

1) часовий проміжок для повного припинення отримання послуг і поетапний графік такого припинення;

2) процеси для своєчасного передавання до банку / нового критичного TPSP-постачальника логічних активів у відповідному форматі, фізичних активів і персоналу (консультантів, працівників за контрактом);

3) затверджену та актуалізовану інформацію про працівників банку, які повинні мати відповідні повноваження, достатню кваліфікацію та навички у здійсненні діяльності з управління кризовими ситуаціями, та є відповідальними за моніторинг та ескалацію інформації щодо критичного TPSP-постачальника;

4) процес оперативного затвердження бюджету / використання резервного фонду для покриття неочікуваних додаткових витрат, пов'язаних із виходом з відносин із критичним TPSP-постачальником, включаючи залучення зовнішніх

працівників і консультантів, необхідних для переходу на інші послуги, залучення альтернативного критичного TPSP-постачальника.”;

4) главу 47 після пункту 299<sup>1</sup> доповнити новим пунктом 299<sup>2</sup> такого змісту:  
 “299<sup>2</sup>. Банк забезпечує узгодженість внутрішньобанківських документів щодо аутсорсингу з політикою залучення TPSP-постачальників і політикою, порядками та процедурами управління ризиком третіх сторін.”;

5) у главі 48:

пункт 301 доповнити новим підпунктом такого змісту:

“5) принципи та підходи банку щодо забезпечення безперервної діяльності в разі збоїв / переривання у наданні послуг TPSP-постачальниками.”;

у пункті 302:

у підпункті 1 слова “recovery time objective” замінити літерами “RTO”;

у підпункті 2 слова “recovery point objective” замінити літерами “RPO”;

главу після пункту 302 доповнити двома новими пунктами 302<sup>1</sup>, 302<sup>2</sup> такого змісту:

“302<sup>1</sup>. Банк під час управління безперервною діяльністю забезпечує:

1) періодичний перегляд та оновлення плану забезпечення безперервної діяльності з урахуванням укладених договорів із TPSP-постачальниками;

2) періодичне тестування плану забезпечення безперервної діяльності, розглядаючи різні заходи відновлення діяльності для критичних процесів банку або запровадження додаткового контролю, що забезпечує дотримання ризик-апетиту та рівня толерантності до збоїв, із застосуванням таких сценаріїв:

залучення іншого / альтернативного TPSP-постачальника;

використання одночасно кількох TPSP-постачальників;

виконання банком робіт самостійно за послугами, що надаються TPSP-постачальником, використовуючи власну інфраструктуру;

3) ураховувати наслідки інцидентів, що мали місце в минулому за договорами з TPSP-постачальниками, та результати періодичного тестування банком плану забезпечення безперервної діяльності;

4) здійснювати періодичну актуалізацію переліку визначених альтернативних TPSP-постачальників.

302<sup>2</sup>. Банк під час управління безперервністю діяльності додатково до вимог, визначених у пункті 302<sup>1</sup> глави 48 розділу VI цього Положення, щодо критичних договорів із TPSP-постачальниками, здійснює:

1) отримання від TPSP-постачальника підтвердження, що він розробляє, періодично переглядає та оновлює план забезпечення безперервної своєї діяльності, в якому встановлено чіткі та вимірювані показники, що узгоджуються з толерантністю банку до збоїв, включаючи (RTO) та (RPO);

2) перевірку надійності процесів забезпечення безперервності діяльності TPSP-постачальника.”;

пункт 303 доповнити новим підпунктом такого змісту:

“б) заходи, спрямовані на забезпечення безперервності надання послуг критичними TPSP-постачальниками послуг банку, якщо немає альтернативних TPSP-постачальників для надання таких послуг.”;

главу після пункту 303 доповнити новим пунктом 303<sup>1</sup> такого змісту:

“303<sup>1</sup>. Банк розробляє та тестує план забезпечення безперервної діяльності із залученням критичних TPSP-постачальників або із залученням незалежних сторін або здійснює симуляцію залучення критичних TPSP-постачальників (якщо немає змоги їх залучити).”;

б) у главі 50:

пункт 314 викласти в такій редакції:

“314. Головний ризик-менеджер / підрозділ з управління ризиками не пізніше наступного робочого дня після виявлення ризику інформує раду банку, комітет з управління ризиками (у разі його створення), правління банку, комітет з управління операційним ризиком (у разі його створення) про:

1) значне підвищення операційних ризиків з метою прийняття своєчасних та адекватних управлінських рішень;

2) установлення за результатами моніторингу виконання TPSP-постачальником умов договору та його діяльності ознак підвищеного ризику в співпраці з TPSP-постачальником, включаючи суттєве погіршення показників діяльності критичного TPSP-постачальника, порушення безпеки, втрати даних, інциденти / збої / переривання в наданні послуг, факти, що можуть вплинути на належне виконання TPSP-постачальником умов договору, інші ознаки підвищеного ризику, установлення ознак небездоганної ділової репутації критичного TPSP-постачальника, його кінцевих бенефіціарних власників та керівників.”.

3. У додатках до Положення:

1) таблицю додатка 2 після рядка 5 доповнити новим рядком 6 такого змісту:

“

1	2	3	4	5	6	7
6	Політика залучення TPSP-постачальників	Затверджує	Бере участь у розробленні	Забезпечує розроблення	Бере участь у розробленні	Бере участь у розробленні

”

У зв'язку з цим рядки 6–26 уважати відповідно рядками 7–27;

2) Положення після додатка 6 доповнити новим додатком 7, виклавши його в такій редакції:

“Додаток 7  
до Положення про організацію системи управління ризиками в банках України та банківських групах (пункт 290<sup>13</sup> глави 45<sup>2</sup> розділу VI)

Дані,

які вносяться до переліку договорів, укладених з TPSP-постачальниками, включаючи угоди про рівень сервісу / обслуговування (SLA)

Таблиця

№ з/п	Дата укладення договору	Дата початку дії договору	Дата закінчення строку дії договору	Найменування TPSP-постачальника	Код TPSP-постачальника	Критичність договору
1	2	3	4	5	6	7

Продовження таблиці

Короткий опис послуг, які надаються TPSP-постачальником	Замінність послуг, які надаються TPSP-постачальником	Перелік альтернативних TPSP-постачальників	Дані про обмін інформацією з TPSP-постачальником	Місце (регіон, країна), з якого надаються послуги TPSP-постачальником
8	9	10	11	12

Продовження додатка 7  
Продовження таблиці

Місцезнаходження (регіон, країна) центрів обробки та збереження даних TPSP-постачальника	Перелік n-х сторін за договором з TPSP-постачальником	Перелік ключових n-х сторін	Дата внесення змін до договору з TPSP-постачальником	Короткий опис змін, унесених до договору з TPSP-постачальником
13	14	15	16	17

Продовження таблиці

Дата набуття TPSP-постачальником статусу критичного TPSP-постачальника	Дата виключення TPSP-постачальника зі статусу критичного TPSP-постачальника	Результати перевірки наявності / відсутності ознак небездоганної ділової репутації критичного TPSP-постачальника, його кінцевих бенефіціарних власників та керівників	Результати аналізу операційної та фінансової спроможності критичного TPSP-постачальника
18	19	20	21

1. Пояснення щодо заповнення таблиці:

1) у колонці 6 зазначається код за даними з Єдиного державного реєстру юридичних осіб, фізичних осіб-підприємців та громадських формувань (для TPSP-постачальника, який є резидентом України) або ідентифікаційний / реєстраційний номер / код офіційного документа, виданого уповноваженим органом іноземної країни, що підтверджує реєстрацію TPSP-постачальника в країні, у якій зареєстровано її головний офіс (для TPSP-постачальника, який є нерезидентом України);

2) у колонці 7 зазначається “критичний” / “некритичний”;

3) у колонці 10 зазначається перелік найменувань альтернативних TPSP-постачальників, які визначені банком;

4) у колонці 11 зазначається про обмін з TPSP-постачальником інформацією, публічне розкриття якої матиме суттєвий негативний вплив на конкурентну ринкову позицію банку та/або його клієнтів / контрагентів на ринку;

5) у колонці 14 зазначається перелік n-х сторін, які є другими та третіми сторонами (третьою стороною в ланцюгу постачання є постачальник послуг для другої сторони в ланцюгу постачання; другою стороною – є постачальник послуг для TPSP-постачальника).”.

У зв'язку з цим додатки 7–10 уважати відповідно додатками 8–11.

4. У тексті Положення посилання на додатки 7–10 замінити посиланнями відповідно на додатки 8–11.