

Кваліфікаційні вимоги до учасника

Колекторська компанія, яка має намір співпрацювати з банком щодо повернення проблемної заборгованості, повинна:

1. мати у своєму складі операторів, які безпосередньо задіяні в процесі стягнення заборгованості у кількості не менше 25 осіб та співробітників, що здійснюють візити/виїзди (якщо послуга передбачає візити/виїзди);
2. мати у своєму складі працівників, які мають досвід роботи із заборгованістю в досудовому порядку не менше 6 місяців на дату подання кваліфікаційної пропозиції;
3. мати досвід роботи на ринку послуг по стягненню проблемної заборгованості з укладанням аналогічних договорів з банками за останні 3 роки;
4. мати власний контакт центр потужністю не менше 20 робочих місць;
5. мати автоматизовані системи управління НПА (CRM, система автоматичного дозвону, збереження запису переговорів з боржниками з терміном зберігання не менше 3-х років, збереження історії дій тощо);
6. бути зареєстрованим в реєстрі колекторських компаній НБУ;
7. мати бездоганну ділову репутацію;
8. забезпечити безперервне живлення та інтернету на робочих місцях у колл-центрах в умовах відсутності централізованого електропостачання (блекауту).

Перелік необхідних документів

Колекторські компанії, які мають намір співпрацювати з банком щодо повернення проблемної заборгованості, повинні надіслати заповнену кваліфікаційну заявку в електронному вигляді (див. форму XLS), обов'язковий пакет документів для акредитації та інформацію про учасника до початку кваліфікаційного добору:

1. Інформація про учасника згідно Додатку 1;
2. копія діючого статуту аутсорсера;
3. копія свідоцтва про реєстрацію платника податків;
4. копія Витягу з ЄДРПОУ (дата витягу, на момент пред'явлення, не повинна перевищувати 10 днів з моменту отримання);
5. копія ліцензії (якщо є в наявності);
6. рекомендації партнерів (якщо є в наявності);
7. комерційні пропозиції у вигляді тарифної сітки;

Строк прострочення в днях на дату здійснення оплати боржником	Винагорода, %
0–30	
31–60	
61–90	
91–180	
181–360	
361–720	
721-1080	

8. копія звіту про баланс (Форма №1) та фінансові результати (Форма №2) за останній звітний рік;
9. оригінал довідки з обслуговуючого банку про відсутність (наявність) заборгованості за кредитами, дійсної на дату подання кваліфікаційної пропозиції;
10. довідка щодо кількості працівників, задіяних у процесі стягнення заборгованості у форматі: ПІБ працівника, штат /або за цивільно-правова угода, стаж роботи у складі аутсорсера, освіта, спеціалізація/посада працівника;
11. довідка щодо досвіду роботи та виконання аналогічних договорів учасника у форматі: дата договору, назва контрагента за договором, предмет договору, сума заборгованості, сума повернутої заборгованості, перелік основних клієнтів, типів кредитних продуктів, інструментів по стягненню заборгованості, тощо;
12. довідка з описом контакт центру, включаючи: кількість робочих місць; тип обладнання; наявність системи автоматичного дозвону; наявність системи запису переговорів; фотографії контакт центру; адресу знаходження;
13. довідка з описом інформаційної системи, включаючи: можливості автоматизації процесу стягнення заборгованості та зберігання інформації про боржників, системи безпеки та захисту конфіденційної інформації, резервне копіювання, тощо;
14. опитувальник щодо відповідності вимогам захисту персональних даних (Додаток 2);
15. письмове запевнення про відповідність колекторської компанії та її діяльності з врегулювання простроченої заборгованості встановленим законодавством України вимогам щодо взаємодії із споживачами фінансових послуг та іншими особами (вимогам щодо етичної поведінки);
16. порядок розгляду аутсорсером звернень споживачів фінансових послуг;
17. порядок організації та проведення навчання і підвищення кваліфікації працівників аутсорсера та осіб, залучених до здійснення колекторської діяльності;
18. порядок взаємодії із споживачами фінансових послуг при врегулюванні простроченої заборгованості (вимоги щодо етичної поведінки);
19. анкету про відсутність зв'язку контрагента з працівником Банку, його близькою особою або пов'язаними з ними юридичними особами згідно Додатку 3.
20. опитувальник щодо системи внутрішнього контролю та системи управління операційними ризиками згідно Додатку 4.
21. опитувальник з інформаційної безпеки, згідно Додатку 5.

Інформація про учасника

№	Питання	Відповідь
Розділ 1. Загальна інформація про учасника:		
1.1	Повне та скорочене найменування	
1.2	Дата реєстрації	
1.3	Є клієнтом АТ КБ "ПриватБанк" (так/ні)	
1.4	Банківські реквізити (обов'язкова вимога - відкритий рахунок учасника в АТ КБ "ПриватБанк")	
1.5	Ідентифікаційний код за ЄДРПОУ	
1.6	ІПН (Індивідуальний податковий номер)	
1.7	Чи є керівником або власником істотної участі*, у т.ч. опосередковано, юридичної особи фізична особа, яка є працівником або керівником Банку та/або його близькою особою** ?	(якщо відповідь «так» необхідно вказати Прізвище, Ім'я та по-батькові такої особи та родинний зв'язок в разі наявності)
1.8	Чи бере участь юридична особа в якості відповідача у будь-якому цивільному, адміністративному, господарському чи кримінальному провадженні, в тому числі на стадії досудового провадження або слідства?	
Розділ 2. Інформація про керівників учасника:		
2.1	Ідентифікаційні дані керівника або особи, на яку покладено функції з керівництва та управління господарською діяльністю (прізвище, ім'я та по-батькові (за наявності), реєстраційний номер облікової картки платника податків, в разі відмови від РНОКПП вказати паспортні дані)	
2.2	Ідентифікаційні дані представника юридичної особи (за наявності) (прізвище, ім'я та по-батькові (за наявності), реєстраційний номер облікової картки платника податків, в разі відмови від РНОКПП вказати паспортні дані)	
Розділ 3. Інформація про власників учасника:		
3.1	Дані про фізичних осіб, які є кінцевими бенефіціарними власниками (контролерами)*** (прізвище, ім'я та по-батькові (за наявності), реєстраційний номер облікової картки платника податків, в разі відмови від РНОКПП вказати паспортні дані)	

3.2	Інформація про материнську компанію, корпорацію, холдингову групу, промислово-фінансову групу або інше об'єднання, членом якого є юридична особа (повне та скорочене найменування (якщо нерезидент - англійською мовою), ідентифікаційний код за ЄДРПОУ; якщо нерезидент - країна реєстрації, орган реєстрації, реквізити свідоцтва про реєстрацію або витягу з банківського, торговельного чи судового реєстру)	(Скорочене найменування; Ідентифікаційний код за ЄДРПОУ)
Розділ 4. Контактна інформація про учасника:		
4.1	Фактична адреса	
4.2	Адреса місцезнаходження	
4.3	Телефон, Факс, E-mail, Веб-сайт	
Розділ 5. Кваліфікаційні відомості про учасника:		
5.1. Soft Collection:		
5.1.1	Розташування (колл-центру, операційного блоку)	
5.1.2	Розмір колл-центру: кількість місць та кількість операторів	
5.2. Hard Collection:		
5.2.1	Кількість співробітників, що здійснюють візити	
5.2.2	Регіони України, в яких присутні співробітники, які здійснюють візити	
5.3.	Максимальний об'єм кредитних справ, який здані відпрацювати за одну передачу (шт.)	
5.3. Дистанційні канали відпрацювання		
5.3.1	Листи(паперові)	
5.3.2	SMS	
5.3.3	IVR / IVM / IVO	
5.3.4	Email	
5.3.5	Інше(вказати, які ще канали дистанційної комунікації використовуються)	

Примітка:

Учасник гарантує достовірність наданих даних.

АТ КБ "ПриватБанк" має право на перевірку всіх даних, наведених в Таблиці.

Керівник _____ Підпис, м.п. П.І.Б.

* - істотна участь – пряме та/або опосередковане володіння однією особою самостійно чи спільно з іншими особами 10 і більше відсотками статутного капіталу та/або права голосу акцій, паїв юридичної особи або незалежна від формального володіння можливість значного впливу на управління чи діяльність юридичної особи. Особа визнається власником опосередкованої істотної участі незалежно від того, чи здійснює така особа контроль прямого власника участі в юридичній особі або контроль будь-якої іншої особи в ланцюгу володіння корпоративними правами такої юридичної особи;

** - близька особа - це:

– члени сім'ї працівника/керівника Банку:

а) особа, яка перебуває у шлюбі із працівником/керівником та діти працівника/керівника до досягнення ними повноліття - незалежно від спільного проживання із

працівником/керівником;

б) будь-які особи, які спільно проживають, пов'язані спільним побутом, мають взаємні права та обов'язки із працівником/керівником (крім осіб, взаємні права та обов'язки яких не мають характеру сімейних), у тому числі особи, які спільно проживають, але не перебувають у шлюбі

та

- чоловік, дружина, батько, мати, вітчим, мачуха, син, дочка, пасинок, падчерка, рідний та двоюрідний брати, рідна та двоюрідна сестри, рідний брат та сестра дружини (чоловіка), племінник, племінниця, рідний дядько, рідна тітка, дід, баба, прадід, прабаба, внук, внучка, правнук, правнучка, зять, невістка, тесть, теща, свекор, свекруха, батько та мати дружини (чоловіка) сина (дочки), усиновлювач чи усиновлений, опікун чи піклувальник, особа, яка перебуває під опікою або піклуванням зазначеного суб'єкта;

МІНІМАЛЬНИЙ ПЕРЕЛІК
запитань для проведення попереднього оцінювання постачальника послуг щодо
відповідності вимогам захисту персональних даних

Питання	Відповідь	Коментарі та посилання на документацію
1. Діяльність компанії щодо захисту персональних даних підпадає під регулювання Європейського Регламенту про захист персональних даних (EU GDPR), законодавство Великобританії про захист даних (UK GDPR) чи інший акт у сфері захисту	● Ні ● Так	
2. Компанія розуміє, що персональні дані, отримані від Банку, можуть використовуватися виключно в цілях, які визначені володільцем персональних даних.	● Ні ● Так	
3. Персонал компанії розуміє, що таке персональні дані та має можливість виокремити персональні дані з інформації, якою володіє або користується.	● Ні ● Наразі ні, заплановано ● Так, частково ● Так, повністю	
4. Компанія має затверджену й опубліковану політику по захисту персональних даних, яка регулярно переглядається, або така політика охоплюється політикою інформаційної безпеки.	● Ні ● Наразі ні, заплановано ● Так, частково ● Так, повністю	
5. Компанія має визначений підрозділ або посадову особу, відповідальну за захист персональних даних.	● Ні ● Наразі ні, заплановано ● Так, частково ● Так, повністю	
6. Захист персональних даних враховується при прийнятті бізнесових рішень менеджментом компанії.	● Ні ● Наразі ні, заплановано ● Так, частково ● Так, повністю	
7. Компанія має можливість своєчасно дізнатися та контролювати передачу	● Ні ● Наразі ні, заплановано ● Так, частково	

персональних даних, якими володіє, до третіх осіб.	• Так, повністю	
8. Компанія має можливість своєчасно дізнатися та повідомити Банк про можливий витік персональних даних, неавторизоване їх розголошення або інше порушення безпеки даних	• Ні • Наразі ні, заплановано • Так, частково • Так, повністю	
9. Компанія має можливість невідкладно повідомити Банк про звернення суб'єктів персональних даних щодо обробки їх персональних даних.	• Ні • Наразі ні, заплановано • Так, частково • Так, повністю	
10. Компанія має можливість контролювати мету використання персональних даних, отриманих від Банку та їх обробку виключно в тому порядку, який визначений Банком.	• Ні • Наразі ні, заплановано • Так, частково • Так, повністю	
11. Компанія має можливість виявити, повернути та видалити всі персональні дані, отримані від Банку після закінчення правовідносин.	• Ні • Наразі ні, заплановано • Так, частково • Так, повністю	

Анкета про відсутність зв'язку контрагента з працівником Банку, його близькою особою або пов'язаними з ними юридичними особами

1 Повне та скорочене найменування (у разі наявності)

Повне найменування: _____

Скорочене найменування: _____

2 Ідентифікаційний код за ЄДРПОУ/РНОКПП: _____

3 Юридична адреса: _____

4 Фактична адреса _____

5 Номери контактних телефонів/факсів _____

6 Адреса електронної пошти _____

7 Чи є керівником або власником істотної участі*, у т.ч. опосередковано, юридичної особи фізична особа, яка є працівником або керівником Банку та/або його близькою особою** ?

____ (якщо відповідь "так" вказати ППП керівника або працівника Банку, родинний зв'язок)

Дата заповнення анкети " ____ " _____ 20__ Підпис _____ /
_____ (ППП)

* - істотна участь – пряме та/або опосередковане володіння однією особою самостійно чи спільно з іншими особами 10 і більше відсотками статутного капіталу та/або права голосу акцій, паїв юридичної особи або незалежна від формального володіння можливість значного впливу на управління чи діяльність юридичної особи. Особа визнається власником опосередкованої істотної участі незалежно від того, чи здійснює така особа контроль прямого власника участі в юридичній особі або контроль будь-якої іншої особи в ланцюгу володіння корпоративними правами такої юридичної особи; ** - близька особа - це: – члени сім'ї працівника/керівника Банку: а) особа, яка перебуває у шлюбі із працівником/керівником та діти працівника/керівника до досягнення ними повноліття - незалежно від спільного проживання із працівником/керівником; б) будь-які особи, які спільно проживають, пов'язані спільним побутом, мають взаємні права та обов'язки із працівником/керівником (крім осіб, взаємні права та обов'язки яких не мають характеру сімейних), у тому числі особи, які спільно проживають, але не перебувають у шлюбі та чоловік, дружина, батько, мати, вітчим, мачуха, син, дочка, пасинок, падчерка, рідний та двоюрідний брати, рідна та двоюрідна сестри, рідний брат та сестра дружини (чоловіка), племінник, племінниця, рідний дядько, рідна тітка, дід, баба, прадід, прабаба, внук, внучка, правнук, правнучка, зять, невістка, тесть, теща, свекор, свекруха, батько та мати дружини (чоловіка) сина (дочки), усиновлювач чи усиновлений, опікун чи піклувальник, особа, яка перебуває під опікою або піклуванням зазначеного суб'єкта;

Опитувальник щодо системи внутрішнього контролю та системи управління операційними ризиками

Питання	Відповідь	Коментарі
Чи наявна ефективна система управління операційним ризиком та/або внутрішнього контролю? Які заходи вживаються для забезпечення її/їх ефективності? (Елементи СВК та Управління ризиками: 1. Наявність ВНД з СВК та Управління Ризиками 2. Наявність підрозділу управління ризиками 3. Наявність процесу управління інцидентами (ідентифікація, реєстрація, усунення, запобіжні заходи) 4. Процес оцінки ризиків)		
Чи наявна ефективна система запобігання внутрішньому шахрайству? Які заходи вживаються для забезпечення її ефективності?		
Як компанія забезпечує ефективну протидію зовнішньому шахрайству при наданні послуг Банку? Які заходи вживаються для забезпечення її ефективності?		
Чи наявна система фіксації та аналізу інцидентів, що пов'язані з наданням послуг? Які заходи вживаються для забезпечення її ефективності? Як компанія повідомлятиме Банк про інциденти, що пов'язані з наданням послуг Банку?		
Чи були у 3-ї сторони в минулому інциденти, які призвели до негативних наслідків для вашого бізнесу та/або клієнтів та/або мали розголос в ЗМІ? Якщо так, будь ласка, надайте пояснення цих інцидентів та/або посилання на них Чи були у вас у минулому інциденти, які могли поставити під загрозу безпеку ваших клієнтів або вашого бізнесу? Якщо так, будь ласка, надайте пояснення цих інцидентів та/або посилання на них		
Чи наявна ефективна система забезпечення неперервності діяльності (ВСР) та/або Політика ВСР? Які заходи вживаються для забезпечення її ефективності?		
Чи існує план безперервності бізнесу (ВСР) для процесів, що надаються Банку третьою стороною? Хто відповідає за розробку та впровадження ВСР? Як часто переглядається та оновлюється плани ВСР?		

Чи існує план реагування на надзвичайні (crisis management) ситуації для процесів, що надаються третьою стороною? Хто відповідає за розробку та впровадження плану реагування на надзвичайні ситуації? Як часто план реагування на надзвичайні ситуації переглядається та оновлюється? Які заходи вживаються для забезпечення їх ефективності?		
Чи має компанія достатні резервні ресурси для забезпечення неперервності діяльності? Які заходи вживаються для забезпечення цього?		
Яким чином забезпечується ефективний контроль якості послуг, що надаються? Які заходи вживаються для забезпечення цього?		
Чи проводився в компанії незалежний аудит / ІТ-аудит за останні 12 місяців? Які результати аудиту?		
Чи має компанія достатню кількість кваліфікованих співробітників для виконання послуг для Банку? Чи існують альтернативні робочі місця для персоналу, який виконує процеси, що надаються Банку? Які заходи вживаються для забезпечення цього? Чи планує компанія залучати зовнішніх постачальників послуг? Які фактори враховуються при прийнятті цього рішення?		
Чи були ідентифіковані ризики для процесів, що надаються третьою стороною? Якщо так, то які? Які заходи вживаються для управління цими ризиками?		
Як часто відбуваються/можуть відбуватися значні зміни у діяльності Зі сторони щодо послуг, які надаються Банку? Як Банк дізнаватиметься про них? Як буде здійснюватися комунікація між Банком та третьою стороною в разі проведення значної зміни?		

Опитувальник з питань інформаційної безпеки

Назва компанії: _____		
Реєстраційний код компанії (код ЄДРПОУ/РНОКПП): _____		
Дата заповнення: _____		
ПІБ, посада: _____		
(відповідальна особа за заповнення опитувальника)		
Розділ	Питання	Відповідь/коментар/ підтверджуючі документи
Загальні питання щодо взаємодії постачальника з Банком	Опишіть характер послуг та специфіку взаємодії постачальника з Банком	<i>Вкажіть суть послуг (наприклад: розробка ПЗ, постачання ліцензій, надання хмарних сервісів (SaaS/IaaS/PaaS), технічна підтримка, аутсорсинг, консалтинг тощо). Зазначте, які саме продукти чи сервіси постачаються</i>
	Яким каналом/способом здійснюється взаємодія постачальника з Банком?	<i>Наприклад, веб-портали/SaaS: доступ працівників Банку до хмарного ресурсу постачальника через браузер (наприклад, для управління ліцензіями, кабінет клієнта, аналітична платформа). Інтеграційна взаємодія (API): автоматизований обмін даними між системами Банку та постачальника через захищені протоколи. Захищені канали зв'язку (VPN): створення шифрованого тунелю для віддаленого доступу фахівців постачальника до систем Банку або навпаки. Обмін файлами (SFTP): завантаження або отримання звітів/даних через захищені сервери передачі файлів. Електронна пошта: взаємодія виключно через e-mail Віддалений робочий стіл: використання інструментів віддаленого керування для надання технічної підтримки. Або опишіть свій варіант.</i>

1.Управління інформаційною безпекою	Чи передбачає надання послуг постачальником доступ, обробку, передачу або зберігання інформації Банку на стороні постачальника?	<i>Якщо «так», вкажіть вид інформації (наприклад: банківська таємниця, конфіденційна інформація, персональні дані клієнтів/працівників, комерційна таємниця, таємниця страхування)</i>
	Чи наявний в організації постачальника підрозділ інформаційної безпеки та працівники і процеси, які відповідають за ризики інформаційної безпеки/кіберризиків?	<i>"Якщо "так", опишіть, будь ласка, більш детально. При можливості, вкажіть, будь ласка, контактний e-mail та посаду працівників"</i>
	Чи наявні затверджені політика/план з інформаційної безпеки, які регулярно переглядаються?	<i>Якщо "так", опишіть, будь ласка, більш детально</i>
	Чи запроваджено та з якою регулярністю проводиться навчання персоналу вимогам інформаційної безпеки, включаючи поширені атаки на працівників?	<i>Наприклад, такі як фішинг та інші способи спонукання працівників розкрити конфіденційну інформацію або завантажити неавторизований код?</i>
2. Управління інцидентами інформаційної безпеки	Чи має постачальник фіксовані вимоги щодо управління інцидентами інформаційної безпеки/кіберризиками та звітування про них, включаючи часові рамки звітування?	<i>Опишіть, будь ласка, наявність задокументованого порядку щодо управління інцидентами інформаційної безпеки/кіберризиками</i>
	Як постачальником послуг забезпечується реєстрація подій безпеки та збирання доказів щодо інцидентів ІБ? Як довго зберігаються журнали реєстрації подій?	<i>Опишіть, будь ласка, більш детально</i>
	Чи існує у постачальника послуг план реагування на інциденти ІБ/кіберризиків?	<i>Опишіть, будь ласка, більш детально</i>
	Чи мав постачальник за час своєї роботи суттєві порушення інформаційної безпеки/інциденти про які він повинен заявити?	<i>Опишіть, будь ласка, більш детально</i>
3. Захист мережі постачальника	Як постачальник захищає свою мережу від зовнішніх зловмисників та DDoS-атак?	<i>Опишіть, будь ласка, компоненти безпеки: наявність міжмережевого екрану, антивірусу, системи запобігання вторгненням, засобів захисту від DDoS-атак тощо</i>
	Як постачальник захищає свій внутрішній периметр мережі від внутрішніх зловмисників?	<i>Наприклад, від працівників, що можуть мати зловмисні наміри</i>

	Чи має постачальник журнал логування дій для аналізу подій у разі такої потреби?	<i>Якщо "так", опишіть, будь ласка, більш детально</i>
	Чи наявний контроль доступу до мережевого обладнання?	<i>Якщо "так", опишіть, будь ласка, більш детально</i>
	Чи налаштовано виявлення/блокування неавторизованих пристроїв у мережі?	<i>Якщо "так", опишіть, будь ласка, більш детально</i>
4. Керування вразливостями та виправленнями	Чи має постачальник в своїй організації процес виявлення та управління вразливостями і виправленнями?	<i>Якщо "так", опишіть, будь ласка, більш детально цей процес та усунення виявлених вразливостей</i>
	Як часто виконується сканування на вразливості мережі та програм постачальника послуг та його субпідрядників (якщо субпідрядник залучається до роботи)?	<i>Опишіть, будь ласка, більш детально</i>
	Чи проводить постачальник будь-які тести безпеки, такі як тести на проникнення своєї внутрішньої та зовнішньої ІТ-інфраструктури і як використовує отримані висновки?	<i>Опишіть, будь ласка, більш детально</i>
	Які заходи щодо контролю витоку даних реалізовано в організації постачальника?	<i>Опишіть, будь ласка, більш детально</i>
5. Організація захисту даних	Яким чином передаються та захищаються дані в процесі їх взаємодії між різними підрозділами постачальника послуг?	<i>Опишіть, будь ласка, через які канали комунікують між собою працівники постачальника, якщо в процесі їх роботи є передача чутливої інформації. Наприклад, корпоративна пошта чи месенджери, які саме?</i>
	Чи надійно постачальник видаляє або знищує інформацію перед утилізацією або повторним використанням знімних носіїв, якщо використовує їх в роботі?	<i>Наприклад, такі знімні носії як USB-накопичувачі та інші</i>
	Чи шифрує постачальник дані на портативних пристроях, таких як ноутбуки, мобільні телефони, планшети та знімні носії, у разі їх втрати або крадіжки?	<i>Якщо "так", опишіть, будь ласка, більш детально</i>
	Чи дозволяє постачальник використовувати своїм працівникам їх власні цифрові пристрої для роботи (власні ноутбуки, власні телефони, планшети тощо) та як забезпечує захист від витоку інформації на власних пристроях працівників?	<i>Якщо "так", опишіть, будь ласка, більш детально</i>
	Чи відповідає Парольна політика постачальника вимогам міжнародних стандартів?	<i>Опишіть, будь ласка, більш детально</i>

	Чи впроваджена багатофакторна аутентифікація до систем та програмних комплексів, які містять в собі критично важливу інформацію (інформацію з обмеженим доступом/персональні дані)?	Опишіть, будь ласка, більш детально
7. Управління і контроль доступів	Чи наявний процес управління доступами?	Якщо "так", опишіть, будь ласка, як видаються, актуалізуються та анулюються доступи до інформаційних ресурсів.
	Чи впроваджує постачальник розмежування доступу до інформації для персоналу?	Працівники мають доступ та права на модифікацію тільки до тієї інформації, яка необхідна їм для виконання своїх обов'язків
	Чи проводиться у постачальника логування дій облікових записів?	Опишіть, будь ласка, більш детально
8. Управління безперервністю систем інформаційної безпеки	Які заходи забезпечення доступності використовуються постачальником послуг?	Опишіть, будь ласка, більш детально (наприклад, наявні резервні канали зв'язку, засоби захист від DDoS-атак)
	Чи має постачальник План забезпечення безперервності бізнесу/аварійного відновлення для підтримки мінімальних рівнів обслуговування, якщо він постраждає від інциденту?	Наприклад, фізичні пошкодження наземних центрів обробки даних, атаки програм-вимагачів, DDoS-атаки тощо? Якщо "Так", вкажіть, будь ласка, першочергові заходи Плану забезпечення безперервності.
	Чи існує у постачальника послуг/товарів резервна інфраструктура (включаючи центр обробки даних) та з якою регулярністю створюються резервні копії конфіденційної та важливої інформації для її відновлення у разі аварії або іншого інциденту?	Якщо "так", опишіть, будь ласка, більш детально
9. Інформаційна безпека субпідрядників при взаємодії з постачальником	Чи планує постачальник залучати (або вже залучає) до виконання робіт субпідрядників?	Якщо "так", надайте, будь ласка, відповіді на наступні питання. Якщо "ні", пропустіть їх.
	Чи буде субпідряднику передаватись інформація з обмеженим доступом? Як дані Банку будуть захищатись під час їх передачі субпідрядникам постачальника послуг?	Опишіть, будь ласка, більш детально