Вимоги до WEB-кабінету клієнта/партнера в ПрАТ «УКРФІНЖИТЛО».

ТЕРМІНИ, СКОРОЧЕННЯ ТА ЇХ ВИЗНАЧЕННЯ

Термін/скорочення	Визначення
BankID	Сервіс електронної ідентифікації та автентифікації користувачів, який дозволяє підтвердити особу онлайн через банк, у якому людина вже ідентифікована.
BPM	Система управління бізнес-процесами за стандартами BPM.
Deep link (deep link)	Спеціальне посилання, яке веде не на головну сторінку, а безпосередньо на конкретний екран, розділ або дію всередині веб-сайту чи мобільного застосунку.
HRM	Програмне забезпечення для ведення кадрового обліку.
Inline-валідація	Перевірка введених користувачем даних, яка відбувається безпосередньо під час заповнення поля форми або одразу після виходу з нього, без перезавантаження сторінки і без відправки всієї форми (технологія, що одразу підказує, що дані введені некоректно.
2FA	Двох факторна авторизація.
БД	База(и) даних.
АБС Б2	Автоматизована банківська система Б2 – основна система обліку операцій та формування звітності ПрАТ «УКРФІНЖИТЛО».
ДІЯ	Портал Дія з відповідними механізмами обміну.
ДСТУ	Державні стандарти України.
ЕЦП	Електронний цифровий підпис.
КЕП	Кваліфікований електронний цифровий підпис.
НБУ	Національний банк України.
ПЗ	Програмне забезпечення.
СЕД Clever Forms	Система електронного документообігу та зберігання кредитних справ.
СУБД	Система управління базами даних.
Технологія Liveness	Технологія перевірки, що підтверджує, що перед системою жива реальна людина, а не фото, відео, маска чи інша підробка.
Товариство, ПрАТ «УКРФІНЖИТЛО»	ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО «УКРАЇНСЬКА ФІНАНСОВА ЖИТЛОВА КОМПАНІЯ».
ФОП	Фізична особа – підприємець.
ІзОД	Інформація із обмеженим доступом
Автентифікація	Процедура перевірки відповідності пред’явленого ідентифікатора користувача або процесу щодо належності його пред’явнику; встановлення або підтвердження автентичності.
Авторизація	Процедура перевірки прав доступу користувача та надання йому цих прав доступу до інформаційної системи
Користувач	фізична або юридична особа, яка в установленому порядку отримала право доступу до інформації в системі

Ідентифікація	Процес надання підстав для входу користувача в інформаційну систему
Шеринг	Процес швидкої та безпечної передачі цифрових даних. Ця технологія дозволяє автоматично заповнювати поля в базах даних за допомогою API, забезпечуючи точність даних.
Онбордінг	Процес інтеграції нового користувача або співробітника, спрямований на швидке знайомство з інтерфейсом, функціоналом та цілями цифрового продукту. Включає автоматизовані підказки, налаштування облікових записів та перегляд бази знань.
Партнер	Юридична особа, з якою укладений договір про отримання, обробку, обмін даними / документами.

Мета та загальний опис концепції

Головною метою веб-кабінету (Системи) є цифровізація та комплексна автоматизація процесів супроводу/ формування кредитних угод, зокрема:

- виконання нефінансових зобов'язань (ковенант);
- створення, збору, підписання та опрацювання документів кредитної справи;
- забезпечення дистанційної взаємодії клієнтів з Товариством та банками-партнерами без необхідності фізичної присутності;
- здійснення ідентифікації та верифікації клієнтів Товариства без необхідності фізичної присутності.

Система має забезпечувати надійне та безпечне підключення користувачів із застосуванням двофакторної автентифікації (2FA), а також обов'язкове логування дій користувачів для цілей контролю та аудиту.
Веб-кабінет надає клієнтам можливість:

- дистанційно надавати документи за для виконання нефінансових зобов'язань за кредитними угодами;
- переглядати актуальну інформацію щодо стану та умов своєї кредитної угоди;
- отримувати push-повідомлення та нагадування про події, дії або зобов'язання, що мають бути виконані у визначені строки.

Система передбачає автоматизацію повного циклу процесів, пов'язаних із виконанням нефінансових зобов'язань та формуванням кредитної справи, документообігом, зокрема за такими сценаріями:

1. Отримання та обробка даних

- автоматизоване отримання даних з державних та інших реєстрів (у тому числі через інтеграційні платформи облікової системи Товариства);
- ініціація отримання даних на підставі подій або встановлених бізнес-правил.

2. Формування та підписання документів

- формування електронних документів на основі отриманих даних;
- підписання сформованих документів клієнтом та або підписання обома сторонами із використанням КЕП.
- зберігання та відображення сформованих / підписаних документів.

3. Передача та опрацювання документів/отриманих даних

- автоматичне направлення підписаних документів до Товариства та/ або до іншого контрагента;
- використання документів як підтвердження виконання відповідних зобов'язань;
- подальша валідація, перевірка та опрацювання документів, збереження документів відповідно до внутрішніх процесів Товариства.

Для процесів, щодо яких автоматизоване отримання даних з реєстрів є неможливим, система передбачає:

- завантаження клієнтом електронних копій документів у форматі PDF;
- підписання завантажених документів КЕП;
- автоматичну передачу документів до систем Товариства для перевірки та подальшого опрацювання (можливість підтвердження документу/підписання зі сторони Товариства за потреби).

Категорії користувачів та модель доступу

Система має передбачати наявність персональних кабінетів для трьох основних категорій користувачів:

- **Фізичні особи (Клієнти**) — кінцеві споживачі послуг, які виконують нефінансові зобов'язання, формують / отримують / підписують документи та отримують повідомлення.
- **Партнери** — юридичні особи, ФОП та державні органи, залучені до процесів формування, підтвердження або перевірки документів / отриманих даних.
- **Адміністратори** — співробітники ПрАТ «УКРФІНЖИТЛО», які здійснюють налаштування процесів, контроль виконання та опрацювання результатів.

Доступ до функціональних можливостей системи регулюється гнучкою рольовою моделлю. Функціонал для партнерів є динамічним та налаштовується відповідно до конкретного бізнес-процесу або сценарію взаємодії. Адміністратори та партнери працюють виключно в межах визначених ролей, що обмежують або розширюють доступ до інструментів обробки документів, електронних форм та workflow-етапів.

Робота з партнерами та третіми сторонами

Веб-кабінет повинен підтримувати можливість залучення до бізнес-процесів партнерів та третіх осіб, зокрема:

- страхових компаній;
- суб'єктів оціночної діяльності;
- ФОП та інших учасників процесу.

Партнери можуть бути інтегровані у відповідні **workflow-сценарії**, з визначенням їх ролей, прав доступу та відповідальності на окремих етапах процесу.

BPM-модуль та управління процесами

Веб-кабінет має включати **BPM-модуль**, який забезпечує:

- самостійну побудову та модифікацію бізнес-процесів;
- налаштування етапів та проходження оформлення угоди;
- налаштування маршрутів документів і сценаріїв виконання ковенант;
- управління подіями, строками та статусами процесів;
- моніторинг виконання та оперативне реагування на відхилення;
- можливість використання у процесах зовнішніх сервісів (як для отримання інформації, так і для відправки), та обробки отриманої інформації у власних процесах;
- можливість отримання інформації про результати роботи процесів, що налаштовані у **BPM-модулі.**

Процеси можуть виконуватися як за участю третіх сторін, так і повністю автоматизовано — з використанням алгоритмів, правил обробки подій та інтегрованих інформаційних систем.

Інтеграційна складова

Веб-кабінет повинен мати можливість інтегруватися з багатьма зовнішніми сервісами, і мати власний інтеграційний рівень.

Функціональні вимоги

Категорія користувача: Клієнт	Обов'язковість	Коментар
Автентифікація та авторизація		
1. Система повинна забезпечувати автентифікацію користувачів через Дія, НБУ, BankID. Після автентифікації повинен використовуватись стандартний логін-пароль. У випадку, коли користувач не авторизувався у системі більш ніж деякий період (окрема змінна), система має вимагати повторну автентифікацію клієнта.	так	
2. Можливість забезпечення багатофакторної автентифікації (MFA) для всіх користувачів.	так	
3. Заповнення/оновлення даних в картці клієнта під час його автентифікації через Дія, НБУ, BankID. Оновлення даних з облікової системи Товариства чи облікових систем Банків-партнерів по клієнтам позичальникам.	так	
4. При першому вході в систему пошук та відображення інформації по: - Заявках клієнта - Угодах клієнта (включно з усіма його зобов'язаннями) - Інформацією отриманою через Open Bank API.	так	
5. Відновлення доступу повинно відбуватись через нову автентифікацію через Дія, НБУ, Bank ID.	так	
6. Система повинна визначати роль та доступний функціонал залежно від способу авторизації та наявних даних про клієнта (клієнт Товариства чи клієнт банку-партнера, які мають кредит, громадянин України, який планує отримати кредит, або який вже подав заявку на отримання через додаток ДІЯ).	так	
7. Під час онбордінгу та автентифікації в системі, користувач повинен мати можливість заповнення та оновлення анкети-опитувальника фінансового моніторингу.	так	
8. Підтримка технології Liveness.	так	Тут бажано зазначити замовника і мету такої ф-ті
9. Підтримка пристроїв біометричної авторизації користувача у системі.	так	
Основний функціонал		
1. Система повинна забезпечувати формування документів з заздалегідь доданих шаблонів, мати змогу виводити сформований документ на перегляд та забезпечувати підписання КЕП як сформованих документів що наповнюється даними з реєстрів/інтегрованих систем так і документів, які надається користувачем через інтерфейс	так	
2. Користувач повинен мати можливість завантажувати документи у форматах .jpg, .pdf, .png через інтерфейс (можливість конвертації через власні бібліотеки чи через сторонній сервіс у PDF) та можливість накладання власного КЕП на такі документи.	так	
3. Система забезпечує введення даних користувачем у форми та можливість налаштування валідації даних, та потреби у такій валідації (тип/формат на етапі введення).		

4. Забезпечується відображення статусу обробки сформованих , або завантажених документів/інформації /даних зазначених користувачем/партнером.	так	
5. Користувач повинен мати можливість надавати доступ до своїх документів іншим користувачам цього ж додатку, відправляти запити на приєднання та шерингові запити. Запити на приєднання або опрацювання документу мають пересилатися або через визначений месенджер, або через електронну пошту. У випадку, коли громадянин, якому надали посилання не є користувачем системи, обов'язкова автентифікація наявними механізмами.	так	
6. Система повинна надавати можливість перегляду інформації: - по заявках; - по рахунках (рух коштів, формування виписок); - по угодах та усіх її складових (кредитній угоді, угоді забезпечення, угоді страхування та інш.); - по ідентифікаційним даним користувача/опитувальнику (у тому числі для своєчасного оновлення); - Можливість сплати по рахунку через deep link у платіжний додаток банку, або за допомогою Open Bank API. Система повинна забезпечувати відображення користувачу статусу угод, заявок, зобов'язань (ковенант) та кредитів, а також надавати перелік необхідних дій у правильній послідовності з відповідним функціоналом для їх виконання.	так	
7. Система повинна мати модуль push-нотифікацій. Забезпечувати отримання push-повідомлень з посиланнями та можливістю переходу з цих посилань до відповідного функціоналу(після авторизації).	так	
8. Система повинна забезпечувати візуалізацію електронного документа у форматі друкованої форми.	так	
9. Користувач повинен мати можливість завантаження підписаних документів на свій пристрій.	так	
10. У системі повинна бути оболонка для онлайн-чату для комунікації користувача, зі збереженням усієї історії спілкування (глибина збереження по налаштуванням). Також можливість вивантаження історії спілкування до CRM системи.	так	
11. Перед накладанням другого, та інших підписів, система має контролювати валідність існуючого підпису на документі, тобто перевіряти чи не було цей документ змінено після накладання минулих підписів.		
UI/UX		
1. Для користувачів «Клієнт» має бути доступний функціонал як у web-інтерфейсі так і у мобільному WebView-додатку.	так	
2. WebView не повинен відрізнятись візуально та поведінково від нативного банківського застосунку.	так	
3. Інтерфейс оптимізований під мобільні екрани та touch-взаємодію.	так	
4. Навігація реалізується за нативними патернами (bottom navigation або ієрархія екранів).	так	
5. Кнопка «Назад» — внутрішня, без перезавантаження сторінок і без використання браузерної навігації.	так	
6. Заборонено відкриття нових вкладок, зовнішніх браузерів і неявні редіректи.	так	

7. Початкове завантаження веб-кабінету (Time to Interactive) має становити не більше 2 секунд за умови: - швидкості інтернет-з'єднання користувача не менше 10 Мбіт/с; - затримки мережі не більше 100 мс; - використання настільного браузера (Chrome, Edge, Firefox, Safari) останніх двох стабільних версій; - клієнтського пристрою з обсягом оперативної пам'яті не менше 8 ГБ; - переходи між екранами веб-кабінету здійснюються без повного перезавантаження сторінки та мають виконуватися не більше ніж за 500 мс, без урахування часу відповіді зовнішніх інтеграційних систем; - переходи між екранами без повного reload.	так	
8. Обов'язкові preload / skeleton-екрани; відсутність "білого екрану".	так	
9. Форми підтримують відповідні типи клавіатур, автофокус та inline-валідацію.	так	
10. Введені користувачем дані не втрачаються у разі помилок або повторних запитів.	так	
11. Єдина дизайн-система без web-ефектів (hover, стандартні HTML-форми).	так	
12. Кожна дія користувача має UI-відповідь (loader, toast, confirmation).	так	
Категорія користувача: Партнери	**Обов'язковість**	**Коментар**
Автентифікація		
1. Система повинна забезпечувати реєстрацію юридичної особи (ФОП) виключно з використанням кваліфікованого електронного підпису (КЕП), який належить відповідній Компанії.	так	
2. Під час реєстрації система повинна здійснювати перевірку чинності та коректності КЕП.	так	
3. Перший користувач, який успішно зареєстрував юридичну особу в системі, автоматично набуває статус адміністратора кабінету Компанії або іншої визначеної ролі з розширеними правами, з можливістю зміни адміністратора компанії або адміністратором системи, або співробітником компанії, з відповідними правами. (підтвердження авторизації з боку бізнес-адміністратора Товариства). Першого користувача має акцептувати адміністратор процесу.	так	Привілейований користувач
4. Система повинна забезпечувати можливість первинному користувачу Компанії запрошувати інших працівників до кабінету юридичної особи (заведення користувачів, надання їм ролі, та відправка посилань на електронну пошту). За посиланням користувачі заходять по тимчасовому доступу, з обов'язковим введенням паролів. Термін дії посилання з тимчасовим паролем, повинен задаватися адміністратором системи.	так	
5. Надсилання запрошень іншим користувачам здійснюється через електронне повідомлення на вказану адресу електронної пошти з заздалегідь визначеною адміністратором роллю.	так	

6. Доступ запрошених користувачів до системи надається після проходження ними процедури авторизації відповідно до встановлених правил системи.	так	
7. Система повинна забезпечувати можливість відновлення доступу користувача (через ті ж механізми, якими користувач автентифікувався у системі, *п 4.- автентифікація-партнери*).	так	
Основний функціонал		
1. Система повинна забезпечувати формування документів з заздалегідь доданих шаблонів, мати змогу виводити сформований документ на перегляд та забезпечувати підписання КЕП (одним підписом КЕП чи декількома, в залежності від типу документу) як сформованих документів що наповнюється даними з реєстрів/інтегрованих систем так і документів, які надаються користувачем через інтерфейс.	так	
2. Забезпечується наявність конструктора шаблонів форм електронних документів.	так	
3. Система повинна підтримувати використання заздалегідь налаштованих та довільних маршрутів проходження документів для категорії Партнери.	ні	
4. Система повинна забезпечувати електронне узгодження документів з можливістю як послідовного, так і паралельного узгодження різними компаніями.	так	
5. Забезпечується моніторинг проходження та обробки документів з візуалізацією статусів та основних реквізитів документів.	так	
6. Користувач повинен мати можливість накладати електронний підпис на документи та файли, згенеровані системою або завантажені в систему.	так	
7. Система повинна забезпечувати перегляд статусу обробки документів та файлів, до яких користувач має доступ. Має бути механізм нагадувань щодо невиконаних подій, шляхом повідомлень на електронну пошту / месенджер.	так	
8. Користувач повинен мати можливість надавати доступ до своїх документів іншим користувачам, компаніям або клієнтам.	так	
9. Система повинна забезпечувати обмін повідомленнями між користувачами, зі зберіганням історії спілкування.	так	
10. Система повинна забезпечувати сервіс поштових повідомлень щодо зміни статусу документа на всіх етапах його життєвого циклу.	так	
11. Користувач повинен мати можливість вивантаження підписаних документів на диск ПК для подальшого використання у вигляді файлу та/або розміщення в окремому електронному архіві (за наявності).	так	
12. Система повинна забезпечувати розгалужений інструмент швидкого пошуку необхідних документів.	так	
UI/UX		
1. Інтерфейс зрозумілий, послідовний, максимально наближений до нативного офісного софту.	так	
2. Чітка навігація: sidebar / панель меню, breadcrumbs, фільтри та сортування без перезавантаження.	так	
3. Списки документів із ключовими атрибутами (назва, дата, статус, відповідальний) та preview у модальному вікні.	так	
4. Inline-перевірка полів та підказки при додаванні документів або метаданих.	так	

5. UI-відповідь на всі дії: loader під час обробки, toast при успіху, confirmation для критичних дій.	так	
6. Пошук і фільтри з багатовибором, динамічне оновлення списку та збереження останніх параметрів.	так	
7. Швидке завантаження списків (lazy loading), preview документів без повного завантаження, підтримка слабкого інтернету.	так	
8. Єдина дизайн-система, кольори статусів документів, видимі та чіткі CTA-кнопки.	так	

Категорія користувача: Адміністратори	**Обов'язковість**	**Коментар**
Автентифікація		
1. Система повинна забезпечувати автентифікацію адміністраторів виключно через внутрішню систему автентифікації Компанії.	так	
2. Система повинна підтримувати інтеграцію з внутрішнім сервісом автентифікації (IdP) із використанням встановлених протоколів безпеки.	так	
3. Доступ до адміністративного функціоналу Системи надається лише користувачам з роллю «Адміністратор».	так	
4. Система повинна підтримувати рольову модель доступу з можливістю розмежування прав адміністраторів за функціональними модулями.	так	
5. Процедура відновлення доступу повинна здійснюватися через внутрішню систему автентифікації Компанії та відповідати вимогам інформаційної безпеки.	так	
6. Дії адміністраторів повинні логуватися та бути захищеними від змін.	так	
Основний функціонал		
1. Система має вести та відображати список користувачів. Призначати, змінювати та керувати системою ролей і прав доступу в межах повноважень. Блокувати користувачів системи.	так	
2. Управління конфігураціями Системи без необхідності внесення змін у програмний код.	так	
3. Налаштування шаблонів документів у конструкторі форм, бізнес-процесів за допомогою BPM-модуля.	так	
4. Можливість примусово змінювати статуси документів, по заздалегідь прописаним правилам.	так	
5. Фіксація усіх дій користувачів Системи у розрізі дат, Компаній і т. п.	так	
6. Перегляд журналу виконання користувачами операцій.	так	
7. Блокування в Системі роботи Компаній, Користувачів.	так	
8. Моніторинг працездатності та рівня навантаження.	так	
9. Система повинна забезпечувати візуалізацію дашборду для моніторингу процесів, налаштованих у BPM, з метою контролю статусу заявок/документів та дотримання регламентних таймінгів їх проходження а саме: - Відображення стану процесів: a. відображати перелік BPM-процесів із різними кроками (steps). b. Для кожного процесу та кожного кроку повинна відображатися: i. кількість заявок/документів, що наразі знаходяться на відповідному кроці;	так	

ii. (опційно) розподіл за статусами: в роботі / на паузі / очікує дій тощо. - Контроль таймінгів (SLA / нормативи) для кожного кроку процесу. Користувач повинен мати можливість перейти з дашборду: - до списку заявок/документів на конкретному кроці; - до картки конкретної заявки/документа.		
10. Адміністратор повинен мати доступ до журналів виконання користувачами операцій, з можливістю фільтрування за датою, Компанією або користувачем. Журнали повинні містити повну інформацію про дії користувачів (автентифікація, створення/зміну/видалення документів, підписання КЕП). Можливість перегляду історії подій та експорт відповідних записів для проведення аналізу чи аудиту.	так	
11. Адміністратор повинен мати можливість налаштовувати інтеграційні параметри із зовнішніми системами (наприклад, внутрішній документообіг, ERP чи CRM) через BP/API або шину інтеграцій ESB.	так	

Нефункціональні вимоги	Обов'язковість	Коментар
WEB кабінет клієнта/партнера		
Загальна інформація		
1. Україномовний інтерфейс.	так	
2. Передбачати реєстрацію (фіксацію та протоколювання) будь-яких подій, проведених у Системі, та часу їх проведення до мілісекунд (у тому числі налаштування прав доступу, авторизації процесів).	так	
3. Має використовувати типи підписів CAdES-LT / CAdES-LTA, та/або PAdES-LT / PAdES-LTA. Контейнер ASIC-E.	так	
4. Інтеграція з хмарним Microsoft AD та наземним Microsoft AD (для співробітників).	так	
Вимоги до документації		
1. Документація для розробника ПЗ, в якій описані механізми налаштування, API інтерфейсів та доопрацювання системи, без залучення співробітників компанії виробника.	так	
2. Документація для адміністратора програмного забезпечення, в якій описані механізми адміністрування та розгортання поточної версії програмного забезпечення, в тому числі для відновлення програмного забезпечення з резервної копії.	так	
3. По всій документації має бути створений Єдиний словник термінів та визначень.	так	
4. Документація для кінцевого користувача системи (у розрізі ролей) – інструкції користувача, в якій повністю описані всі функції поточної версії ПЗ.	так	
Система розподілення прав доступу		
1. Розмежування та налаштування прав доступу (перегляд, редагування, підписання, адміністрування) без розробників ПЗ – застосування рольової моделі	так	

доступу з урахуванням структури організації, функцій та повноважень; Захищеність даних.		
Навантаження на систему		
1. Кількість активних клієнтів не менше 100 000 шт.	так	
2. Кількість користувачів, які одночасно знаходяться в системі не менше 1000 шт.	так	
Використання КЕП		
1. Використання ДІЯ підпис для клієнтів фізичних осіб для накладання КЕП на документи	так	
2. Використання КЕП організації для накладання КЕП на документи зі сторони юридичної особи.	так	
Інтеграції		
1. Вивантаження опрацьованих документів до сховища (реєстру) кредитних справ (інтеграція с СЕД Clever Forms у відповідності до існуючого API)	так	
2. Зі страховими компаніями (відповідно до переліку авторизованих страхових).Вибір продуктів страхування, передача запитів на оформлення, та фіксація результату обробки запитів на стороні Страхової	так	
3. Державними реєстрами , такими як (але не виключно): ЄДР, ДРРПНМ, ДРОРМ, бази даних ПФУ/ДПІ, ЄДЕССБ, портал ДІЯ.	так	
4. АБС Б2 (отримання / передача даних, подій)	так	
4.1. Отримання подій та їх обробка.	так	
4.2. Формування електронних документів у відповідності до шаблонів	так	
4.3. Запуск документів за маршрутами підписання	так	
5. З системою HRM, для заведення користувачів Товариства	так	
Маршрути		
1. Розподіл та налаштування маршрутів проходження кожного типу документу	так	
Заведення користувачів		
1. Фізичні особи позичальники	так	
1.1. За допомогою посилання з обов’язковою авторизацією.	так	
2. Юридичні особи	так	
2.1. Заведення адміністраторами юридичних організацій.	так	
2.2. Адміністратори юридичних організацій заводяться/акцептуються бізнес-адміністраторами Товариства.	так	
2.3. Можливість реєстрації у Системі за допомогою КЕП відповідної Компанії.	так	
3. Співробітники Товариства	так	
3.1. Заведення адміністраторами Товариства.	так	
Аналітика		
1. Функціонал повинен забезпечувати збір, зберігання / передачі даних по подіям створених користувачами.	так	

2. Налаштування аналітики мають здійснюватися без значних внесень змін у програмний код. Один з варіантів, за допомогою Remote Config. Адмінка / Config Service ↓ (JSON) Remote Config API ↓ Mobile App ↓ Event Processor (в коді) ↓ Analytics Collector API (ваш backend) ↓ DB / DWH / BI.	так	
3. Система повинна підтримувати визначення та управління переліком подій, що фіксуються.	так	
4. Для кожної події має бути можливість налаштування параметрів (атрибутів), типів даних та обов'язковості заповнення (налаштування через адмінку).	так	
5. Повинна бути можливість вмикати або вимикати збір окремих подій.	так	
6. Аналітичні дані, що формуються клієнтським застосунком, повинні передаватися разом із уніфікованим набором метаданих, які описують час формування даних, контекст їх виникнення, характеристики клієнтського середовища та параметри сесії користувача.	так	
7. Система повинна підтримувати передачу аналітичних даних до зовнішніх систем (BI / DWH) через API або інші інтеграційні механізми.	так	
8. Має бути передбачена можливість анонімізації або маскування даних.	так	
9. Система повинна надавати можливість проведення A/B тестування функціоналу.	так	
Інформаційна безпека та захист даних		
В системі WEB-кабінет позичальника, має оброблятись інформація що містить — персональні дані, банківську таємницю, відомості з державних реєстрів та юридично значимі документи з накладеним КЕП, що передбачено процесами автентифікації, збору ідентифікаційних даних, доступу до кредитних матеріалів, фінансової інформації та інтеграцій з державними інформаційними реєстрами (системами). Сукупність таких даних відноситься до інформації з обмеженим доступом і підпадає під посилені вимоги захисту відповідно до законодавства України (банки, фінансові компанії), що зумовлює необхідність комплексного впровадження заходів інформаційної безпеки та контролю доступу в системі.		
1. Вимоги до контролю доступу (управління ідентифікацією, автентифікацією та доступом):		
1.1. Система повинна підтримувати інтеграцію з Microsoft Active Directory (локальним та хмарним) для автентифікації співробітників.	так	
1.2. Повинна бути реалізована 2-факторна автентифікація для всіх типів користувачів: співробітників, фізичних та юридичних осіб.	так	
1.3. При першому вході система має генерувати тимчасовий пароль з обов'язковим підтвердженням через Microsoft/Google Authenticator, СМС, e-mail або еквівалентним Системам.	так	
1.4. Після входу користувач зобов'язаний змінити тимчасовий пароль на власний відповідно до політики паролів.	так	

1.5. Облікові записи мають автоматично блокуватись після певної кількості невдалих спроб входу або тривалої не активності у відповідності до налаштованих правил.	так	
1.6. Доступ до системи повинен бути можливий лише для автентифікованих користувачів; всі спроби доступу без підтвердженої автентифікації повинні блокуватись.	так	
1.7. Система повинна завершувати сесію користувача при неактивності понад встановлений час (налаштовується).	так	
1.8. Повинна бути реалізована система управління ролями (RBAC) з можливістю налаштування типових ролей.	так	
2. Аудит, контроль дій та незмінність журналів:		
2.1. Система повинна логувати всі дії користувачів (включаючи привілейованих), із зазначенням ідентифікатора, часу, IP-адреси, дії та об'єкта впливу.	так	
2.2. Для всіх важливих операцій (зміна даних, підпис документів, видалення) має бути реалізовано підтвердження (2FA або CAPTCHA).	ні	
2.3. Повинна зберігатись історія змін та версійність документів із можливістю відновлення.	так	
2.4. Логи повинні зберігатись в незмінному вигляді (WORM, хеш-ланцюг) не менше одного року. Доступ до журналів має бути обмеженим за ролями.	так	
3. Криптографічний захист (захист даних та управління інформацією):		
3.1. Система повинна забезпечувати класифікацію інформації (ІзОД, персональні дані, банківська таємниця, таємниця фінансової послуги). Тобто система має дозволяти маркувати документи, які є у довідниках системи різними типам у відповідності до довідника класифікації.	так	Підтримка моделі класифікації даних
3.2. До кожного типу даних повинні застосовуватись відповідні: • правила доступу (ролі, рівні доступу, об’єкти доступу та. інш.); • типи маскування (часткове, повне, динамічне, інше), журналювання (доступу, змін, операцій, розширеного аудиту); • механізми контролю обробки. (перевірка повноважень, інтеграційних потоків, масових операцій, workflow-затвердження). Вимога щодо застосування правил доступу, маскування, журналювання та контролю обробки поширюється на ті типи даних, для яких це передбачено їхньою категорією, рівнем чутливості, ролями користувачів та вимогами безпеки.	так	
3.3. Повинна бути реалізована підтримка КЕП/ЕЦП згідно з ДСТУ, включаючи підпис довготривалого зберігання.	так	LTA (Long-Term Archive)
3.4. Підтримка токенів ІІТ, Автор та різних HSM, у тому числі і хмарних.	так	
4. Захист каналів передачі даних:		
4.1. Система повинна забезпечувати безпеку при взаємодії із зовнішніми інформаційними програмними комплексами з використанням засобів шифрування (має забезпечуватись шифрований обмін між серверами додатків та серверами СУБД, або в рамках лінку між БД).	так	TLS 1.2+ або VPN/IPSEC.
4.2. Система не повинна використовувати незахищені протоколи.	так	HTTP, FTP, Telnet тощо
5. Захист веб-додатку та API*:		
5.1. WEB-кабінет та його API повинні бути захищені через впровадження WAF (Web Application Firewall).	так	

5.2. Повинно бути реалізовано захист API.	так	API keys, throttling, JWT або OAuth2
5.3. Система має бути піддана тестуванню на проникнення відповідно до методології OWASP. Усі виявлені вразливості повинні бути усунені постачальником, факт їх усунення має бути підтверджений результатами повторного тестування.	так	OWASP
Технічна інфраструктура		
1. Наявність BPM модулю для самостійної побудови та управління процесами.	так	
2. Система у рамках функціонування має бути багатокомпонентною системою, тобто побудована за багаторівневою архітектурою (програмний додаток, що підключений до сервера(-ів) додатків, який у свою чергу підключений до сервера бази даних), з WEB інтерфейсом і підтримувати операційні системи Windows 10 та вище, MacOS, та браузери MS EGE, Google Chrome, Safari.	так	
3. Всі сторінки веб-додатків повинні бути відображені правильно (без перерв у макеті) в тій же зручній формі на настільному комп'ютері та на мобільному пристрої (планшет, ноутбук, смартфон), незалежно від типу пристрою (без використання окремої мобільної версії Системи), тобто Web – клієнт повинен перебувати в адаптивному «Google Material Design» інтерфейсі.	так	
4. Для певного типу користувачів (фізичні особи) має бути доступний функціонал у мобільному WebView-додатку	так	
5. Архітектура системи повинна підтримувати роботу в кластері, для забезпечення максимальної відмово стійкості компонент системи.	так	
6. База даних, яка використовується для зберігання даних, повинна мати можливість роботи в ACTIVE/PASIVE режимі з мінімальним терміном переключення, у разі виходу з ладу ACTIVE бази, та/або мати можливість роботи в кластері.	так	
7. Багатокористувацький режим роботи.	так	
8. Можливість централізованого автоматичного оновлення Системи, без зупинки процесів (не стосується БД).	так	
9. Система повинна мати підсистему адміністрування.	так	
10. Система повинна надавати можливість апаратного та програмного масштабування.	так	
11. Система має бути реалізовано з урахуванням вимоги безперервності ведення діяльності, у тому числі: резервне копіювання (гарячий та холодний бекап) баз даних та інформації, встановлення оновлень.	так	
12. Система має підтримувати роботу з промисловою СУБД (одна з: Microsoft SQL, Oracle, PostgreSQL) включаючи роботу з застосування вищевказаних СУБД в хмарному середовищі.	так	
13. Система має працювати по невиділеному каналу зв'язку між клієнтською робочою станцією і сервером додатків. Допускається мобільний доступ (3G\LTE), виділена лінія, локальна мережа.	так	
14. Система має підтримувати роботу клієнтських робочих місць у віддаленому доступі у будь-якій точці світу, у тому числі засобами VPN.	так	

15. Система повинна забезпечувати задовільну швидкість роботи за умови, що середні показники обладнання на робочих місцях: ✓ комп'ютер 8 ГБ ОЗУ, Частота процесору 2,5 Ghz, 150Gg HDD (мінімальна конфігурація ПК робочих місць користувачів - PC, CPU: 2 Core @ 2,5 Ghz, RAM: 8Gb, HDD: 150Gb); ✓ операційна система Win 11 або вище; ✓ веб-браузер: відповідно до вимог, наведених вище; ✓ мережа: 2 Mbps і вище.	так	
16. Серверна частина Система повинна підтримувати роботу у хмарному віртуалізованому середовищі.	так	
17. Система має бути розгорнуто на промислових операційних системах (Windows, Linux).	так	
18. Система повинна мати механізми діагностики та моніторингу стану всіх компонентів та стану серверних додатків.	так	
19. Система повинна мати автоматичний збір даних про програмні помилки, збої в Системі, некоректне завершення сеансів користувачів Системи, та збереження у журналі подій.	так	
20. Можливість коригування та створення друкованих шаблонів.	так	
21. Розробник/Постачальник повинен надавати всі наявні оновлення версій згідно з договором підтримки, повідомляючи про їх наявність регулярно або за запитом.	так	
22. Система має підтримувати прозорий механізм оновлень з застосуванням 3-рівневої моделі середовищ (Розробки-Тестове-Продуктивне);	так	
23. Система має передбачати формування звіту про роботу користувачів.	так	
24. Система має передбачати можливість архівування інформації журналів роботи користувачів.	так	
25. Система не повинна використовувати системних файлових мережних дисків/ресурсів для обміну між серверами бази даних та серверами додатків/додатків або веб-серверами, взаємодія повинна відбуватися виключно по портах бази даних та портах, що використовують веб-додатки. Всі інші порти блокуються відповідно до політик безпеки Товариства.	так	
Інші вимоги		
Ліцензії на використання ПЗ		
Якщо програмний продукт продається за умови строкової дії ліцензій, в розрахунок комерційної пропозиції має бути включена вартість володіння ліцензіями протягом 3-5 років.	так	
Підтримка		
В комерційну пропозицію мають бути включені витрати на сервісну підтримку ПЗ, при цьому:		
- Строк гарантійного (безкоштовного) обслуговування не може бути меншим 12 місяців з моменту переходу до продуктивної експлуатації.	так	
- Під сервісним та гарантійним обслуговуванням мається на увазі усунення виявлених помилок в роботі програмного забезпечення, моніторинг та проактивне налаштування ПЗ щодо змін в законодавстві, налаштування звітів та виконання необхідних доопрацювань.	так	