**АНКЕТА ПО АУДИТУ  
СИСТЕМЫ УПРАВЛЕНИЯ РИСКАМИ (СУОР) В  
СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ 716-П**

|  |  |
| --- | --- |
|  | |
| Наименование НФО/Банка |  |
|  | |
| Контактное лицо |  |
|  | |
| Телефон |  |
|  | |
| Email |  |
|  | |
| Дата заполнения |  |
|  | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. Цель проведения | | | | |
|  | | | | |
| Выполнение требования Положения ЦБ РФ 716-П к системе управления операционными рисками  Оценка действующей СУОР  Подготовка к проверке регулятора | | | | |
| Другое |  | | | |
|  | *Указать* | | | |
| *- выбрано;*  *- не выбрано* | | | | |
|  | | | | |
|  | | | | |
| 1. Имеется ли служба управления рисками? | | | | |
|  | | | | |
| Да, занимается всеми видами операционных рисков (ОР)  Да, занимается исключительно финансовыми рисками  Нет | | | | |
|  | | | | |
|  | | | | |
| 1. Проведена ли классификация рисков? | | | | |
|  | | | | |
| Да, в соответствии с 716-П  Да, по иной методике  Нет | | | | |
|  | | | | |
|  | | | | |
| 1. Укажите, какие процедуры по управлению рисками реализованы? | | | | |
|  | | | | |
| **Процедура** | | **Реализация** | | |
|  | | | | |
| Идентификация рисков | | | Да | Нет |
|  | | | | |
| Сбор и регистрация событий и потерь | | | Да | Нет |
|  | | | | |
| Определение и возмещение потерь | | | Да | Нет |
|  | | | | |
| Количественная оценка уровня ОР | | | Да | Нет |
|  | | | | |
| Качественная оценка уровня ОР | | | Да | Нет |
|  | | | | |
| Самооценка рисков не реже одного раза в год по собственной методике | | | Да | Нет |
|  | | | | |
| Выбор и применение способа реагирования на ОР | | | Да | Нет |
|  | | | | |
| Мониторинг ОР | | | Да | Нет |
|  | | | | |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Ведется ли работа с рисками IT? | | | | | | | | | | | |
|  | | | | | | | | | | | |
| Да, в соответствии с 716-П  Да, по иной методике  Нет | | | | | | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Ведется ли работа с рисками ИБ? | | | | | | | | | | | |
|  | | | | | | | | | | | |
| Да, в соответствии с 716-П  Да, по иной методике  Нет | | | | | | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Укажите количество человек в штате отдела управления рисками, включая филиалы | | | | | | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| *Указать* | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Оцените степень документирования процессов системы управления рисками | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | | 6 | 7 | 8 | 9 | 10 | |
|  | | | | | | | | | | | |
| *1 - не документировано* | | | | | | *10 - документировано в полном объеме* | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Кто из персонала вовлечен в работу с рисками? | | | | | | | | | | | |
|  | | | | | | | | | | | |
| Высшее руководство (Правление, Наблюдательный Совет)  Руководство структурных подразделений  Сотрудники профильного подразделения  Все сотрудники (хотя бы в части обнаружения событий) | | | | | | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Ведётся ли база событий ОР | | | | | | | | | | | |
|  | | | | | | | | | | | |
| Да, в соответствии с 716-П  Да, по иной методике (включая возмещение)  Да, по иной методике (только события/убытки, без возмещения)  Нет | | | | | | | | | | | |
|  | | | | | | | | | | | |
| |  |  | | --- | --- | | 1. Существует в Вашей организации специализированное подразделение по информационной безопасности? | | |  | | | Да | Нет | |  | | | Если да, то сколько человек в данном подразделении? | | |  | | |  | |  |  |  |  | | --- | --- | --- | | 1. Имеются ли процессы, переданные на аутсорсинг? | | | |  | | | | Да | | Нет | |  | | | | Если да, то какие? | | | |  | | | |  | | | |  | | | | 1. Каким образом Вы проверяете, обеспечивают ли Ваши партнеры, поставщики или подрядчики необходимый уровень защиты Вашей информации при ее обработке, передачи и хранении? | | | |  | | | | Анализ результатов оценок и иных сертификаций, проводимых внешними поставщиками или подрядчиками (например, ISO/IEC 27001, BS 25999);  Анализ результатов проведения независимых оценок партнеров, поставщиков или подрядчиков, проведенных внешними организациями (например, SSAE 16);  Проведение оценки силами Вашего подразделения информационной безопасности или службы внутреннего аудита (напр., выезд на место, тестирование системы безопасности);  Анализ или оценка не проводится | | | | Иное |  | |  |  | | --- | | 1. Включены ли в договоры, заключаемые с клиентами, партнерами или подрядчиками, конкретные требования по обеспечению информационной безопасности? | |  | | Да, все договора включают в себя конкретные требования к обеспечению информационной безопасности; | | Да, отдельные договора включают в себя конкретные требования к обеспечению информационной безопасности; | | Нет, конкретные требования к обеспечению информационной безопасности не включаются в договора |  |  |  |  |  | | --- | --- | --- | --- | | 1. Укажите типы информационных систем (ИС) и количество пользователей | | | | |  | | | | | **Тип ИС** |  | **Количество пользователей «удаленные»** | **Количество пользователей «офисные»** | |  | | | | |  |  |  |  | |  | | | | |  |  |  |  | |  | | | | |  |  |  |  | |  | | | | |  |  |  |  | |  | | | | |  |  |  |  | |  | | | | |  |  |  |  | |  | | | | |  |  |  |  | |  |  |  |  | |  | | | |  |  | | --- | | 1. Перечень программно–технических средств | |  | | Укажите перечень программно–технических средств, включенных в область действия системы управления информационной безопасности: | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | | *numbers of servers and desktops, types of networks, application development, access controls, use of encryption etc.* | |  |  |  | | --- | | 1. Проведена ли в Вашей организации инвентаризация и классификация информационных ресурсов? | |  | | Да, для всех критичных ресурсов; | | Да, для некоторых критичных ресурсов, работа не завершена; | | Нет, не проведена |  |  |  | | --- | --- | | 1. Какие из перечисленных пунктов входят в программу по обеспечению непрерывности бизнеса в Вашей организации? | | |  | | | Определение очередности восстановления критичных бизнес-процессов;  Согласованные полномочия и обязанности всех участников группы по восстановлению в условиях инцидента или кризисной ситуации;  Выявление и оценка основных угроз и рисков, влияющих на непрерывность деятельности;  Процедуры управления инцидентами или кризисной ситуацией (в том числе, порядок эскалации кризисной ситуации, а также внутренние и внешние коммуникации);  План восстановления ИТ инфраструктуры после сбоев (IT DRP);  Процедуры восстановления бизнес-процессов;  План тестирования системы обеспечения непрерывности бизнеса, включающий в себя обзор упражнений и тестов;  Стратегия по обеспечению непрерывности бизнеса, направленная на восстановление ИТ и телекоммуникаций, сопутствующей инфраструктуры, а также критичных бизнес-процессов в случае экстренной ситуации;  Планы повышения осведомленности и обучения персонала по вопросам обеспечения непрерывности бизнеса | | |  | | | 1. Каким образом в Вашей организации проходит оценка программы по обеспечению непрерывности деятельности? | | |  | | | Тестирование с использованием контрольных листов;  Тестирование полного нарушения деятельности организации и функционирования ИТ-инфраструктуры (тестирование фактических отказов);  Проведение имитационного тестирования восстановления деятельности бизнес-подразделений после сбоев;  Проведение имитационного тестирования восстановления ИТ-инфраструктуры после сбоев;  Проведение полного имитационного тестирования восстановления ИТ после сбоев;  Моделирование процесса управления кризисной ситуацией (для руководителей операционных подразделений и высшего руководства);  Проведение полного имитационного тестирования нарушения непрерывности деятельности организации (моделирование экстренной ситуации);  Параллельное тестирование (проводится на резервных площадках);  Оценка не проводится | | |  | | | 1. Как в Вашей организации построено взаимодействие с ключевыми контрагентами в контексте обеспечения непрерывности деятельности? | | |  | | |  | | |  | | |  | | |  | | |  | | |  | | |  | | | 1. Какие вопросы рассматриваются в программе повышения осведомленности по вопросам безопасности, принятой в Вашей организации? | | |  | | | Повышение осведомленности по вопросам обеспечения информационной безопасности;  Проверка, согласование и соблюдение действующих политик и стандартов в области безопасности;  Оценка эффективности мероприятий по повышению осведомленности и улучшение существующей программы на основании результатов такой оценки;  Распространение наглядных и регулярных новостей/оповещений о существующих угрозах для Вашей организации;  Распространение информационных сводок по новым актуальным темам;  Проведение специальных мероприятий или тренингов в области безопасности для пользователей, входящих в группы высокого риска | | | Иное |  |  |  |  | | --- | --- | | 1. Какие из перечисленных документов имеются в Вашей организации? | обязательно | |  | | | Политика управления операционными рисками (ОР);  Политика информационной безопасности (ИБ);  Политика информационных систем (ИС);  Порядок управления рисками ИБ;  Порядок ведения базы событий риска ИБ;  Требования к внешним контрагентам, выполняющим функции обеспечения ИБ (аутсорсинг), а также определение порядка взаимодействия и ответственности между ними;  Требования к организации ресурсного (кадрового и финансового) обеспечения системы обеспечения ИБ;  Порядок обеспечении информационной безопасности на стадиях (этапах) жизненного цикла автоматизированных информационных систем (АИС);  Повышение осведомленности работников в вопросах информационной безопасности;  Методические указания к порядку расчета и обоснованию сигнальных и контрольных значений КПУР ИБ;  Организация и функционирование системы ИБ;  Организация контроля за функционированием системы обеспечения ИБ;  Сканирование на проникновение и анализ уязвимостей ИБ объектов информационной инфраструктуры (ИИ);  Управление инцидентами ИБ;  Управление рисками ИБ;  Порядок обеспечения непрерывности и качества функционирования информационных систем;  Положение по обеспечению качества данных в информационных системах (ИС);  Использование ресурсов сети Интернет;  Защита от воздействия вредоносных кодов;  Порядок и методы определения потерь от реализации событий ОР, а также способов возмещения;  Система КПУР;  Положение об оценке персонала;  Система мотивации персонала к участию в управлении ОР;  Концепция о применимости мер защиты информации (ЗИ) в отношении объектов информационной инфраструктуры (ИИ);  Положение об оценке СУОР;  Положение о группе реагирования на подозрительные платежи в антифрод-системе;  Правила проведения сценарного анализа ОР;  Положение о резервном копировании;  Положение о проведении аудитов;  Перечень (реестр) информационных систем, обеспечивающих соответствующие им бизнес-процессы. | | | | | | | | | | | | | |
| 1. Желаемый перечень работ по Положению 716-П | | | | | | | | | | |
|  | | | | | | | | | | |
| Аудит соответствия требованиям 716-П  Разработка рекомендаций по приведению в соответствие 716-П  Разработка необходимой организационно-распорядительной документации (ОРД) для соответствия 716-П  Аудит соответствия требованиям главы 7 716-П (риски ИБ)  Разработка необходимой организационно-распорядительной документации для соответствия главы 7 716-П (риски ИБ)  Аудит соответствия требованиям главы 8 716-П (риски ИТ)  Разработка необходимой организационно-распорядительной документации (ОРД) для соответствия главы 8 716-П (риски ИТ)  Аудит соответствия требованиям глав 7 и 8 716-П (риски ИБ и ИТ)  Разработка необходимой организационно-распорядительной документации (ОРД) для соответствия глав 7 и 8 716-П ((риски ИБ и ИТ) | | | | | | | | | | |
|  | | | | | | | | | | |
|  | | | | | | | | | | |
| 1. Желаемый перечень сопутствующих работ | | | | | | | | | | |
|  | | | | | | | | | | |
| Аудит организации в направлении обработки/защиты персональных данных  ☐ Определение ВНД в рамках обеспечения операционной надежностью в соответствии с требованиями Положения Банка России 787-П (779-П) | | | | | | | | | | |
|  | | | | | | | | | | |
|  | | | | | | | | | | |
| 1. Поставка технических решений (ПО, ПАК) ИБ/ИТ и СУОР | | | | | | | | | | |
|  | | | | | | | | | | |
| Планируется ли поставка решений ИБ/ИТ, СУОР?  Требуется ли консультация по вопросам поставки и внедрения решений ИБ/ИТ, СУОР? | | | | | | | | | | |
|  | | | | | | | | | | |
| Какие решения по ИБ/ИТ, СУОР Вами рассматриваются? | | | | |  | | | | | |
|  | | | | | *Указать* | | | | | |
|  | | | | | | | | | | |
|  | | | | | | | | | | |

Спасибо!

На основании заполненной анкеты сформируем коммерческое предложение и отправим Вам ответным письмом