**ОПРОСНЫЙ ЛИСТ ПО АУДИТУ  
СИСТЕМЫ УПРАВЛЕНИЯ РИСКАМИ В  
СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ 716-П**

|  |  |
| --- | --- |
|  | |
| Наименование организации |  |
|  | |
| Контактное лицо |  |
|  | |
| Телефон |  |
|  | |
| Email |  |
|  | |
| Дата заполнения |  |
|  | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. Цель проведения | | | | |
|  | | | | |
| Выполнение требования Положения ЦБ РФ 716-П о корректном формировании системы управления операционными рисками  Оценка действующей системы управления операционными рисками  Подготовка к проверке регулятора | | | | |
| Другое |  | | | |
|  | *Указать* | | | |
| *- выбрано;*  *- не выбрано* | | | | |
|  | | | | |
|  | | | | |
| 1. Имеется ли служба управления рисками? | | | | |
|  | | | | |
| Да, занимается всеми видами рисков  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 оперрисков | | | Да | Нет |
|  | | | | |
| Качественная оценка уровня оперрисков | | | Да | Нет |
|  | | | | |
| Самооценка рисков не реже одного раза в год по собственной методике | | | Да | Нет |
|  | | | | |
| Выбор и применение способа реагирования на оперрисков | | | Да | Нет |
|  | | | | |
| Мониторинг оперрисков | | | 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  Руководство подразделений  Сотрудники профильного подразделения  Все сотрудники (хотя бы в части обнаружения событий) | | | | | | | | | | |
|  | | | | | | | | | | |
|  | | | | | | | | | | |
| 1. Ведётся ли база событий оперрисков | | | | | | | | | | |
|  | | | | | | | | | | |
| Да, в соответствии с 716-П  Да, по иной методике (включая возмещение)  Да, по иной методике (только события/убытки, без возмещения)  Нет | | | | | | | | | | |
|  | | | | | | | | | | |
|  | | | | | | | | | | |
| 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 для соответствия 716-П  Аудит соответствия требованиям главы 7 716-П (риски ИС)  Разработка необходимой организационно-распорядительной документации для соответствия главы 7 716-П (риски ИС)  Аудит соответствия требованиям главы 8 716-П (риски ИБ)  Разработка необходимой организационно-распорядительной документации для соответствия главы 8 716-П (риски ИБ)  Аудит соответствия требованиям главы 7 и 8 716-П (риски ИС и ИБ)  Разработка необходимой организационно-распорядительной документации для соответствия главы 7 и 8 716-П (7 и 8 716-П)  Разработка модели угроз по новой методике ФСТЭК  Аудит организации в направлении обработки/защиты персональных данных  Тестирование на проникновение и анализа защищенности (пентест внешний/внутренний) | | | | | | | | | | |
|  | | | | | | | | | | |
|  | | | | | | | | | | |
| 1. Желаемый перечень сопутствующих работ | | | | | | | | | | |
|  | | | | | | | | | | |
| Проведение тестирования на проникновение и анализа защищенности  Анализ платежного ПО по ОУД4  Разработка модели угроз по новой методике ФСТЭК  Аудит на соответствие требованиям 719-П, 683-П, 747-П, иных источников требований ЦБ/Приведение в соответствие требованиям 719-П, 683-П, 747-П, иных источников требований ЦБ  Аудит на соответствие требованиям ГОСТ 57580/Приведение в соответствие требованиям ГОСТ 57580 | | | | | | | | | | |
|  | | | | | | | | | | |
|  | | | | | | | | | | |
| 1. Желаемый перечень иных работ | | | | | | | | | | |
|  | | | | | | | | | | |
| Аудит организации в направлении обработки/защиты персональных данных  Аудит степени выполнения 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»  Независимая внешняя оценка SWIFT | | | | | | | | | | |
|  | | | | | | | | | | |
|  | | | | | | | | | | |
| 1. Поставка технических решений (ПО, ПАК, оборудование) ИБ/ИТ | | | | | | | | | | |
|  | | | | | | | | | | |
| Планируется ли поставка решений ИБ/ИТ?  Требуется ли консультация по вопросам поставки и внедрения решений ИБ/ИТ? | | | | | | | | | | |
|  | | | | | | | | | | |
| Какие решения по ИБ/ИТ вами рассматриваются? | | | | |  | | | | | |
|  | | | | | *Указать* | | | | | |
|  | | | | | | | | | | |
|  | | | | | | | | | | |

Благодарим за уделенное время!