Практика оценки соответствия Положению Банка России № 382-П. Спорные вопросы и способы их решения. Взгляд аудитора

Информзащита
Системный интегратор

Об оценке

- ЗАО НИП «ИНФОРМЗАЩИТА» провела в декабре 2013 года оценку соответствия Банка «Возрождения» требованиям Положения Банка России № 382-П.
- Оценка проведена за **20 рабочих дней**.
- Группа оценки включала **9 человек**:

  - Руководитель проекта,

  - Руководитель группы оценки (Сертифицированный ABISS аудитор)

  - Аудиторы.
- В Банке «Возрождение» (ОАО) значение качественной оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств - **«хорошая»**.

Информзащита
Системный интегратор

Статистика

Распределение итоговых оценок по 382-П среди **всех** проектов ЗАО НИП «ИНФОРМЗАЩИТА»

*(прецедент: устранить за **10 рабочих дней при оценке 0,25**)*

Информзащита
Системный интегратор

Причины спорных ситуаций

- Неопределенность в формулировке некоторых требований и методов проверок

Банк старается получить более высокие обоснованные со своей стороны оценки

?

Аудитор, соблюдая этику, стремится найти как можно больше несоответствий

- Банк может оказаться не готовым к выполнению требований, в связи с технологическими, бизнес или иными ограничениями, например,

- технологические ограничения при реализации двухсторонней аутентификации участников платежного обмена;

- организационные проблемы внедрения ролевого доступа;

- сложности политического характера, при информировании ОПС о произошедших инцидентах.

Информзащита
Системный интегратор

Что проверять?

- Область действия Положения явно определена, но Область оценки часто вызывает споры

Проводить ли оценку на всей Области действия?

Если нет, то какую при этом делать выборку, какой % выборки будет репрезентативным?

Какой подход использовать для определения выборки

от ПС к информационным ресурсам или от типов платежной информации к ПС?

Решение

- Выборка не менее 10% платежных ИС:

- разных ПС, обязательно отечественные и иностранные

- системозначимые ИС, которым присущи критичные для организации риски (например, АБС)

- попадают ИС, которым свойственно большое количество рисков (процессинговые ИС, ДБО)

- Администрируют разные подразделения

- PCI DSS не равно 382-П

Информзащита
Системный интегратор

Как проверять?

- Какие свидетельства достаточны для подтверждения факта выполнения требования? Положение 382-П определяет категории проверки, но не детализирует метод проверки. **Интервью администратора достаточно?** Или необходимо проанализировать конфигурацию? Каких методов проверки достаточно: анализ документальных свидетельств, интервью, анкетирование, наблюдение?

Решение

- Инструкция от Регулятора по проведению Оценки, с указанием Необходимых и Достаточных свидетельств выполнения каждого требования. Пример такого документа представлен PCI Консулом, для стандарта PCI DSS.
- В отсутствии подобной инструкции рекомендуем пользоваться методиками ЦБ РФ для Комплекса СТО БР, при этом придавая Методу проверки «Интервью» наименее значимый вес при оценке выполнения

Информзащита
Системный интегратор

Как проверять?

- Нужно ли выполнять требования Положения для систем, введенных в действие за долго до появления ФЗ-161 «О НПС»?
- Можно ничего не делать и оставить ИС без документированной подсистемы ЗИ? Или необходимо Описать функционал по ЗИ «AS IS», в текущем виде? Как это сделать, если на Разработчик не готов предоставить «эксплуатационную документацию за давностью лет»?
- «Закон обратной силы не имеет»

Решение

- Понять какие риски регулятор предлагает закрыть данным требованием. Если в Банке не описаны принципы функционирования подсистемы ЗИ, обеспечивающей безопасность платежной ИС, как мы сможем оценить насколько правильно и эффективно работает эта подсистема?
- Разработать Эксплуатационную документацию на «старые системы».

Как оценивать?

- Есть особенности оценки, если Банк одновременно является ОПДС и ОУПИ (операционный центр, платежный клиринговый центр и расчетный центр). Есть особенные требования только по одной роли (например требование № 2.6.3 распространяются только на ОПДС

Решение

- *ПС -> Роль -> ИС, обеспечивающая выполнение Роли -> оценка требований для данной ИС*

- Как совмещать оценки? Оценивать отдельно, как оператора по ПДС и ОУПИ, или «распространять» оценку для ОПДС на ОУПИ, поскольку, как правило ОУПИ является всегда и ОПДС?

Решение

- *Требование -> в ИС (ОУПИ) выполняется, но в ИС (ОПДС) не выполняется –> Требование выполняется не в полном соответствии или почти полном*

Информзащита
Системный интегратор

Требование или Категория

- 2.9.3. В случае применения СКЗИ ОПДС …. определяют во внутренних документах **и выполняют** порядок применения СКЗИ, включающий …… (Категория проверки – 2 **документирование**)
- 2.6.5 Приняты ли и **зафиксированы ли во внутренних документах решения о необходимости** применения организационных или технических мер контроля физического доступа …… (Категория проверки – 3 **выполнение**)

Решение

- Необходимо определить какие риски закрывает требование. Если документированности недостаточно, то оценивать также и степень Выполнения. При адекватной аргументации такого подхода у Банка не возникает противоречий.

Категория 1	Документирование и Выполнение
Категория 2	Документирование
Категория 3	Выполнение

Детализация требований

- 2.7.5. В случае обнаружения вредоносного кода …ОПДС …. **обеспечивают информирование оператора платежной системы**

Кто, кому, в каких случаях, какие сведения отправляет? Если в Правилах ПС не определен порядок выполнения требований (например, вопросы взаимодействия участников ПС), кто будет отвечать за их невыполнение: ОПДС или сам ОПС? Сведения об инцидентах, уязвимостях, угрозах и т.д. носят конфиденциальный характер. *Как ими обмениваться? Кто устанавливает порядок обмена? Если ОПС выдвинет неадекватные требования по предоставлению информации, которой Банк не готов делится?*

Решение

- 2.13.1 «…ОПС определяет требования к порядку, форме и срокам информирования…»
- УКАЗАНИЕ ЦБ РФ от 9 июня 2012 г. N 2831-У содержит

Методику составления отчетности

Информзащита
Системный интегратор

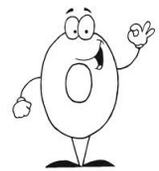
Детализация требований

- 2.17.2. «….ОПДС…. **регламентируют порядок принятия мер**, направленных на совершенствование защиты информации при осуществлении переводов денежных средств…» Какова детализация регламентирования? Банк может настаивать на Достаточности документирования только Требования в формате «Банк должен….» без описания порядка действий. Т.е. документирование только на уровне Политики. Документы 2 и 3 уровня отсутствуют.

Решение:

- Смысловая нагрузка слова «Порядок» подразумевает детализированное описание – документ 2-3 уровня. Во время оценки, проводятся дополнительные разъяснения.

- В Организации не регламентирована фактически реализуемая процедура. Тогда выполнение требования 382-П оценивается **нулевым** значением



Информзащита
Системный интегратор

Выводы

- Острых проблем при оценке требований Положения 382-П **нет**. Есть спорные вопросы.
- В крупных Банках, таких как Возрождение, многие процессы уже были документированы и реализованы еще до появления ФЗ-161. Тогда основной задачей становиться осуществление сбора свидетельств для регулятора. Это задача построения системы контролей.
- Ожидаем совершенствования требований 382-П, с учетом пожеланий, в первую очередь, самих участников НПС.
- Мы предлагаем разработать комплексный подход к оценке с учетом требований СТО БР и уточнить Методику проведения оценки, в части методов проверки.

Плетнев Леонид
CISM, CISA, PCI QSA
Департамент консалтинга и аудита
Компании ИНФОРМЗАЩИТА
☎ +7(495) 980-2345
☎ +7(926) 411-4100
✉ l.pletnev@infosec.ru
www.infosec.ru

Информзащита
Системный интегратор