deiteriy compliance

Аутсорсинг: выполнение требований ИБ и прохождение оценок соответствия

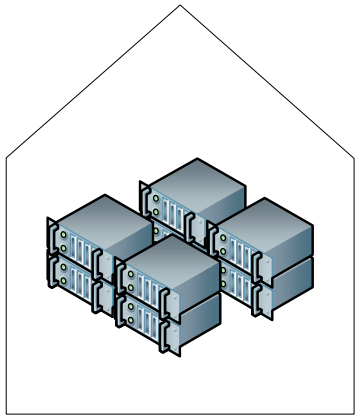
АЛЕКСАНДР ИВАНЦОВ | DEITERIY COMPLIANCE | КОНФЕРЕНЦИЯ АБИСС 2023

Аутсорсинг в финансовых организациях

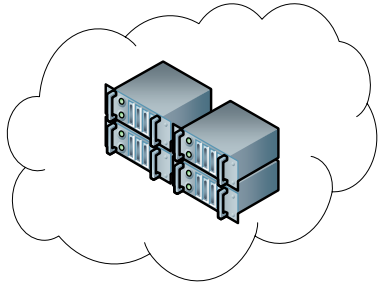
- На данный момент в НПА ЦБ нет требований при взаимодействии и порядка взаимодействия с поставщиками услуг. Требования появляются в ГОСТ 57580.3 и в запланированном ЦБ документу по аутсорсингу.

- Вопрос аутсорсинга актуален и до вступления данных НПА в силу. Перед кредитными организациями стоит задача обеспечить безопасность и комплаенс при взаимодействии с поставщиками услуг.

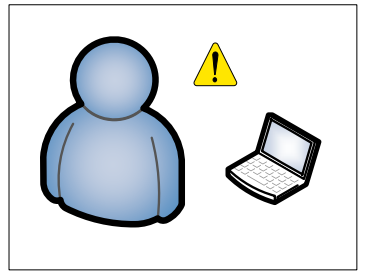
Поставщики услуг



ЦОД

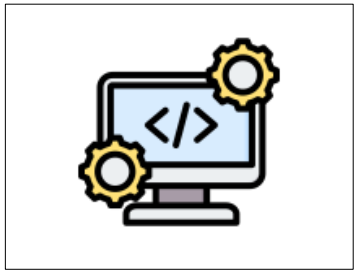


Облачный
хостинг



SOC

SaaS
(ПО как сервис)



Разработка ПО

Безопасность и комплаенс

- Безопасность
  - При взаимодействии с поставщиками услуг риски ИБ остаются актуальными.
  - Риск должен быть обработан на том же уровне, как если бы это делала сама организация.
- Комплаенс
  - Необходимо убедиться, что риск обработан на необходимом уровне.
  - Необходимо убедить проверяющих, что этого достаточно.

Начать нужно с вопросов

1. Как поставщик влияет на безопасность?

2. Как обработать данные риски?

3. Как убедиться, что риски обработаны, если они в зоне ответственности третьей стороны?

Разработчики ПО

1

Вендор, поставляющий ПО и обновления к нему

2

Внешний разработчик, разрабатывающий ПО под нужды компании

3

Своя команда разработки в той же или дочерней организации

Зона ответственности

1. Процесс безопасной разработки (ЖЦ)

2. Безопасность среды разработки и тестирования (СМЭ)

3. Защита исходного кода (защищаемая информация)

4. Обеспечение целостности при передаче исходного кода или пакетов обновлений и деплое (ЦЗИ)

Способ подтверждения соответствия – анализ уязвимостей по требованиям к оценочному уровню доверия (ОУД)

Хостинг провайдеры и SaaS

	Co-location	Облако	Облако +	SaaS
Уровень прикладного ПО	АБС	АБС	АБС	АБС
Уровень промежуточного ПО	Вспомогательное ПО	Вспомогательное ПО	Вспомогательное ПО	Вспомогательное ПО
Уровень ОС	ОС	ОС	ОС	ОС
Уровень APM и серверов	VM Серверное оборудование	VM Серверное оборудование	VM Серверное оборудование	VM Серверное оборудование
Уровень сети	Сетевые устройства	Сетевые устройства	Сетевые устройства	Сетевые устройства
Физический уровень	Серверное помещение	Серверное помещение	Серверное помещение	Серверное помещение

Зона ответственности SOC

1. Мониторинг и анализ событий ИБ (МАС)

2. Информирование, участие в регистрации и расследовании инцидентов ИБ (РИ)

3. Защита и ограничение доступа к хранящимся событиям ИБ (РИ)

Разделение ответственности

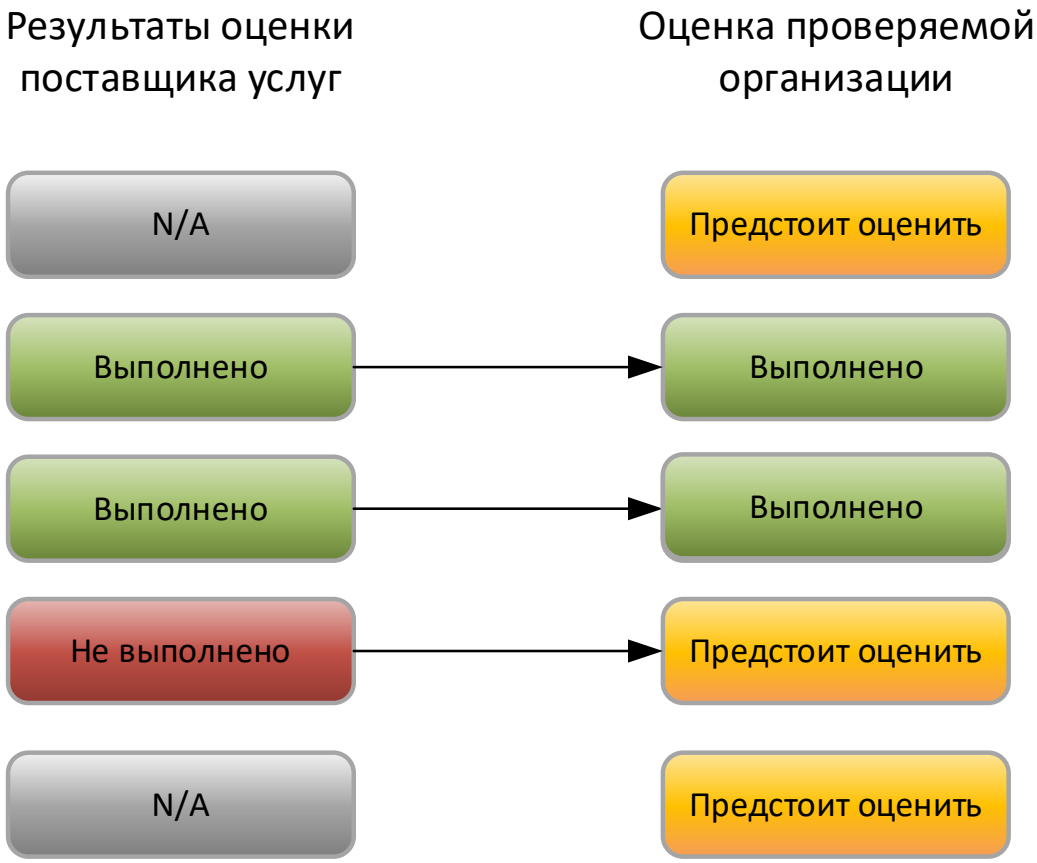
- Для определения границы и разделения ответственности за обеспечение ИБ можно составить матрицу ответственности.

Требование	Клиент	Поставщик услуг
…	…	…
ФД.13 Контроль доступа к серверному и сетевому оборудованию, расположенному в запираемых серверных стоечных шкафах	Для собственных помещений	Для арендуемых помещений
…	…	…

Аудит: учет соответствия третьей стороны

- AOC PCI DSS:
  - Сертифицированные бизнес-процессы и услуги.
  - Набор выполненных требований.
- ГОСТ 57580:
  - (не регламентировано)

- Сложившаяся практика – привлечение поставщика в рамках аудита или перезачет требований из результатов оценки третьей стороны.



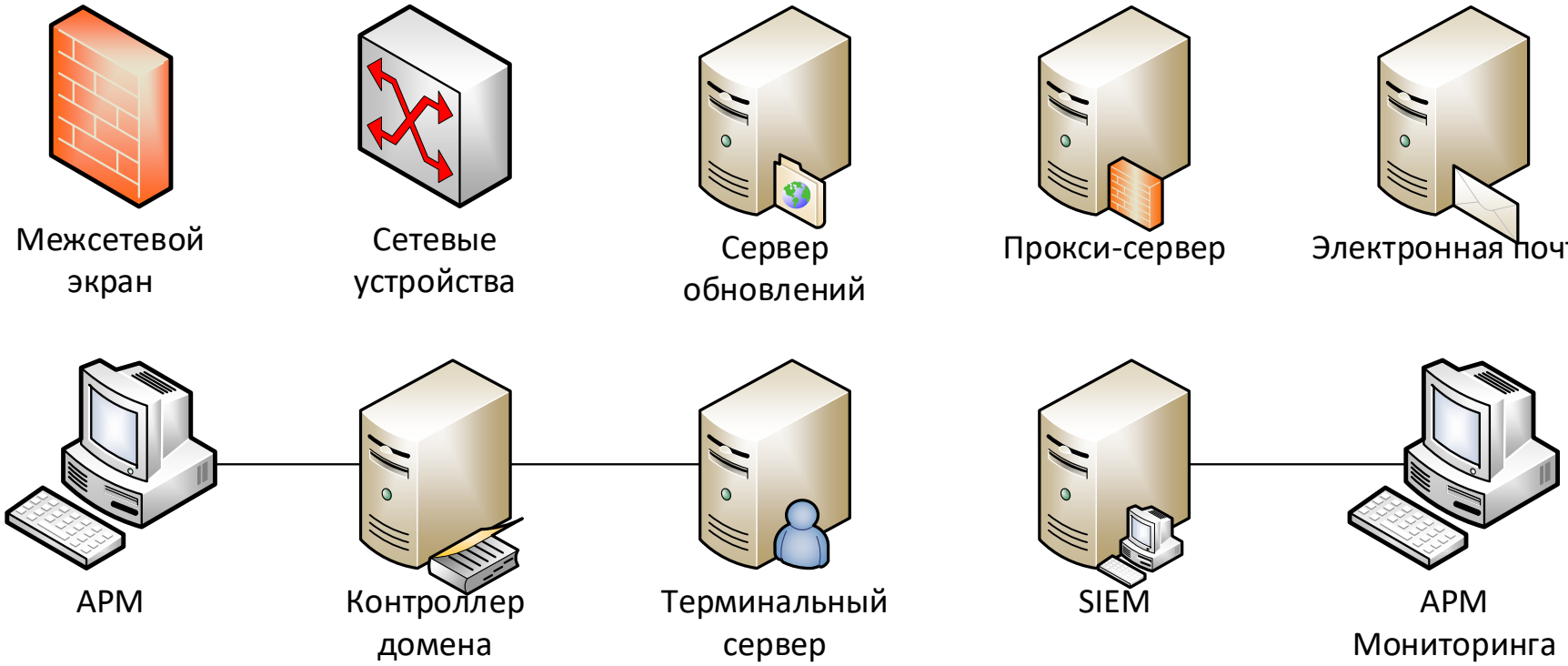
Вопросы

1. Полностью ли применять стандарты к поставщикам, или только в части требований в их зоне ответственности?

---

2. Какой информации достаточно для подтверждения соответствия поставщика?

Область применимости стандарта



Полнота применения требований

Процесс ГОСТ 57580.1	ЦОД	SOC
Процесс 1 «Обеспечение защиты информации при управлении доступом»		
Управление учетными записями и правами субъектов логического доступа	-	?
Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа	-	?
Защита информации при осуществлении физического доступа	+	?
Идентификация, классификация и учет ресурсов и объектов доступа	-	?
Процесс 2 «Обеспечение защиты вычислительных сетей»		
Сегментация и межсетевое экранирование вычислительных сетей	-	?
Выявление сетевых вторжений и атак	-	?
Защита информации, передаваемой по вычислительным сетям	-	?
Защита беспроводных сетей	-	?
Процесс 3 «Контроль целостности и защищенности информационной инфраструктуры»	-	?
Процесс 4 «Защита от вредоносного кода»	-	?
Процесс 5 «Предотвращение утечек информации»	-	?
Процесс 6 «Управление инцидентами защиты информации»		
Мониторинг и анализ событий защиты информации	-	+
Обнаружение инцидентов защиты информации и реагирование на них	-	+
Процесс 7 «Защита среды виртуализации»	-	?
Процесс 8 «Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств»	-	?
Защита информации на этапах жизненного цикла автоматизированных систем и приложений	-	?

Раскрытие результатов оценки

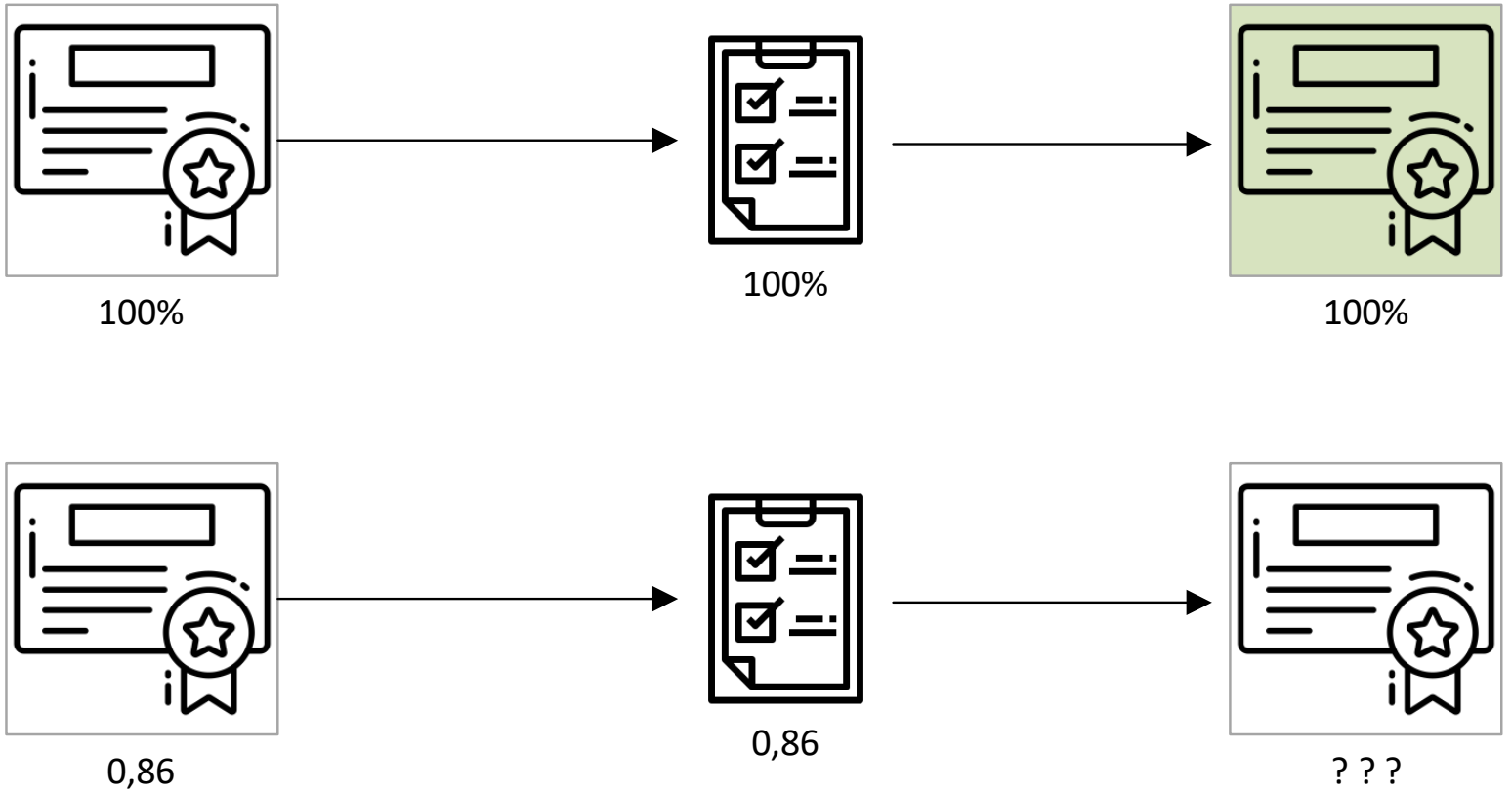
- Первый вариант:
  - Раскрытие итоговой оценки

0,86

- Второй вариант:
  - Полная информация о выполнении каждого требования

…	…
ФД.10 Оборудование помещений средствами (системами) контроля и управления доступом	-
ФД.13 Контроль доступа к серверному и сетевому оборудованию, расположенному в запираемых серверных стоечных шкафах	+
…	…

Раскрытие только итоговой оценки



Как могут быть описаны требования для провайдеров облачных услуг

Закрепленная роль «Поставщик услуг облачного хостинга» как в 161-ФЗ	Абстрактный «поставщик услуг»
Определенный набор критериев оказываемых услуг	Гибкий набор критериев, позволяющих сохранить актуальность в течение долгого времени
Четкий набор требований к деятельности	«Кирпичики», набор которых меняется в зависимости от процессов и влияния на безопасность
Соответствие требованиям ГОСТ 57580.1 по определенному уровню	Соответствие требованиям ГОСТ 57580.1 по уровню клиента

Выводы

1. ЦБ активно движется к регулированию вопросов обеспечения ИБ при аутсорсинге.

2. Не обязательно ждать появления всех НПА ЦБ, чтобы выстроить правильные процессы взаимодействия с поставщиками услуг.

3. Общие подходы обеспечения безопасности уже сформированы: обработка рисков ИБ и определение границ ответственности.

4. С точки зрения обеспечения комплаенса разные бизнес-процессы требуют индивидуального подхода.

Спасибо за внимание!