

От In-house модели к MSSP

ПАО «МТС-Банк» 02.2018

Назаров П.В.

Начальник Управления Информационной Безопасности

- **Предпосылки**
- Риски
- Выбор и принятие решения
- Подводные камни при переходе



Угрозы



СТОИТ ЗАДУМАТЬСЯ:

- Недостаток собственной экспертизы
- Нехватка и сложность подбора узкоспециализированного персонала
- Требование 24/7/365
- Сжатые сроки на реализацию
- Необходимость наращивания мощностей
- Большая гибкость при реализации (независимость от внутренней политики)

Направления
развития
бизнеса



МИФЫ

1

Уменьшения затрат
может и не быть

2

Срок на запуск =
обещания X 3



3

Аутсорсеры могут не быть
более квалифицированы,
чем свои

4

Отдать можно всё



MSSP – это только про операционные процессы:

- security monitoring
- infrastructure monitoring
- vulnerability monitoring

Governance – **ВСЕГДА IN-HOUSE**

- Предпосылки
- **Риски**
- Выбор и принятие решения
- Подводные камни при переходе



Регуляторный риск

- Как относятся регуляторы, особенно в области безопасности, к аутсорсу?
- Что нельзя отдавать с точки зрения регулятора?
- **Контролировать область и контент**

Риск доверия к аутсорсеру

- Quis custodiet ipsos custodes?
- **Сертификация, независимые референсы, дополнительные внутренние меры контроля, финансовые гарантии**

Финансовый риск

- Неправильно составленная финмодель
- **Считать всё, знать, что включать в score**

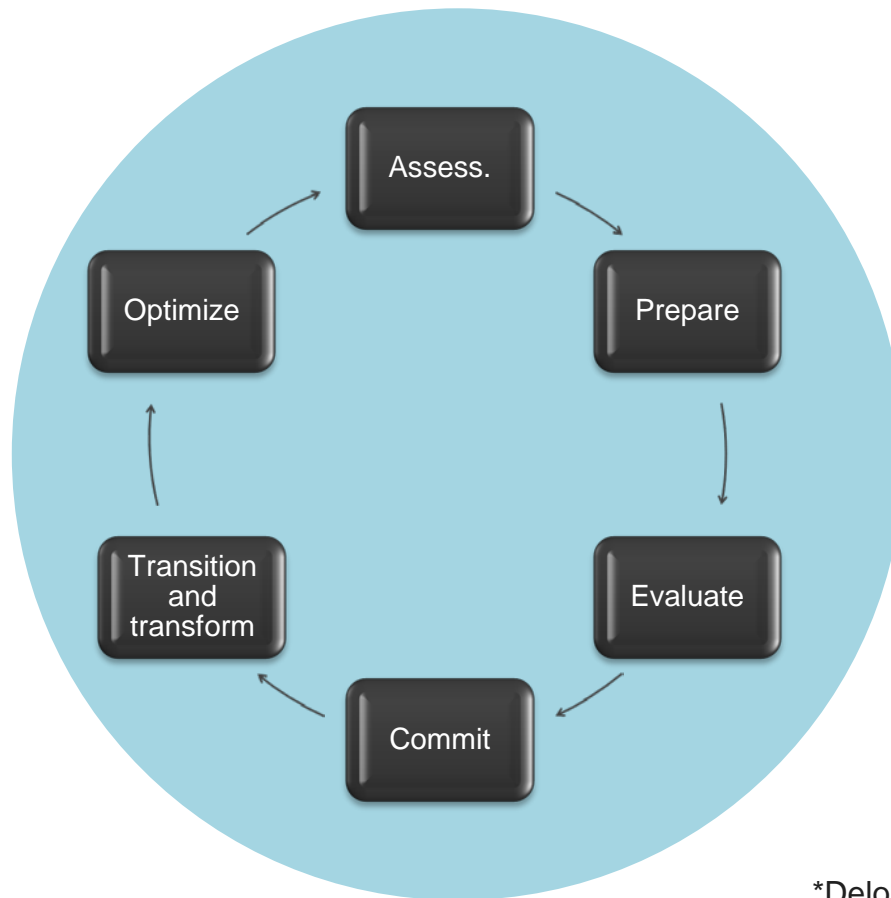


Никакой аутсорсер никогда не будет нести полный риск, связанный с потерями от инцидентов

- Предпосылки
- Риски
- **Выбор и принятие решения**
- Подводные камни при переходе



Модель перехода



Assess: define aims, objectives, scope, stakeholders, risks, costs	Commit: contract development and finalization
Prepare: service level, RFP	Transition and transformation: implementation
Evaluate: response evaluation and supplier selection	Optimize: on-going management



В процессе важно понять: single или multi сервисная модель, гибридная модель или полный аутсорс



Ресурсная модель
оценки

- Портфель процессов и сервисов, с указанием расчетов стоимостей по внутренней реализации и передаче аутсорсеру, сравнение затрат.

Проектная модель
оценки

- Оценивается как инвестиционный проект. NPV, IRR



Если рассматривать только процесс ИБ, в отрыве от бизнес/ИТ составляющей, результат может быть отрицательным.



- Предпосылки
- Риски
- Выбор и принятие решения
- **Подводные камни при переходе**



1

Не учитывается факт, что нужно трансформировать и подготовить внутренние процессы.

2

Настроить связь MSSP с ИТ

3

Неправильно определён score, не определена модель управления.

4

Нехватка ресурсов для управления изнутри.

5

Неправильно определён SLA в обе стороны

6

Как правило, расходы операционные, не капитализируемые

СПАСИБО ЗА ВНИМАНИЕ!
ВОПРОСЫ?

