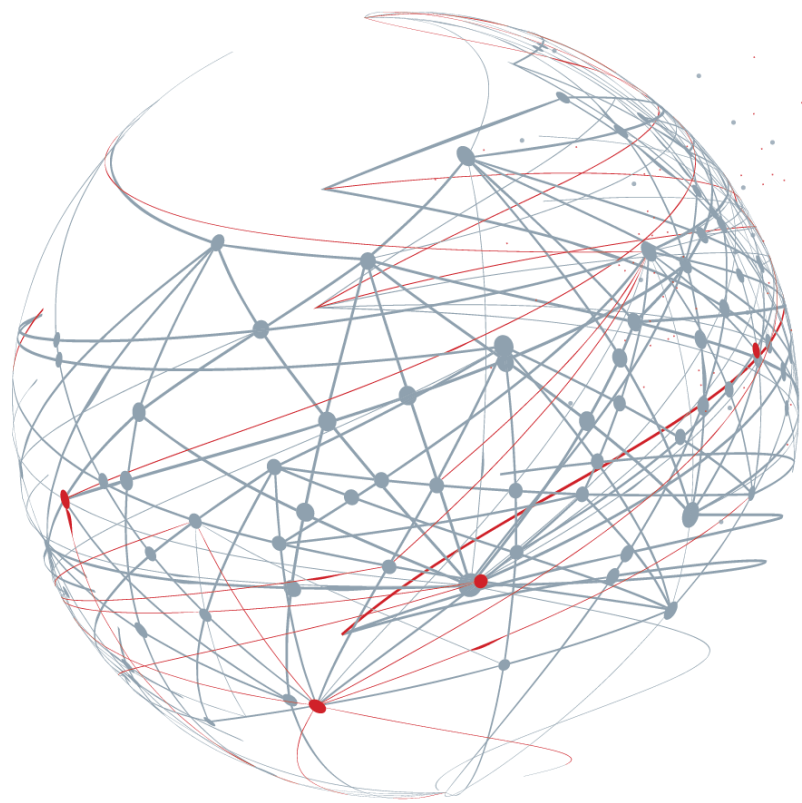


The logo consists of a red square with a white 'L' shape cutout on the left side. The letters 'MOEX' are written in white, bold, sans-serif font within the red area.

MOEX

**МОСКОВСКАЯ
БИРЖА**



**ПОДХОД К ОЦЕНКЕ
ПРОЦЕССОВ ОБЕСПЕЧЕНИЯ
НЕПРЕРЫВНОСТИ БИЗНЕСА
МОСКОВСКОЙ БИРЖИ**

СОДЕРЖАНИЕ:

1

Почему важно
проверять

стр. 3 – 8

2

Применяемый
подход

стр. 10 – 13

3

Привлечение
внешней
экспертизы

стр. 15

Биржа – критичный элемент финансовой системы РФ

Группа «Московская Биржа» является крупнейшим российским биржевым холдингом, управляющим единственной в России многофункциональной биржевой площадкой по торговле акциями, облигациями, производными инструментами, валютой, инструментами денежного рынка, углеродными единицами, драгоценными металлами и агропродукцией

В состав Группы входят:

Московская Биржа Фондовый рынок Денежный рынок Срочный рынок Валютный рынок Рынок драгметаллов	Товарная биржа (НТБ) Рынок зерна, сахара и др. Углеродные единицы	№1 в РФ 5 000 инвестиционных продуктов	1,3 квдрлн руб. объем торгов в 2023
НКЦ Клиринговый центр Центральный контрагент на всех рынках	МБ Инновации Развитие инновационных технологий Сотрудничество с финтехстартапами	> 300 профучастников работают на рынках на Московской Бирже	> 150 корпоративных клиентов, имеющие прямой доступ ¹
НРД Центральный депозитарий Расчетный центр Регистратор финансовых транзакций	МБ Защита информации	33,3 млн частных инвесторов	>5 трлн руб. ежегодно привлекают компании РФ за счет выпуска акций и облигаций на Московской Бирже

и др.

1. Без учета страховых, НПФ, УК, нерезидентов, которые имеют доступ к рынку депозитов и валютному рынку напрямую (ранее относились к общей категории корпораты)

Сложность торговых платформ (ТКС) и инфраструктуры

180 млн

транзакций на **каждом** из трех основных рынков в волатильные дни

50 млн

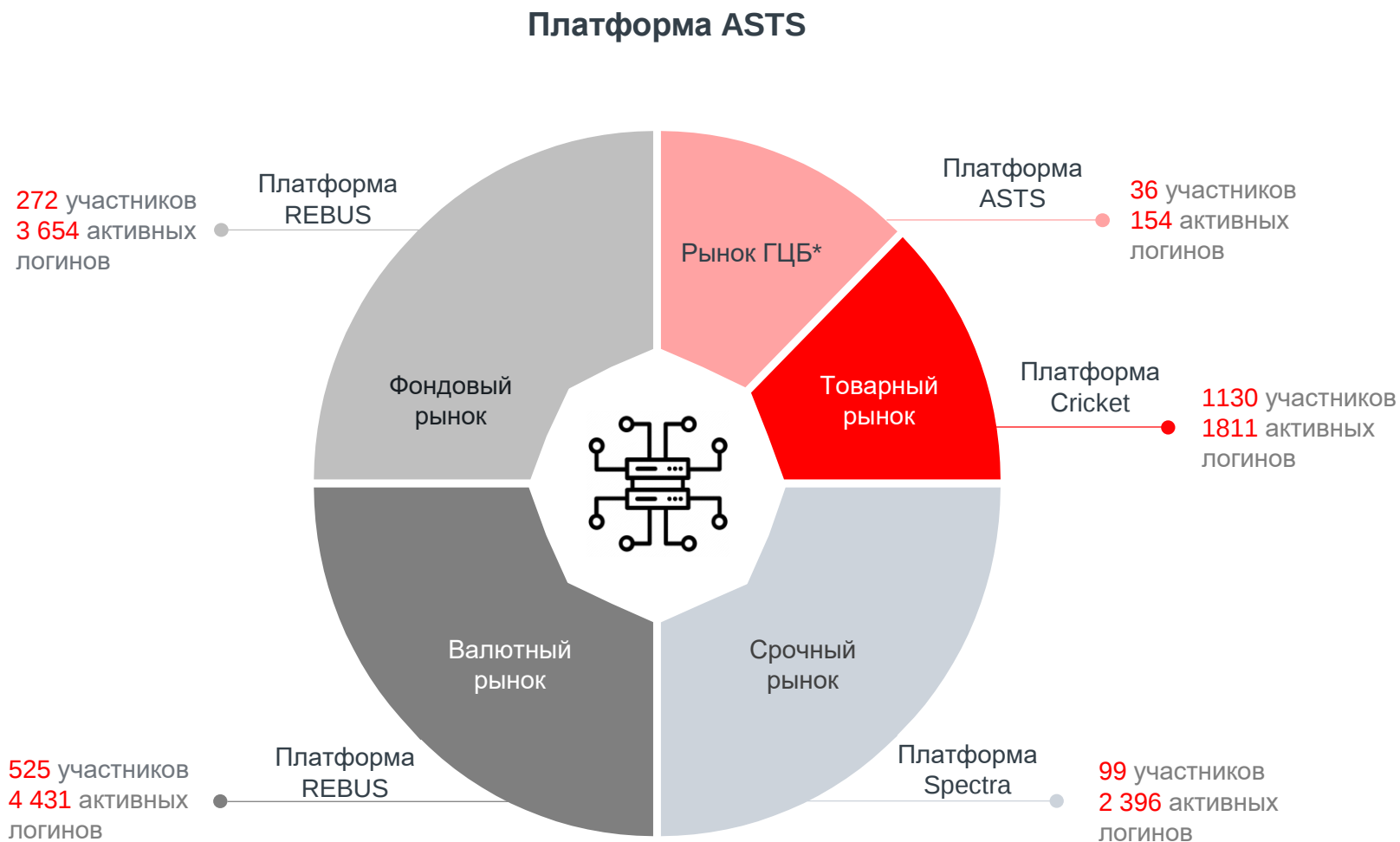
транзакций на **каждом** из трех основных рынков в обычные дни

~ 500

серверов под все платформы в прод среде (+ идентичные бою полигоны)

~ 400

серверов под все платформы в тестовых средах (функциональные, интеграционные, игровые, UAT и т.д.)



Непрерывность бизнеса

Обеспечение непрерывности бизнеса (далее ОНБ) – стратегическая и тактическая способность организации по планированию своих действий и реагированию на случай возникновения чрезвычайных ситуаций, влекущих за собой нарушение нормального хода деятельности, с целью продолжения выполнения операций и взятых на себя обязательств на определенном уровне.

КЛЮЧЕВЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОСТИ

1. ОРГАНИЗАЦИЯ/ПРОЦЕССЫ
2. АРХИТЕКТУРА ИТ-СИСТЕМ
3. ИТ-ИНФРАСТРУКТУРА

ЗАДЕЙСТВОВАННЫЕ ПОДРАЗДЕЛЕНИЯ

1. НАПРАВЛЕНИЕ ОНБ
2. ЭКСПЛУАТАЦИЯ ИТ
3. УПРАВЛЕНИЕ РИСКАМИ
4. БИЗНЕС-ПОДРАЗДЕЛЕНИЯ
5. ВСЕ СОТРУДНИКИ

АНАЛИЗ ВЛИЯНИЯ НА БИЗНЕС (АВБ)

АВБ/ВИА – оценка последствий возможного нарушения функционирования бизнес-процессов организации в количественном и качественном выражении в динамике по времени и определение ресурсов, необходимых для их выполнения в случае нарушения режима штатного функционирования

По итогам АВБ определяются уровни критичности всех процессов Биржи:

- ▶ MISSION CRITICAL (MC)
- ▶ BUSINESS CRITICAL (BC)
- ▶ BUSINESS OPERATIONAL (BO)
- ▶ BUSINESS SUPPORTING (BS)
- ▶ DO NOT RECOVER (NR)

Критичность зависимых процессов определяет критичность ИТ-систем:

- ▶ 1A – Real-time, Mission Critical (ТКС)
- ▶ 2A – Mission Critical (около-ТКС)
- ▶ 3A – Business Critical (отчетность)
- ▶ B – Business Operational (ITSM, 1C)
- ▶ C – Business Supporting (E-mail)

Критерии непрерывности

Архитектура ТКС

Критерии состояния архитектуры ТКС, влияющие на непрерывность:

Отказоустойчивость	Доступность
Катастрофоустойчивость	Производительность
Обеспечение целостности и корректности данных	Организация развития
Обеспечение доставки данных	Наличие и качество техподдержки системы
Масштабируемость	Адаптация / устойчивость к изменениям
Технологический стек	Качество документации

ИТ-инфраструктура

Характеристики объектов инфраструктуры, влияющие на непрерывность:

Срок эксплуатации	Поддержка	Запчасти
End-of-life	Мониторинг	Актуальность ПО

Процессы

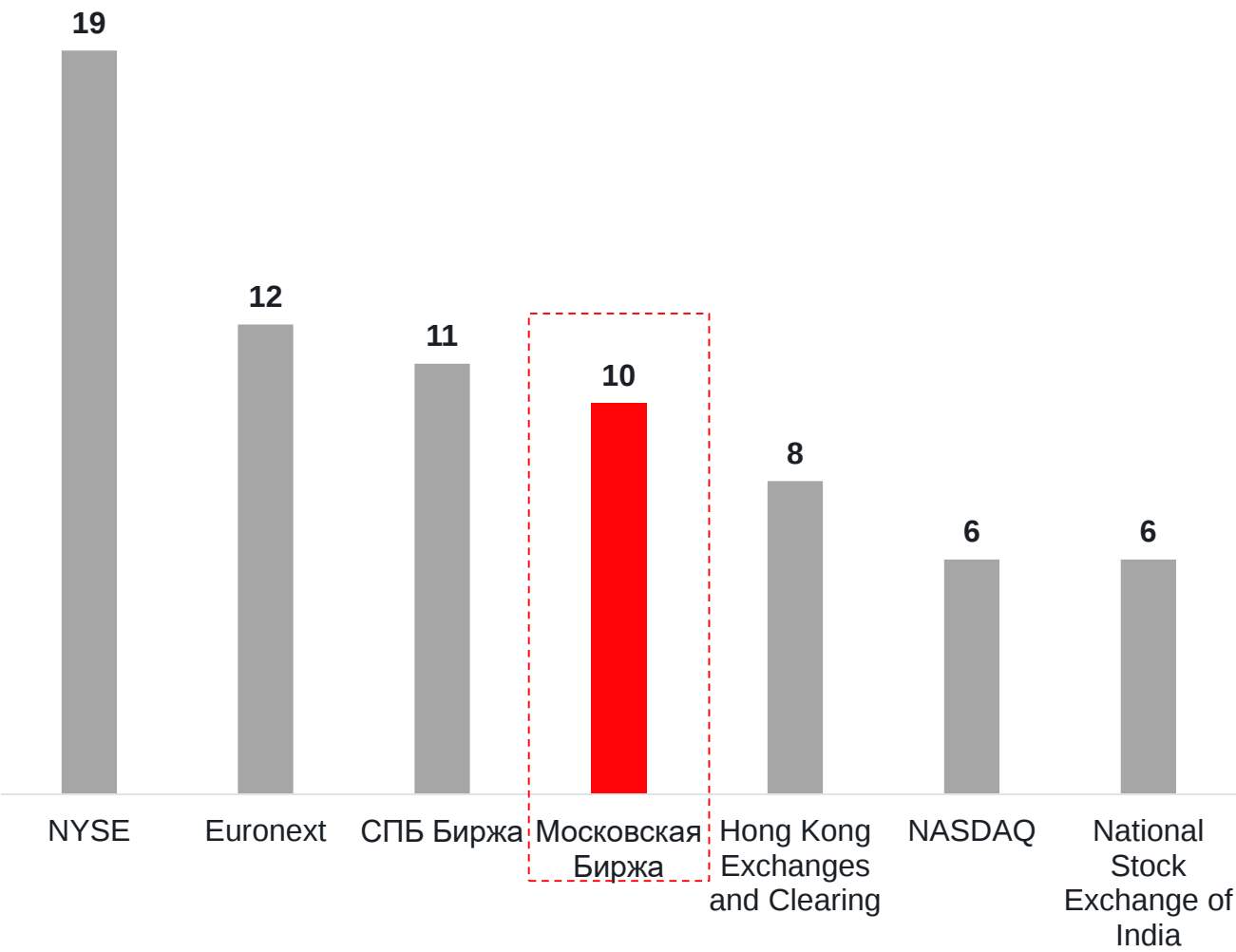
Критерии оценки управления непрерывностью:

Стратегическое целеполагание в области непрерывности	Соответствие организационных и технологических мер задокументированным процедурам
Полнота и актуальность структур и команд BCP/DRP*	Обучение персонала
Обучение и подготовка персонала, обеспечивающего BCP/DRP	Охват тестирования BCP/DRP (план)
Полнота и актуальность методологического обеспечения в области BCP/DRP	Тестирование BCP/DRP (факт)
Наличие, полнота и актуальность метрик в области BCP/DRP	Интеграция ИТ-процессов с процессами управления непрерывностью

* BCP – планирование непрерывности деятельности (Business Continuity Planning), DRP – планирования аварийного восстановления (Disaster Recovery Planning)

Значение непрерывности бизнеса для биржи

Количество сбоев с 2016 по 2023



Общие регуляторные рекомендации и требования в области обеспечения непрерывности бизнеса

- Рекомендации и 2 Положения Банка России
- 2 ФЗ, 2 постановления Правительства РФ и постановление Правительства Москвы
- Международные стандарты и лучшие практики

ЦЕЛЕВЫЕ ПОКАЗАТЕЛИ ДОСТУПНОСТИ	ПОРОГ
Доступность систем реального времени, %	99,97
Доступность систем, обеспечивающих прочие клиентские сервисы, %	99,90

Новые вызовы и меры противодействия

Вызовы	Меры противодействия	
› Повышение вероятности реализации киберугроз, включая увеличение количества DDoS атак	• Импортозамещение системы защиты от DDOS атак на уровне инфраструктуры • Закупка дополнительных каналов с защитой от DDOS на уровне провайдеров • Внедрение защиты от DDOS WEB ресурсов на уровне WAF (Web Application Firewall)	
› Угроза отключения РФ от системы SWIFT	• Проработка альтернативных каналов связи с банками-корреспондентами, участниками клиринга • Наличие альтернативного Сервис-Бюро SWIFT (при отключении от SWIFT НРД) • С 01.10.2023 все платежи в рублях внутри страны проходят через СПФС • Разработка роботизированных схем обмена финансовыми сообщениями по альтернативным каналам связи	
› Уход с российского рынка поставщиков телекоммуникационного и ИТ оборудования, средств обеспечения ИБ	• Формирование списка ПО с ранжированием по уровню критичности, сроков и риска прекращения его функционирования, составление плана по импортозамещению и его реализация	
› Угроза военных действий	• Расширение программы тренингов и учений по восстановлению деятельности • Закупка дополнительных резервных каналов связи	
› Угроза террористических атак, в т. ч. беспилотными летательными аппаратами		
› Возможность мобилизации работников		
› Угроза включения РФ или компаний Группы в санкционные списки (FATF, SDN) – <i>реализовалась: МБ, НКЦ, НРД включены в SDN</i>	• Поддержание актуальности планов восстановления и противодействия финансовым угрозам • Проведение тренингов и учений по реализации планов	• Планы успешно реализованы, последствия реализации угрозы минимизированы

СОДЕРЖАНИЕ:

1

Почему важно
проверять

стр. 3 – 8

2

Применяемый
подход

стр. 10 – 13

3

Привлечение
внешней
экспертизы

стр. 15

Как проводятся аудиты непрерывности

Периодичность тематической комплексной оценки процесса управления непрерывностью - не реже 1 раза в 2 года

Дополнительно вопросы непрерывности проверяются при проверках других направлений, например:

Оценка соответствия внешним и внутренним требованиям осуществляется с учетом:

- аудиты управления и стратегического планирования ИТ – на предмет учета вопросов непрерывности и надежности при формировании стратегических целей ИТ
 - аудиты ключевых систем – на предмет полноты и корректности применяемых к системам мер обеспечения непрерывности
 - аудиты кибербезопасности – на предмет влияния угроз ИБ на непрерывность деятельности
 - аудиты бизнес-процессов – на предмет качества проведения BIA, своевременности проведения DR-тестирования поддерживающих систем
-
- фактического дизайна процессов и уровня остаточного риска с учетом внедренных контрольных процедур
 - утвержденного Набсоветом Биржи риск-аппетита
 - анализа реализовавшихся за период угроз и рисков событий
 - уже существующих планов по развитию направления

Компоненты непрерывности

КЛЮЧЕВЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОСТИ:

ТИПИЧНЫЕ ОШИБКИ И ПРОБЛЕМЫ

ОРГАНИЗАЦИЯ/ПРОЦЕССЫ	АРХИТЕКТУРА	ИТ-ИНФРАСТРУКТУРА
- Неполнота карты угроз - Неактуальные планы восстановления - Отсутствие ситуационного или кризисного центра - Низкий уровень зрелости ИТ-процессов - Отсутствие единой системы мониторинга «Человеческий фактор» и недостаточность ресурсов	- Технический долг (временные ИТ-решения, устаревшее ПО) - Асинхронность систем, слабый клиентский сервис при отказе бэк-систем - Отсутствие распределения и балансировки нагрузки - Отсутствие резервных экземпляров ИТ-систем	- Недостаточность мощностей (ЦОД), отсутствие резервного ЦОД - Недостатки в организации сети (точки отказа) - Низкий уровень развития средств автоматизации - Слабая стандартизация - Несвоевременное обновление оборудования

Ключевые области проверок СВА

ОРГАНИЗАЦИЯ/ПРОЦЕССЫ

Оцениваемые области		Потенциальные недостатки	
	Управление системой менеджмента непрерывности бизнеса	>	Неполное или некорректное отражение показателей непрерывности в отчетности, несвоевременные корректирующие действия
	Управление рисками непрерывности деятельности	>	Неучтенные риски непрерывности, отсутствие планов по их митигации
	Взаимодействие между компаниями Группы	>	Невозможность своевременного восстановления взаимосвязанных процессов или систем компаний Группы
	Повышение осведомленности в области непрерывности деятельности	>	Недостаточная осведомленность работников о процедурах восстановления деятельности, невозможность возобновления процессов в требуемое время
	Контроль соблюдения регуляторных требований	>	Нарушение регуляторных требований, влекущее приостановку деятельности
	Оценка влияния на бизнес (АВБ/ВІА)	>	Некорректная оценка целевых показателей восстановления процессов или связанных систем, приводящая к невозможности своевременного восстановления
	Управление планами обеспечения непрерывности и восстановления деятельности	>	Отсутствие или недостаточная детализация планов восстановления, приводящая к увеличению времени или невозможности возобновления бизнес-процесса

Ключевые области проверок СВА

АРХИТЕКТУРА



- Управление резервным копированием информации и баз данных



- Неполное покрытие резервным копированием систем и их компонентов влечет потерю данных за пределами приемлемых порогов



- Техническое обеспечение функционирования основного и резервного ЦОД, офисов и мобильного офиса



- Неоптимальная архитектура локальных и гео-распределенных резервных контуров влечет невозможность бесшовного перехода на резервную инфраструктуру

ИТ-ИНФРАСТРУКТУРА



- Определение требований по управлению информационной инфраструктурой для обеспечения непрерывности



- Некорректно установленные требования к инфраструктуре даже при их выполнении не позволят своевременно восстановить системы и возобновить связанные процессы



- Оценка применения мер обеспечения непрерывности и надежности информационной инфраструктуры



- Установленные требования к инфраструктуре корректны, но фактически не выполняются, что не позволяет своевременно восстановить системы и возобновить связанные процессы



- Обеспечение функционирования каналов связи в целях обеспечения непрерывности деятельности



- Недостаточное оснащение резервного офиса влечет риск несвоевременного возобновления процессов, а недостаточное оснащение ЦОД – к полной невозможности восстановления
- Потеря связности ЦОД из-за нехватки пропускной способности или резервных каналов

СОДЕРЖАНИЕ:

1

Почему важно
проверять

стр. 3 – 8

2

Применяемый
подход

стр. 10 – 13

3

Привлечение
внешней
экспертизы

стр. 15

Привлечение внешней экспертизы

За 5 лет направление ОНБ комплексно оценивалось 3 раза - основной фокус в аудитах делался на организацию процесса
При этом существуют ограничения в виде отсутствия у СВА:

- экспертизы в области эксплуатации специализированных оборудования и технологий
- опыта построения архитектуры высоконагруженных систем
- доступа к базам знаний зарубежных вендоров

РЕЗУЛЬТАТ	ПРЕИМУЩЕСТВА	НЕДОСТАТКИ И ОГРАНИЧЕНИЯ
Комплексные рекомендации по критичным платформам в разрезе процессов (включая смежные), инфраструктуры и архитектуры с акцентом на технических аспектах ОНБ	▶ Техническая оценка надежности инфраструктуры и ИТ-систем ▶ Независимая оценка «свежим взглядом» ▶ Сравнение с применимыми рыночными практиками	▶ Высокая стоимость экспертизы ▶ Сложность адаптации лучших практик к специфике Компании ▶ Сложность глубокого погружения в уникальные процессы Группы и поиска релевантных объектов бенчмаркинга с учетом специфики требований к ТКС ▶ Разница в оценке критичности выявленных недостатков у консультантов и Компании

СПАСИБО
ЗА ВНИМАНИЕ