Приложение 3
к решению Правления
АО «Самрук-Казына»
от «07»августа 2012 г.
Протокол № 33/12

Методика
проведения аудита
информационных систем
в дочерних и зависимых организациях
АО «Самрук-Казына»

Содержание

1 Термины и сокращения

АО «Самрук-Казына» или Фонд	Акционерное общество «Фонд национального благосостояния «Самрук-Қазына»
Аутсорсинг (outsourcing)	Передача отдельных функций в управление внешней организации
ДЗО	Дочерние Зависимые Организации АО «Самрук-Казына»
ИБ	Информационная безопасность
ИКТ	Информационно коммуникационные технологии
ИТ	Информационные технологии
ИТ-аудит	Процесс оценки и подтверждения эффективности организации, управления и обеспечения безопасности ИТ инфраструктуры
ИС	Информационная система
СВА	Служба Внутреннего Аудита
KPMG	ТОО “КПМГ Такс энд Эдвайзори»"
CIA	Сертифицированный Внутренний Аудитор (Certified Internal Auditor)
CISA	Сертифицированный Аудитор Информационных Систем (Certified Information Systems Auditor)
CISM	Сертифицированный Менеджер Информационной Безопасности (Certified Information Security Manager)
CISSP	Сертифицированный Профессионал по Безопасности Информационных Систем (Certified Information Systems Security Professional)
CGEIT	Сертифицированный Специалист по Управлению ИТ (Certified in the Governance of Enterprise IT)
CRISC	Сертифицированный Специалист по Управлению ИТ Рисками (Certified in Risk and Information Systems Control)

2 Общие положения

Настоящий документ представляет собой методологию проведения внутреннего ИТ-аудита для ДЗО Фонда (далее – Методология). Методология основывается на передовых стандартах и подходах в области организации, управления и обеспечения безопасности ИТ-инфраструктуры, таких как:

- Cobit, Control Objective in IT and related technologies (Цели контроля в ИТ и смежных технологиях) (2007 г.);
- СТ РК ИСО/МЭК 17799, Свод правил по управлению защитой информации (2005 г.)
- KPMG ITRMB, KPMG IT Risk Management Benchmarking (Бенчмаркинг системы управления ИТ рисками) (2011 г.).

В рамках Методологии определены подходы к проведению процедур ежегодного внутреннего ИТ-аудита Службой внутреннего аудита ДЗО Фонда, либо внешним экспертом. Предложенным в Методологии подходам могут следовать все сотрудники, участвующие в процессе внутреннего ИТ-аудита.

Методология включает в себя комплексную оценку эффективности организации, управления и обеспечения безопасности ИТ, в разрезе четырех областей деятельности ИТ:

- Планирование и Организация;
- Приобретение и Внедрение;
- Эксплуатация и Сопровождение;
- Мониторинг и Оценка.

СВА является ответственной за проведение внутреннего ИТ-аудита согласно настоящей Методологии. Сроки проведения ИТ-аудита определяются в соответствии с доступными ресурсами и фактической программой аудита. Окончательные сроки проведения процедур внутреннего ИТ-аудита должны быть согласованы и утверждаются в рамках годового плана аудита.

Руководитель СВА должен обеспечивать выполнение следующих требований:

- Методика должна проходить ежегодный анализ на предмет ее актуальности и, при необходимости актуализироваться, путем внесения соответствующих изменений.
- Перед проведением внутреннего ИТ-аудита, следует убедиться в том, что состав назначенных внутренних аудиторов отвечает требованиям Международных Стандартов Внутреннего Аудита, в части раздела 1100 – Независимость и объективность и раздела 1210 – Профессионализм.

квалификационные требования к задействованным специалистам в процессе ИТ-аудита:

- степень магистра или бакалавра в ИТ или ИБ;
- минимум 5 лет практики администрирования ИТ- систем.

Рекомендуемые квалификационные требования к задействованным специалистам:

- членство в профессиональной ассоциации в области ИТ (например ISACA, (ISC)²);
- в зависимости от потребностей организации, наличие сертификации:
  - CIA - в случае необходимости наличия компетенции в области внутреннего аудита;
  - CISA – в случае необходимости наличия компетенции в области аудита, контроля, мониторинга и оценки организации ИТ;
  - CGEIT - в случае необходимости наличия компетенции в области управления ИТ;
  - CISM, CISSP – в случае необходимости наличия компетенции в области управления информационной безопасностью;
  - CRISC – в случае необходимости наличия компетенции в области управления ИТ рисками.

Подходы к проведению процедур внутреннего ИТ-аудита описанные в настоящей Методике не должны рассматриваться как исчерпывающие для оценки эффективности всей системы внутреннего контроля в области ИТ и информационной безопасности.

3 Порядок выполнения внутреннего ИТ-аудита

Настоящая Методология предполагает выполнение следующего порядка выполнения процедур внутреннего ИТ-аудита:

1. Планирование проведения ИТ-аудита, в том числе определение перечня работников и руководителей Фонда, с которыми необходимо провести интервью.
2. Определение перечня документов, требуемых для анализа и оценки, и направление соответствующего запроса в ответственное подразделение.
3. Проведение предварительного анализа предоставленных документов.
4. Проведение интервью с работниками и руководителями ДЗО, а также другими заинтересованными лицами, в случае необходимости.
5. Оценка эффективности системы внутреннего контроля в области ИТ.

При проведении процедур ИТ-аудита необходимо учитывать как процедуры, закрепленные внутренними документами ДЗО, так и процедуры, фактически осуществляемые на практике. При этом, наличие той или иной процедуры, закрепленной во внутреннем документе, при невыполнении на практике, не является достаточным свидетельством того, что ДЗО соблюдают соответствующие условия.

3.1 Области ИТ-аудита

Подтверждение соответствия системы управления информационными технологиями стратегии и целям организации осуществляется путем оценки эффективности реализованных ИТ- процессов.

Методология определяет выполнение оценки деятельности ИТ в организации посредством анализа эффективности 34 высокоуровневыхИТ-процессов(включающих выполнение порядка 200 ИТ- контролей), сгруппированных в рамках 4 областей деятельности ИТ:

1 Планирование и Организация (PO) – область объединяет ИТ-процессы направленные на стратегическое планирование и развитие ИТ, включая следующие процессы:

- PO1 Разработка стратегического плана.
- PO2 Определение ИТ архитектуры.
- PO3 Определение направлений развития технологий.
- PO4 Формализация ИТ процессов, организации и взаимоотношений с бизнесом.
- PO5 Управление инвестициями в ИТ.
- PO6 Согласованное управление целями и задачами.
- PO7 Управление ИТ персоналом.
- PO8 Управление качеством.
- PO9 Оценка и управление рисками ИТ.
- PO10 Управление проектами.

2 Приобретение и Внедрение (AI) – ИТ-процессы обеспечивающие выбор и эффективное внедрение ИТ решений, включает:

- AI1 Идентификация и выбор решений по автоматизации.
- AI2 Проектирование и разработка приложений.
- AI3 Проектирование и поддержка технической инфраструктуры.
- AI4 Обеспечение работы и использования ИС.
- AI5 Закупка ИТ-ресурсов.
- AI6 Управление изменениями.
- AI7 Установка и утверждение решений и изменений.

3 Эксплуатация и Сопровождение (DS) – данная область включаетИТ-процессысфокусированные на предоставлении качественных, безопасных и доступных ИТ решений и их поддержки для конечных пользователей.

- DS1 Определение и управление уровнем обслуживания.
- DS2 Управление услугами сторонних организаций.
- DS3 Управление производительностью и мощностями.
- DS4 Обеспечение непрерывности ИТ-сервисов.
- DS5 Обеспечение безопасности систем.
- DS6 Определение и распределение затрат.
- DS7 Обучение и подготовка пользователей.
- DS8 Управление службой поддержки и инцидентами.
- DS9 Управление конфигурацией.
- DS10 Управление проблемами.
- DS11 Управление данными.
- DS12 Управление физической безопасностью и защита от воздействия окружающей среды.
- DS13 Управление операциями по эксплуатации систем.

4 Мониторинг и Оценка (ME) – сосредоточена на оценке эффективности достижения ИТ процессами поставленных целей и включает следующий перечень:

- ME1 Мониторинг и оценка эффективности ИТ.
- ME2 Мониторинг и оценка системы внутренних контроля.
- ME3 Обеспечения соответствия внешним требованиям.
- ME4 Обеспечение корпоративного управления ИТ.

В рамках Методики, под оценкой эффективности ИТ-процесса понимается получение разумной уверенности в том, что цели ИТ-процесса должным образом достигаются. Заключение о достижении ИТ-процессами поставленных перед ними целей осуществляется путем подтверждении эффективности выполнения соответствующих этому процессу внутренних ИТ-контролей .

Настоящая Методология предусматривает оценку каждого ИТ- контроля по критериям оценки. В случае наличие ответов «Да» для всех критериев оценки относящихся к тестируемому контролю,

то вес такого контроля становится равным «1» баллу. Если хотя бы один из критериев оценки имеет ответ «Нет», то итоговый балл для данного ИТ- контроля равен «0».

В виду специфики различных ИТ-инфраструктур для части ИТ-контролей , определенные критерии оценки могут быть не применимы (такие критерии сопровождаются фразой «если применимо»). В этом случае, данный критерий в оценке ИТ- контроля не участвует.

Для оценки эффективности ИТ процесса, полученные баллы по соответствующим ИТ- контроля м суммируются и делятся на максимально возможное количество баллов по данному ИТ-процессу. Аналогичным образом, в процентном выражении определяется эффективность реализации всех анализируемых ИТ-процессов.

4 Подход к ИТ Аудиту

Настоящая Методология рассматривает два альтернативных подхода к проведению ИТ-аудита:

1. Стандартный подход.
2. Расширенный подход.

4.1 Стандартный подход

Стандартный подход включает комплексную оценку основных ИТ процессов, присущих для любой организации не зависимо от ее размера, индустрии и специфики деятельности. Для проведения ИТ-аудита на основе стандартного подхода необходимо провести оценку эффективности реализованных контролей в рамках минимального перечня ИТ процессов:

- PO4 Формализация ИТ- процессов, организации и взаимоотношений с бизнесом.
- PO5 Управление инвестициями в ИТ.
- PO6 Согласованное управление целями и задачами.
- PO9 Оценка и управление рисками ИТ.
- AI6. Управление изменениями.
- AI7. Установка и утверждение решений и изменений.
- DS5. Обеспечение безопасности систем.
- DS8. Управление службой технической поддержки и инцидентами.
- DS11 Управление данными.
- DS12. Управление физической безопасностью и защита от воздействия окружающей среды.
- DS13. Управление операциями по эксплуатации систем.
- ME4 Обеспечение корпоративного управления ИТ.

По усмотрению СВА перечень ИТ-процессов, описанный выше, может расширен дополнительными ИТ- процессами.

4.2 Расширенный подход

Расширенный подход реализует риск ориентированный подход в ИТ-аудиту. Данный вариант является предпочтительным для организаций с высокой зависимостью от информационных и смежных технологий, таких как: финансовые институты, телекоммуникационные или ИТ компании.

На первом этапе осуществляется качественная оценка ИТ-рисков влияющих на достижение стратегических бизнес целей организации. На данном этапе оценка ИТ-рисков может быть проведена профильным подразделением в области управления рисков организации. Перечень ключевых высокоуровневых ИТ- рисков включает:

- Бизнес фокус.
- Информационные ресурсы.
- Зависимость от ИТ.
- Зависимость от ИТ-персонала.
- Зависимость от ИТ-поставщиков.
- Надежность ИТ-систем.
- Изменения в ИТ.
- Регуляторные требования к ИТ.

Ниже представлено описание каждого высокоуровневого ИТ-риска и предложены критерии для оценки его влияния и вероятности реализации.

4.2.1 ИТ- риски

4.2.1.1 Бизнес фокус

ИТ-функции и процессы не согласованы с бизнес-требованиям и потребностями пользователей, в связи с этим существует риск того, что ИТ не удовлетворяет потребностям бизнеса и пользователей, либо ИТ не интегрирован соответствующим образом в бизнес, стратегию и будущие планы организации.

В результате это может привести к следующим последствиям и убыткам:

- Неэффективные методы работы, неиспользуемые интерфейсы и дублирование информации, ИТ-системы не удовлетворяют потребностям пользователей.
- Недостаточный уровень управления ИТ- рисками, вызванное непониманием этих рисков руководством, ведет к большим потерям.
- Лишние расходы и инвестиции в ИТ, которые не способствуют реализации бизнес стратегии и планов организации.

Критерии оценки влияния

Степень важности бизнес процессов, поддерживаемых со стороны ИТ, влияет на увеличение/уменьшение расходов, в случае, если оно не обусловлено потребностями бизнес подразделений.

Критерии оценки вероятности

Осведомленность руководства – вероятность потерь увеличивается, если руководство не в полной мере осведомлено о рисках, выявленных при использовании ИТ в организации, и определении направления в котором ИТ должно удовлетворить бизнес потребности.

Удовлетворенность пользователей - недовольные пользователи регулярно применяют искусственные обходные пути, дублируют процессы или принимают неэффективные методы, чтобы компенсировать недостатки в ИТ системах, что ведет к увеличению расходов / потерь для бизнеса.

Автономность - степень автономности работы ИТ-подразделения относительно контроля со стороны бизнеса. Как правило, влияет на вероятность роста потерь.

4.2.1.2 Информационные ресурсы

Наличие информационных активов может повлечь за собой риски потери и убытков для организации. Потери или убытки могут выражаться в следующем:

- Прямые финансовые потери, в случае мошенничества или воровства;
- Косвенная финансовая, воздействие на репутацию организации. Например: «Взлом корпоративного веб-сайта хакерской группой» или утеря важной бизнес информации или интеллектуальной собственности.

Критерии оценки влияния

Персональная информация - если организация хранит или обрабатывает персональные данные, такие как медицинские данные сотрудников, то правовые и репутационные последствия раскрытия или потери информации, увеличиваются.

Интеллектуальная собственность - если данные имеют значительную конкурентную ценность, такую как список клиентов, спецификации новых продуктов, то это ведет к вероятности кражи или раскрытия этих данных.

Финансовые данные - если организация имеет важную финансовую, такую как информацию о операциях с пластиковыми карточками, то это может привести к прямым денежным потерям от кражи или манипуляции данной информацией.

Критерии оценки вероятности

Поводы для мошенничества – природа информационных активов и конкурентная среда организации будет влиять на вероятность мошенничества. Чем больше ценной информации в руках организации, и чем больше уровень конкуренции на рынке, тем больше вероятность мошенничества.

Публичная информация об организации – чем большее публичной информации об организации, особенно если организация работает на таких рынках как (продажи оружия, испытание на животных, производство ядовитых или отравляющих веществ и т.п.), тем больше повода для внешнего нападения на информационные активы организации.

4.2.1.3 Зависимость от ИТ

Этот риск описывает последствия при потери определенных частей ИТ-инфраструктуры организации. Чем больше зависимость организации от ИТ, тем больше вероятность финансовых или репутационных потерь. Результатом потерь может быть следующее, пример:

- Один или несколько бизнес-процессов не могут выполняться, пока система не будет восстановлена.
- Клиенты недовольны скоростью и качеством предоставляемых услуг.

Критерии оценки влияния

Природа бизнес-процессов - если бизнес-процессы, которые в значительной степени зависят от ИТ, являются основными / критическими процессами для организации, то это ведет к увеличению риска.

Степень автоматизации - степень автоматизации указывает, будет ли бизнес или клиент сильно страдать из-за потери ИТ-функций или будет только незначительное воздействие на бизнес.

Договор купли-продажи - если организация как правило, имеет договоры купли-продажи с жесткими сроками поставки, то убытки от потери ИТ-средств будут увеличиваться.

Критерии оценки вероятности

Количество бизнес-процессов - чем больше число бизнес-процессов зависимых от ИТ-систем, тем больше вероятность убытков или потерь.

ИТ поддержка - степень ИТ-поддержки основных бизнес-процессов может также указывать на вероятность каких-либо неблагоприятных последствий.

Сложность - чем сложнее ИТ-система для понимания и работе с ней, тем больше вероятность убытков из-за трудностей обеспечения непрерывного режима ее работы.

4.2.1.4 Зависимость от ИТ персонала

Характер и степень зависимости организации от внутреннего ИТ-персонала ведет к потере времени. Это может быть связано с потерей знаний или навыков, имеющихся у сотрудников организации, либо с специальными навыками, которые применяются ИТ-подразделением.

Критерии оценки влияния

Концентрация: чем больше концентрация ключевых навыков / знаний у небольшого числа людей, тем больше влияние при их увольнении на организацию. Это также относится к физической концентрации ИТ-персонала, то есть все сотрудники ИТ-подразделения размещены в одном здании, особенно там, где это здание / место, представляет собой какой-либо риск (землетрясение, техногенная катастрофа и т.д.)

Соответствие и актуальность – если навыки ИТ сотрудников не соответствуют ИТ-среде организации и/или не являются актуальными, потенциальное влияние на организацию посредством неоптимального использования ИТ ведет к увеличению услуг со стороны третьих лиц.

Критерии оценки вероятности

Текучесть кадров: чем больше уровень текучести кадров, особенно на старших / опытных уровнях, тем выше вероятность того, что ценные навыки будут утеряны.

4.2.1.5 Зависимость от ИТ поставщиков

Существует риск потерь в случае высокой зависимости организации от третьих сторон, таких как аутсорсинг, поставщики, подрядчики и консультанты.

Убытки могут возникнуть в результате потери или снижения ключевых навыков, отсутствия понимания бизнес-процессов со стороны третьих лиц, связанных договорными условиями и чрезмерными расходами в сравнении, если проект внедрялся бы собственными силами.

Критерии оценки влияния

Характер бизнес-процессов, в которых вовлеченная третья сторона будет влиять на вероятность каких-либо потерь. Если это основные бизнес-процессы и системы, это может привести к большой зависимости и, следовательно, высокому влиянию от третьих лиц. Незначительные бизнес-процессы могут не иметь какого либо существенного финансового воздействия.

Размер и репутация привлекаемых третьих сторон, будет влиять на потенциальный размер потерь.

Критерии оценки вероятности

Степень участия третьей стороны - степень участия определяет потенциальные потери от транзакций третьей стороны. Если все ИТ-подразделение будет на аутсорсинге, то потенциальные финансовые последствия могут быть выше. В случае если только 1 процесс передан на аутсорсинг то риски потерь уменьшаются прямо пропорционально количеству процессов отданных на аутсорсинг.

Количество третьих сторон - вероятность потерь будет расти с увеличением числа третьих сторон и количеством систем и бизнес-процессов, в которых они будут принимать участие.

4.2.1.6 Надежность ИТ систем

Отсутствие надежности ИТ-систем приводит к потерям, понесенных организацией. Эти потери могут возникнуть в результате непоследовательной или неточной обработки бизнес информации, ремонтных работ, необходимых для исправления, обработки проблем и вопросов или использования неэффективных или дублирующих процессов пользователями из-за отсутствия доверия к ИТ-системам.

Критерии оценки влияния

Влияние каких-либо неисправностей в ИТ-системах определяется посредством критичности автоматизируемых или поддерживаемых бизнес-процессов. Проблемы, связанные с информационной системой поддерживающей основные бизнес-процессы (например: он-лайн система продаж билетов) вызвали бы большие потери чем, если бы бизнес-процесс имел менее жизненно-важное значение.

Критерии оценки вероятности

Сложность: большая сложность ИТ-систем, будь то единое интегрированное приложение или мульти интерфейсное решение, имеет вероятность того, что эти системы будут подвержены риску ненадежности.

"Bleeding Edge" - использование передовых и еще непроверенных (не обкатанных) технологий, повышает вероятность возникновения проблем с надежностью.

Конечный пользователь вычислительной техники - высокая степень манипуляции конечного пользователя с данными и существование двойной обработки информации пользователями, может указывать на отсутствие уверенности в надежности основной ИТ-системы.

Ошибки – частота фактических ошибок и проблем указывает на степень не надежности ИТ-системы.

4.2.1.7 Изменения в ИТ

Здесь описывается риск потерь из-за изменений в ИТ-среде. Эти потери могут происходить из-за следующего:

- Неэффективные или быстрые проекты, которые не отвечают потребностям бизнеса.
- Ошибки и потеря надежности в приложениях из-за непрерывного обслуживания и значительных изменений.
- Влияние изменений не протестировано должным образом или слабо изучено.

Критерии оценки влияния

Крупные проекты - чем больше размер проектов, связанных с ИТ, тем больше потенциальных финансовых убытков для организации.

Природа бизнес-процессов - При оценке изменений рассматривается природа бизнес-процессов, в которых выполняются изменения. Риск может быть значительно выше, при внесении изменений в основные бизнес-процессы, чем в второстепенные.

Критерии оценки вероятности

Текущее обслуживание - непрерывное обслуживание систем необходимо учитывать при оценке вероятности потенциальных потерь. Так ли необходимо ИТ-персоналу непрерывно вносить изменения, мелкие или другие корректировки в существующую систему?

Характер изменений - характер изменений определяет вероятность появления ошибок. Так, вероятность потерь из-за одного незначительного изменения меньше, чем в случае крупного проекта - редизайна.

Сложность – чем сложнее система, тем больше вероятность того, что воздействие любого изменения не будет должным образом протестировано или полностью проверено. Следовательно это приведет к увеличению вероятности возможных потерь.

4.2.1.8 Регуляторные требования

Существует риск того, что несоблюдение законодательства, касающегося обработки, хранения и использования информации, приведет к финансовым или репутационным потерям для организации. Это может привезти к штрафным санкциям со стороны регулирующего органа, либо огласке нарушений с последствиями для репутации бизнеса.

Примеры регуляторных требований, которые необходимо соблюдать:

- Закон Сарбейнса-Оксли.
- Международные стандарты финансовой отчетности;
- Базель II.
- Требования Национального Банка Республики Казахстан.

Критерии оценки влияния

Регулирующий орган – полномочия и права регулирующих органов могут оказать влияние на потенциальные потери за нарушения соответствующего законодательства.

Общедоступная информация – чем больше освещается деятельность организации, особенно если она работает в узком сегменте рынка тем больше возможностей использовать данную информацию против организации.

Критерии оценки вероятности

Регулируемая индустрия – степень регулирования индустрии напрямую влияет на необходимость соответствия требованиям регуляторов.

Финансовый институт – обязан придерживаться определенных стандартов ведения бухгалтерского учета, особых процессов для записей проводок и обновления финансовых и бухгалтерских данных.

Данные – характер данных, используемых организацией, которая может подвергнуться дополнительному регулированию, такого как защита данных о частной жизни, отмывание денег, налоги и социальное обеспечение.

4.2.2 Оценка ИТ рисков

На этапе подготовки проведения качественной оценки ИТ-рисков, устанавливаются основные параметры такой оценки. Оценка ИТ-рисков проводится по двум показателям – вероятность и влияние риска. Для обеспечения сопоставимости рисков между собой и облегчения качественной оценки вводится балльная шкала: от 1 до 5 баллов.

Оценка влияния ИТ рисков производится в денежном выражении на основе удерживающей способности, определенной в соответствующих политиках Фонда и ДЗО. Однако, в случае если влияния ИТ риска трудно оценить в финансовых показателях, дополнительно введены качественные (нефинансовые) критерии оценки (см.Таблица 1. Влияние рисков)

Таблица 1. Влияние риска

Балл	Значение	Финансовое влияние	Нефинансовое влияние
1	Незначительный	До рабочей удерживающей способности	Отсутствие каких-либо последствий в случае реализации риска
2	Заметный	До удерживающей способности	Последствия от реализации риска не

			значительные
3	Крупный	Минимум: до 25% потери ликвидности или до 50% потери доходности	Последствия от реализации риска не значительные и могут быть полностью исправлены
4	Критический	Минимум: до полной потери доходности или до 25% потери собственного капитала	Последствия от реализации риска очень значительные, но могут быть исправлены до определенной степени
5	Катастрофический	Начиная с минимума: полная потеря доходности или 25% потери собственного капитала	В случае реализации риска, компания практически не сможет восстановиться от последствий, связанных с данным риском

При оценке вероятности реализации ИТ-риска необходимо пользоваться критериями оценки приведенными ниже. (см.

Таблица 2. Вероятность риска)

Таблица 2. Вероятность риска

Балл	Значение	Частота или вероятность
1	Очень редко	Вероятность наступления до 5% (Один раз в 7 и более лет)
2	Редко	Вероятность наступления до 25% (Один раз в 5 лет)
3	Время от времени	Вероятность наступления до 40% (Один раз в 3 года)
4	Часто	Вероятность наступления до 80% (Один раз в год)
5	Очень часто	Вероятность наступления свыше 80% (Один раз в пол года или чаще)

Для окончательного расчета величины ИТ-риска, результаты оценки влияния и вероятности перемножаются (см. Таблица 3. Величина риска).

Таблица 3. Величина риска

		Влияние				
		1	**2**	**3**	**4**	**5**
Вероятность	**1**	**1**	**2**	**3**	**4**	**5**
	2	**2**	**4**	**6**	**8**	**10**
	3	**3**	**6**	**9**	**12**	**15**
	4	**4**	**8**	**12**	**16**	**20**
	5	**5**	**10**	**15**	**20**	**25**

В результате оценки полученные значения величин ИТ-рисков в диапазоне от 1 до 25 отражаются на карте рисков.

- Величина риска в диапазоне от 1 до 4 баллов является низкой и попадает в зеленый сектор.
- Величина риска в диапазоне от 5 до 12 баллов является средней и попадает в желтый сектор.
- Величина риска в диапазоне от 12 до 25 баллов является высокой и попадает в красный сектор.

Цели ИТ-аудита и частота проверки определяется в соответствии с оценочным уровнем ИТ-риска:

- Для ИТ-рисков, оценочная величина которых является высокой (отраженные на карте рисков в красном секторе) проверка соответствующих им ИТ-процессов проводится постоянно в рамках ИТ-аудита.
- Для ИТ-рисков, оценочная величина которых является средней (отраженные на карте рисков в желтом секторе) проверка соответствующих им ИТ-процессов проводится с периодичность раз в 3 года.
- Для ИТ-рисков, оценочная величина которых является низкой (отраженные на карте рисков в зеленом секторе) проверка соответствующих им ИТ-процессов проводится с периодичность раз в 4 года.

4.2.3 Выбор ИТ- контролей

Определение перечняИТ-процессовосуществляется в соответствии с Матрицей соответствияИТ-процессови ИТ рисков (см. Отобранные, таким образом,ИТ-процессы оцениваются на эффективность по уменьшению рисков, влияющих на достижение поставленных перед ними целей.

Таблица 4. Матрица соответствияИТ-процессови ИТ рисков). Для каждого ИТ риска (расположенного в колонке) выбирается переченьИТ-процессов(расположенных по строкам), контроли которых направлены на снижение влияния данного риска (красный индикатор). Отобранные, таким образом,ИТ-процессы оцениваются на эффективность по уменьшению рисков, влияющих на достижение поставленных перед ними целей.

Таблица 4. Матрица соответствияИТ-процессови ИТ рисков

	Наименование процесса	Бизнес фокус	Информационные ресурсы	Зависимость от ИТ	Зависимость от ИТ персонала	Зависимость от ИТ поставщиков	Надежность ИТ систем	Изменения в ИТ	Регуляторные требования
Планирование и организация (PO)	PO1. Разработка стратегического плана развития ИТ.	●	●	●	●	●			
	PO2. Определение информационной архитектуры.		●	●			●		
	PO3. Определение направления технологического развития.			●					●
	PO4. Определение ИТ процессов, организационной структуры и				●	●	●		●

	Наименование процесса	Бизнес фокус	Информационные ресурсы	Зависимость от ИТ	Зависимость от ИТ персонала	Зависимость от ИТ поставщиков	Надежность ИТ систем	Изменения в ИТ	Регуляторные требования
	взаимосвязей.								
	PO5. Управление ИТ инвестициями.	●			●	●			●
	PO6. Информирование о целях и направлениях развития ИТ.	●			●	●	●		●
	PO7. Управление персоналом.	●		●	●	●	●		
	PO8. Управление качеством.	●		●	●		●	●	
	PO9. Оценка и управление ИТ рисками.	●	●	●	●	●	●	●	●
	PO10. Управление проектами.	●		●	●	●		●	
Приобретение и внедрение (AI)	AI1. Выбор решений по автоматизации.	●		●					
	AI2. Приобретение и поддержка программных приложений.		●	●			●	●	●
	AI3. Приобретение и обслуживание технологической инфраструктуры.	●	●				●	●	
	AI4. Обеспечение выполнения операций.	●		●			●		
	AI5. Поставки ИТ ресурсов.				●		●		
	AI6. Управление внесением изменений.	●			●		●	●	
	AI7. Внедрение и приемка решений и изменений.	●					●	●	
Эксплуатация и сопровождение (DS)	DS1. Определение и управление уровнем обслуживания.	●	●			●			
	DS2. Управление услугами сторонних организаций.	●	●			●			
	DS3. Управление производительностью и мощностями.	●	●	●	●	●	●		
	DS4. Обеспечение непрерывности.			●			●		
	DS5. Обеспечение безопасности систем.		●	●	●	●			
	DS6. Определение и распределение затрат.	●	●		●	●			●
	DS7. Обучение и подготовка пользователей.		●					●	●
	DS8. Управление службой технической поддержки и инцидентами.	●		●			●		
	DS9. Управление конфигурацией.			●			●	●	
	DS10. Управление проблемами.	●		●			●		
	DS11. Управление данными.		●	●			●		●
	DS12. Управление физической безопасностью и защита от воздействия окружающей среды.		●	●			●		

	Наименование процесса	Бизнес фокус	Информационные ресурсы	Зависимость от ИТ	Зависимость от ИТ персонала	Зависимость от ИТ поставщиков	Надежность ИТ систем	Изменения в ИТ	Регуляторные требования
	DS13. Управление операциями по эксплуатации систем.		●	●			●		
Мониторинг и оценка (ME)	ME1. Мониторинг и оценка эффективности ИТ.	●		●					
	ME2. Мониторинг и оценка системы внутреннего контроля.	●			●	●	●		
	ME3. Обеспечение соответствиями с внешними требованиями.		●						●
	ME4. Обеспечение корпоративного управления ИТ.	●		●			●		

4.3 Результаты ИТ-аудита

Результат оценки эффективности ИТ-процессов может быть представлен в графическом виде, как показано на Рисунке 1. Оценка эффективности ИТ процессов.

Рисунок 1. Оценка эффективности ИТ процессов

Также, полученные результаты оценки эффективности ИТ-процессов является основой для подготовки обобщенного отчета эффективности ключевых областей организации, управления и обеспечения безопасности ИТ. Определение итогового балла эффективности ИТ в процентном выражении производится путем расчета среднего арифметического значения процентов эффективностиИТ-процессовпо соответствующим областям ИТ (см. Рисунок 2. Обобщенная оценка эффективности организации и управления ИТ).

Рисунок 2. Обобщенная оценка эффективности организации и управления ИТ

После проведения оценки эффективности ИТ организации, СВА подготавливает отчет по результатам внутреннего ИТ-аудита. В свою очередь, владельцы ИТ-процессов разрабатывают план мероприятий по дальнейшему совершенствованию ИТ-контролей . В дальнейшем СВА оказывает поддержку владельцамИТ-процессовв вопросах разработки и документирования плана мероприятий по дальнейшему совершенствованию системы внутренних контролей в области ИТ. Данная поддержка оказывается в той мере, в которой не возникает конфликт интересов.

Подготовленный отчет, а также план мероприятий по дальнейшему совершенствованию ИТ-контролей согласовываются и рассматриваются в соответствии с действующими процедурами СВА организации.

4.4 ИТ-процессы

4.4.1 PO. Планирование и Организация

PO1. Разработка стратегического плана развития ИТ

Стратегическое планирование ИТ необходимо для того, чтобы управление всеми ИТ-ресурсами было взаимосвязано со стратегией и приоритетами организации. ИТ-подразделение наряду со всеми заинтересованными сторонами ответственно за получение оптимальных результатов от проектов и услуг организации. Стратегический план улучшает понимание акционеров в отношении возможностей и ограничений ИТ, помогает оценить текущую эффективность, определяет требования к персоналу и уровень необходимых инвестиций. Корпоративная стратегия и приоритеты должны быть отражены в портфеле проектов и реализованы посредством тактических планов ИТ. В тактических планах ИТ кратко определяются цели, планы действий и задачи, которые понятны и принимаются как со стороны корпоративного управления, так и со стороны ИТ. Оценка процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 5. Контроли ИТ-процесса «Разработка стратегического плана развития ИТ».

Таблица 5. Контроли ИТ-процесса «Разработка стратегического плана развития ИТ»

№	Контроль	Цель контроля	Критерии оценки
PO 1.1	Управление пользой от ИТ	Убедиться в том, что корпоративный портфель ИТ инвестиций включает в себя решения, которые обоснованы бизнес деятельностью организации.	• Применяется ли в организации процедура бизнес обоснования, включающую оценку финансовой ценности ИТ услуг, а также риска не реализации возможности ожидаемых преимуществ?
PO 1.2	Соответствие между бизнесом и ИТ	Убедится в том, что установлена связь между бизнесом и ИТ с целью взаимного согласования приоритетов.	• Является ли ИТ частью долгосрочных и краткосрочных планов развития организации, раскрывающих миссию и цель организации?
PO 1.3	Стратегический план ИТ	Удостовериться, что в организации разработан стратегический план развития ИТ и достигнуты поставленные цели.	• Разработан ли стратегический план ИТ?
			• Стратегический план ИТ включает операционную модель и ИТ архитектуру?
			• Достигнуты ли поставленные цели стратегического плана (за последние 5 лет)?
PO 1.4	Оценка текущих возможностей и эффективности ИТ	Следует убедиться, что в организации проводится оценка текущих возможностей и эффективности решений и услуг с целью установить отправную точку для сравнения текущей ситуации и будущих требований.	• В организации проводится ли мониторинг и оценка возможностей и эффективности ИТ?
PO 1.5	Тактические планы ИТ	Убедится в наличии тактических планов ИТ, которые будут вытекать из стратегического плана ИТ.	• В организации разработан тактический план развития функций ИТ сервисов?
PO 1.6	Управление стратегическим планом ИТ	Убедится в существовании процесса управления стратегией развития ИТ.	• В организации осведомлены о планах развития ИТ?
			• Проводится ли мониторинг и оценка тактических и стратегических планов развития ИТ?

№	Контроль	Цель контроля	Критерии оценки
			• Оценивается ли руководством текущая ИТ система в сравнении с системой до разработки или изменения стратегического плана ИТ?

PO2. Определение информационной архитектуры

Информационные системы создают и регулярно обновляют корпоративную информационную модель и определяют системы для оптимального использования информации. Сюда относятся развитие справочника корпоративных данных и правил представления данных, схему классификации данных и уровни безопасности. Этот процесс повышает качество принятия решений руководством, поскольку возникает уверенность в том, что поступает достоверная и защищенная информация. Кроме того, рационализация ресурсов информационных систем ведет к повышению соответствия корпоративной стратегии. Данный ИТ-процесс также необходим для улучшения отчетности в вопросах целостности и безопасности данных, а также для повышения эффективности и контроля при совместном использовании информации приложениями и субъектами. Оценка процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 6. Контроли ИТ-процесса «Определение информационной архитектуры».

Таблица 6. Контроли ИТ-процесса «Определение информационной архитектуры»

№	Контроль	Цель контроля	Критерии оценки
PO 2.1	Модель информационной архитектуры	Удостовериться в том, что в организации разработана и поддерживается модель информационной архитектуры.	• Существует ли в организации модель информационной архитектуры, которая поддерживается и обновляется на регулярной основе?
PO 2.2	Справочник данных	Определить, что в организации создан и обновляется на регулярной основе справочник данных.	• Существует ли организации справочник данных, который поддерживается и обновляется на регулярной основе?
PO 2.3	Схема классификации данных	Удостоверится в том, что разработана и поддерживается схема классификации данных.	• В организации существует схема классификации данных?
PO 2.4	Управление целостностью	Убедится в том, что процедуры по управлению целостности разработаны и внедрены.	• В организации описаны требования по безопасности для каждого класса данных?

PO3. Определение направления технологического развития

ИТ-подразделение направляет технологическое развитие с целью поддержки бизнеса. Это требует разработки плана развития технологической инфраструктуры и создания комитета по вопросам информационной архитектуры, который должен предлагать понятные и реалистичные оценки того, что могут предложить технологии с точки зрения продуктов, услуг и механизмов внедрения. План должен регулярно обновляться и учитывать такие аспекты как архитектура систем, направление технологического развития, планы приобретений, стандарты, стратегии миграции и непрерывность. Это позволит своевременно реагировать на изменения в конкурентной обстановке, экономить на масштабах инвестиций и затратах на персонал для поддержки информационных систем, а также улучшить взаимодействие платформ и приложений. Оценка

процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 7. Контроли ИТ-процесса «Определение направления технологического развития».

Таблица 7. Контроли ИТ-процесса «Определение направления технологического развития»

№	Контроль	Цель контроля	Критерии оценки
PO 3.1	Планирование технологического развития	Убедится в том, что в организации проводиться анализ существующих и возникающих технологий и планирование, какое направление технологического развития будет адекватно реализовывать ИТ стратегию и архитектуру бизнес систем.	• В рамках стратегического развития организации определен ли план технологического развития ИТ? • Включает ли план технологического развития такие аспекты, как: ▪ описание технологической инфраструктуры; ▪ архитектура ИС; ▪ технологическое направление; ▪ непрерывность деятельности; ▪ стратегии миграции.
PO 3.2	План технологической инфраструктуры	Удостоверится в том, что в организации разработан и поддерживается план технологической инфраструктуры в соответствии со стратегическим и тактическими планами ИТ.	• В рамках стратегических и тактических планов организации определен ли план технологической инфраструктуры? • Включает ли план технологической инфраструктуры такие аспекты, как: ▪ непрерывности деятельности ▪ рекомендации по приобретению технологических ресурсов; ▪ экономии на масштабах инвестиций и затратах; ▪ изменения в конкурентной среде.
PO 3.3	Анализ перспективных направлений и нормативных требований	Следует удостовериться в том, что в организации осуществляется анализ перспективных направлений и нормативных требований.	• Существует ли в организации процесс анализа и прогнозирования в области информационных технологий, инфраструктуры, законодательных и регуляторных требований? • Включаются ли результаты данного анализа при разработке плана технологической инфраструктуры?
PO 3.4	Технологические стандарты	Необходимо убедится, что в организации осуществляется управление технологическими стандартами. Существует форум	• Сформирован ли в организации технологический форум для обмена опытом по применению технологий, консультирования по инфраструктурным решениям, руководству по выбору технологий, оценки совместимости со стандартами?
PO 3.5	Комитет по вопросам проектирования ИТ архитектуры	Убедится в существовании комитета по вопросам развития ИТ архитектуры.	• В организации учрежден коллегиальный орган по вопросам проектирования ИТ архитектуры?

PO4. Определение ИТ процессов, организационной структуры и взаимосвязей

Организационная структура ИТ определяется требованиями по кадрам, навыкам, функциям, отчетности, руководству, должностям и обязанностям, надзору. Эта структура включена в методологиюИТ-процессови обеспечивает прозрачность и контроль, а также участие высшего руководства и бизнес менеджмента. Комитет по стратегии должен осуществлять контроль над ИТ

со стороны Совета директоров, а один или несколько руководящих комитетов, в которых участвует руководство бизнеса и ИТ, должны расставлять приоритеты в использовании ИТ-ресурсов согласно требованиям бизнеса. Процессы, административные политики и процедуры должны охватывать все функции, а особенно, контроль, обеспечение качества, управление рисками, информационную безопасность, принадлежность данных и систем, а также, разделение обязанностей. Для того, чтобы обеспечить своевременную поддержку бизнес требований, ИТ-служба должна быть вовлечена в процессы принятия решений. Оценка процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 8. Контроли ИТ-процесса «Определение ИТ процессов, организационной структуры и взаимосвязей».

Таблица 8. Контроли ИТ-процесса «Определение ИТ процессов, организационной структуры и взаимосвязей»

№	Контроль	Цель контроля	Критерии оценки
PO 4.1	Методология ИТ процесса	Необходимо убедится в том, что определена методология по реализации плана ИТ развития.	• Определен ли в организации подход к формализации ИТ процесса, включающий определение: ▪ владельцев процесса; ▪ зрелость процесса; ▪ оценку эффективности процесса; ▪ совершенствование процесса; ▪ соответствие требованиям; ▪ планы по достижению целевых значений.
PO 4.2	Коллегиальный орган по ИТ стратегии	Удостоверится в том, что в организации сформирован и функционирует коллегиальный орган по ИТ стратегии на уровне Совета директоров.	• Сформирован ли в организации коллегиальный по ИТ стратегии? • Наделен ли полномочиями данный орган по даче рекомендаций стратегического характера? • Проводится ли данным органом анализ основных инвестиций в области ИТ?
PO 4.3	Коллегиальный орган по управлению ИТ	Удостоверится в том, что в организации сформирован и функционирует Коллегиальный орган по управлению ИТ (или эквивалентный ему орган).	• Сформирован ли в организации коллегиальный орган по управлению ИТ? • Наделен ли данный орган полномочиями определять приоритеты инвестиционных программ? • Проводится ли данным органом мониторинг реализации отдельных проектов, уровня оказания услуг и улучшения в области ИТ?
PO 4.4	Место ИТ подразделения в организации	Следует убедиться, что ИТ подразделение включено в организационную структуру организации с учетом значимости ИТ для организации.	• В организации выделено структурное подразделение по ИТ?
PO 4.5	Организационная структура ИТ	Необходимо удостоверится, что организационная структура ИТ подразделения создана в соответствии с потребностями бизнеса.	• Проводится ли периодический анализ организационной структуры ИТ с точки зрения соответствия кадровым потребностям и стратегиям в области аутсорсинга?
PO 4.6	Определение должностных	Необходимо убедится в том, что должностные обязанности и полномочия	• В организации разработаны и установлены и доведены до сведения должностные инструкции

№	Контроль	Цель контроля	Критерии оценки
	обязанностей и полномочий	ИТ персонала установлены и донесены до сведения всех заинтересованных сторон.	для ИТ персонала, которые включают подотчетность в соответствии с потребностями организации?
PO 4.7	Ответственность за обеспечение качества ИТ	Удостоверится в том, что в организации назначены ответственные лица по вопросам обеспечения качества.	• Назначены ли в организации ответственные лица по вопросам обеспечение качества предоставляемых ИТ услуг?
			• Содержат ли должностные инструкции персонала ответственность по обеспечению качества?
PO 4.8	Ответственность за риск, безопасность и соответствие требованиям	Необходимо удостовериться, что в организации определены и назначены ключевые должностные лица по управлению ИТ рисками, включая особую ответственность за информационную безопасность, физическую безопасность и соответствие требованиям.	• Определены ли в организации ответственности: ▪ по управлению ИТ рисками; ▪ за информационную и физическую безопасность; ▪ за соответствие регуляторным требованиям? • Определена ли ответственность руководства по управлению рискам и безопасности на уровне организации?
PO 4.9	Владение данными и системами	Убедится в том, что организация обеспечена бизнес процедурами и инструментами, позволяющими обеспечить функцию бизнеса как собственника данных и информационных систем.	• Существует ли в организации процесс назначения владельцев и ответственных за информационные активов? • Все ли информационные активы организации имеют владельцев?
PO 4.10	Надзорные функции	Необходимо удостовериться, что в организации реализованы практики по надзору в области ИТ.	• Реализована ли в организации практика по контролю в области ИТ, необходимая для оценки правильности выполнения обязанностей ИТ персоналом?
PO 4.11	Разделение полномочий	Удостоверится в том, что в организации разделены роли и обязанности в области ИТ.	• Должностные инструкции в организации четко описывают роли и обязанности для каждого сотрудника ИТ? • Существует ли в организации разделение обязанностей между инициатором и исполняющим при внесении изменений, предоставления доступа, и резервного копирования? • Сотрудники выполняют только регламентированные обязанности, предусмотренные их должностными обязанностями?
PO 4.12	Кадровое обеспечение ИТ	Удостоверится в том, что функции ИТ адекватно и в достаточной мере обеспечены кадровыми ресурсами для реализации целей и задач бизнеса.	• Проводится ли на регулярной основе или по мере существенных изменений оценка потребностей в кадровых ресурсах для ИТ подразделения?

№	Контроль	Цель контроля	Критерии оценки
PO 4.13	Ключевой ИТ персонал	Необходимо убедится в том, что в организации минимизирован риск зависимости от конкретных сотрудников.	• Определены ли в организации ключевые должностные лица в ИТ подразделении ответственные за определенные области(в том числе дублирующий персонал)?
PO 4.14	Политика и процедуры в отношении привлекаемых специалистов	Необходимо удостоверится, что привлекаемые специалисты ознакомлены и исполняют политики процедуры организации.	• Ознакомлены ли и выполняются политики и процедуры по безопасности организации привлекаемыми специалистами?
PO 4.15	Взаимосвязи	Убедится в том, что в организации установлена и поддерживается оптимальная координация и взаимодействие между ИТ подразделением и другими заинтересованными сторонами организации.	• Описывают ли должностная инструкция правила взаимодействия сотрудников ИТ подразделения с заинтересованными сторонами организации, такими как Совет директоров, высшее руководство, бизнес подразделения, индивидуальные пользователи, поставщики, сотрудники службы безопасности, риск менеджеры, группа по корпоративному соответствию, подрядчики и менеджмент других организаций?

PO5. Управление ИТ инвестициями

Управление ИТ-инвестициями обеспечивает и поддерживает управление связанными с ИТ инвестиционными программами и включает в себя вопросы затрат и преимуществ, приоритетов при формировании бюджета, формализации и управления бюджетным процессом. Заинтересованные стороны проводят консультации для того, чтобы выявить и контролировать общий объем затрат и преимуществ в контексте стратегического и тактических планов ИТ и имеют возможность, в случае необходимости, провести коррекцию. Процесс стимулирует взаимодействие между заинтересованными сторонами в ИТ и в бизнес подразделениях; устанавливает эффективное использование ИТ-ресурсов; обеспечивает прозрачность и отчетность в рамках общей стоимости владения, реализацию корпоративных преимуществ и получение прибыли от ИТ инвестиций. Оценка процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 9. Контроли ИТ-процесса «Управление ИТ инвестициями».

Таблица 9. Контроли ИТ-процесса «Управление ИТ инвестициями»

№	Контроль	Цель контроля	Критерии оценки
PO 5.1	Методология управления финансами	Следует убедиться, что в организации разработана и поддерживается методология управления финансами для управления инвестициями и стоимостью ИТ активов и услуг посредством портфелей ИТ инвестиций, бизнес-планов и ИТ бюджетов.	• Разработана ли в организации методология управления финансами?
PO 5.2	Расстановка приоритетов внутри ИТ бюджета	Удостоверится в том, что в организации существует процесс расстановки приоритетов в ИТ	• Реализован ли на практике процесс принятия решений при расстановки приоритетов в формировании ИТ бюджета?

№	Контроль	Цель контроля	Критерии оценки
		бюджете.	
PO 5.3	Формирование ИТ бюджета	Убедится в реализации практики по формированию ИТ бюджета в соответствии с бизнес требованиями организации.	• В организации внедрен ежегодный процесс по формированию ИТ бюджета?
PO 5.4	Управление затратами	Необходимо убедится в том, что в организации внедрен процесс управления затратами, проводя сравнения текущих затрат и бюджетов.	• Внедрен ли в организации процесс управления затрат/выгод?
			• Проводиться ли в организации мониторинг затрат и отчетность по его итогам?
PO 5.5	Управление преимуществами	Удостоверится в том, что в организации на практике реализован процесс мониторинга преимуществ, получаемых в результате использования возможностей ИТ.	• Проводится ли процесс мониторинга преимуществ, получаемых при использовании ИТ?
			• Документирован ли, согласован и оформлен в виде отчета вклад ИТ в бизнес?

PO6. Информирование о целях и направлениях развития ИТ

Процесс информирования реализуется для объяснения миссии, целей услуг, политики и процедур в области ИТ. Информирование поддерживает достижение целей ИТ и обеспечивает лучшее понимание ИТ-рисков, целей и направления развития. Процесс обеспечивает соответствие законодательству и нормативным требованиям. Оценка процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 10. Контроли ИТ-процесса «Информирование о целях и направлениях развития ИТ».

Таблица 10. Контроли ИТ-процесса «Информирование о целях и направлениях развития ИТ»

№	Контроль	Цель контроля	Критерии оценки
PO 6.1	ИТ политика и среда контроля	Необходимо удостоверится, что в организации определены элементы контроля в соответствии с философией корпоративного управления и стилем руководства.	• Определены ли в организации элементы среды контроля? • Включают ли элементы контроля ожидания/требования в отношении: ▪ пользы от ИТ инвестиций; ▪ рисков; ▪ целостности; ▪ компетентности персонала; ▪ отчетности и ответственности.
PO 6.2	Методология управления рисками в области ИТ	Убедится в том, что в организации разработана и поддерживается методология управления рисками в области ИТ.	• Разработана ли в организации методология управления рисками в области ИТ?

№	Контроль	Цель контроля	Критерии оценки
PO 6.3	Управление ИТ политиками	Удостоверится в том, что в организации разработан комплекс мер для поддержки ИТ стратегии.	• Разработан ли в организации комплекс политик для поддержки стратегии ИТ, включающий: ▪ описание целей; ▪ роли и обязанности; ▪ исключительные процессы; ▪ подход к вопросам совместимости; ▪ ссылки на конкретные процедуры; ▪ стандарты и руководства в области ИТ.
PO 6.4	Внедрение политик, стандартов и процедур	Необходимо удостоверится в том, что в организации внедрены, поняты и приняты политики, стандарты и процедуры в области ИТ.	• Существует ли в организации план по внедрению политик, стандартов и процедут?
			• Существуют ли процедуры для определения соответствия действий персонала с политиками, процедурами и стандартами?
			• Составлены ли политика безопасности и внутреннего контроля?
			• Разработана ли и внедрена политика по правам интеллектуальной собственности?
PO 6.5	Информирование о целях ИТ и направлении развития	Удостоверится, что в организации проводится информирование заинтересованных сторон о целях и направления развития ИТ.	• В организации существует программа по повышению осведомленности заинтересованных сторон о целях и направления развития в области ИТ?

PO7. Управление персоналом

Управление осуществляется посредством применения определенных и согласованных практик по набору, обучению, оценке эффективности, продвижению и увольнению персонала. Данный процесс относится к числу критичных, так как кадры являются важным активом, а управление и среда внутреннего контроля в значительной степени зависят от мотивации и компетентности персонала. Оценка процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 11. Контроли ИТ-процесса «Информирование о целях и направлениях развития ИТ».

Таблица 11. Контроли ИТ-процесса «Информирование о целях и направлениях развития ИТ»

№	Контроль	Цель контроля	Критерии оценки
PO 7.1	Набор и удержание персонала	Необходимо убедится, что в организации проводится управление процессами подбора и найма ИТ персонала .	• Проводится ли процесс набора и найма ИТ персонала в соответствии с общей кадровой политикой и процедурами?
PO 7.2	Компетентность персонала	Удостоверится в том, что персонал обладает достаточной	• Определены ли основные требования к компетентности ИТ персонала?

№	Контроль	Цель контроля	Критерии оценки
		компетентностью для исполнения своих обязанностей.	• Проводятся ли проверки ИТ персонала с целью удостоверится, что персонал обладает достаточной компетентностью для исполнения своих обязанностей?
PO 7.3	Распределение обязанностей	Необходимо удостоверится в том, что в организации определены и осуществляется надзор за ролями и обязанностями.	• Определены ли роли и обязанности ИТ персонала в должностных инструкциях?
			• Осуществляется ли в организации надзор: ▪ за ролями и обязанностями ИТ персонала; ▪ за соблюдение требований политик и процедур организации; ▪ профессионального опыта и профессиональной этики.
PO 7.4	Обучение персонала	Необходимо удостоверится, что в организации проводится обучение ИТ персонала.	• Проводится ли организации введение в курс дел при найме и ИТ персонал? • Обеспечивается ли ИТ персонал специальными курсами обучения по усовершенствованию знаний, навыков, мерам внутреннего контроля и обеспечения безопасности необходимых для достижения бизнес целей?
PO 7.5	Зависимость от отдельных сотрудников	Необходимо убедится, что в организации минимизированы риски зависимости от отдельных сотрудников.	• Обеспечивается ли достаточная подготовка или дублирование определенных ключевых сотрудников в случае их недоступности?
			• Проводится ли в организации документирование знаний сотрудников ИТ подразделения?
			• Проводится ли в организации процедура обмен опытом и планирования на случай увольнений?
PO 7.6	Проверка персонала на предмет допуска к работе	Удостоверится в том, что в организации проводится проверка персонала на предмет допуска к работе.	• Проводится ли в организации процедура проверки персонала на выполнение определенных задач (соответствие квалификации, образование, опыт)?
PO 7.7	Оценка эффективности работы персонала	Убедится, что в организации проводится регулярная оценка эффективности работы персонала.	• Проводится ли на регулярной основе оценка эффективности работы сотрудников?
			• Получают ли сотрудники ИТ персонала инструктаж по увеличению эффективности работы?
PO 7.8	Переход на другую работу и увольнение	Удостоверится, что в организации предприняты надлежащие действия при переходе сотрудников на новую должность или при увольнении.	• Налажена ли передача знаний, перераспределение ответственностей и ликвидация прав доступа при переходе на другую работу или увольнении сотрудников?

PO8. Управление качеством

Разработана и поддерживается система управления качеством, которая включает надлежащие процессы и стандарты в области разработки и приобретения. Это достигается путем планирования, внедрения и поддержки системы управления качеством посредством четких требований к качеству, процедур и политик. Требования к качеству сформулированы и донесены до исполнителей в виде количественных и достижимых показателей. Постоянное совершенствование происходит в результате мониторинга, анализа и коррекции отклонений, а также информирования заинтересованных сторон о результатах. Управление качеством требуется для повышения ценности ИТ, а также постоянное совершенствование и прозрачность для заинтересованных сторон. Оценка процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 12. Контроли ИТ-процесса «Управление качеством».

Таблица 12. Контроли ИТ-процесса «Управление качеством»

№	Контроль	Цель контроля	Критерии оценки
PO 8.1	Система управления качеством	Удостоверится в том, что в организации создана и поддерживается система управления качеством.	• Внедрена ли в организации система управления качеством?
			• Определены ли требования и критерии качества?
			• Осуществляется ли мониторинг и измерение эффективности и адекватности системы управления качеством?
PO 8.2	ИТ стандарты и практики управления качеством	Убедится в том, что в организации определены и поддерживаются стандарты в области управления качеством.	• Определены ли в организации стандарты, процедуры в области управления качеством?
PO 8.3	Стандарты в области разработки и приобретения	Необходимо удостоверится в том, что в организации приняты и поддерживаются стандарты в области разработки и приобретения ИТ услуг.	• В организации приняты стандарты в области разработки и приобретения?
PO 8.4	Акцент на потребностях заказчика	Необходимо убедится, что в работе системы управления качеством сделан акцент на определение потребностей заказчиков.	• Проводится ли процедура определения потребностей заказчиков и нахождении соответствий между ними со ИТ стандартами и практиками?
			• В организации определены роли и обязанности при разрешении конфликтной ситуации между пользователем/заказчиком и ИТ подразделения?
PO 8.5	Постоянное совершенствование	Удостоверится в том, что в организации проводится постоянное совершенствование в области ИТ.	• Доводится ли до персонала общий план по повышению качества в области ИТ?

№	Контроль	Цель контроля	Критерии оценки
PO 8.6	Оценка уровня качества, мониторинг и обзор	Убедится в том, что в организации определены и внедрены на практике измерения для постоянного мониторинга соответствия уровня качества требованиям системы управления качеством.	• Осуществляется ли владельцами процессов измерение и мониторинг уровня качества?

PO9. Оценка и управление ИТ рисками

В рамках процесса должна быть создана и поддерживаться методология управления рисками. Задача методологии — документирование общего и согласованного уровня ИТ-рисков, плана по минимизации рисков и остаточных рисков. Любое потенциальное воздействие на достижение целей организации, вызванное незапланированным событием должно учитываться, анализироваться и оцениваться. Планы минимизации рисков направлены, прежде всего, на приведение остаточных рисков к приемлемому уровню. Результат оценки должен быть понятным заинтересованным сторонам и выражен в финансовых показателях, чтобы заинтересованные стороны могли определить приемлемый для себя уровень рисков. Оценка процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 13. Контроли ИТ-процесса «Оценка и управление ИТ рисками».

Таблица 13. Контроли ИТ-процесса «Оценка и управление ИТ рисками»

№	Контроль	Цель контроля	Критерии оценки
PO 9.1	Методология управления рисками в сфере ИТ	Необходимо удостоверится в том, что в организации разработана методология по управления ИТ рисками.	• Разработана ли в организации методология по управлению рисками?
PO 9.2	Организация рисковой среды	Необходимо убедиться, что организована среда, в которой применяется методология по оценки рисков.	• Существует ли в организации среда по оценки рисков?
PO 9.3	Идентификация происшествий	Удостоверится в том, что в организации идентифицированы происшествия (существенные угрозы, которые могут реализоваться на наиболее уязвимых участках) с точки зрения потенциального негативного воздействия на цели или на текущую деятельность организации.	• В организации существует определенный подход к идентификации ИТ и ИБ угроз?
			• Документируются и обновляются соответствующие угрозы в карте рисков?
PO 9.4	Оценка рисков	Необходимо убедится в том, что в организации проводится регулярная оценка вероятности и последствия выявленных рисков в области ИТ.	• В организации существует определенный подход к оценке рисков?
			• Существует ли в организации процедуры определения вероятности и последствий рисков?

№	Контроль	Цель контроля	Критерии оценки
PO 9.5	Реагирование на риски	Удостоверится в том, что в организации разработан и поддерживается процесс реагирования на риски, предназначенный для минимизации рисков эффективными с точки зрения затрат методами на постоянной основе.	• Существует ли в организации процесс по реагированию на риски, включающий стратегию по: ▪ минимизации рисков; ▪ избеганию рисков; ▪ разделению или признанию риска. • Устанавливает ли процесс реагирования связанные с рисками ответственности, и учитывает ли предельные уровни допустимых рисков?
PO 9.6	Поддержка и мониторинг плана обработки рисков	Убедится, что в разработан и поддерживается план обработки рисков.	• В организации разработан план по обработке рисков?
			• Установлены ли приоритеты и спланированы ли контрольные мероприятия для реализации должного реагирования на риски, включающие определение затрат, выгод и ответственность исполнителей?
			• Имеют ли контрольные мероприятия своих владельцев?
			• Отчитываются ли перед высшим руководством в случае отклонений от плана?

PO10. Управление проектами

Разработана методология управления всеми ИТ-проектами и программами. Методология обеспечивает координацию между отдельными проектами в соответствии с приоритетами. Она включает в себя план, оценку ресурсов, определение результатов, согласование со стороны пользователей. План предоставлен в виде этапов, управление качеством, формализованный план тестирования, обзор, результат тестирования и анализ результатов проекта после внедрения. Данный подход ведет к минимизации риска непредвиденных затрат и приостановок реализации проекта, улучшает взаимодействие бизнеса и конечных пользователей, обеспечивает качественные результаты проекта и повышает их вклад в инвестиционные программы, связанные с ИТ. Оценка процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 14. Контроли ИТ-процесса «Управление проектами».

Таблица 14. Контроли ИТ-процесса «Управление проектами»

№	Контроль	Цель контроля	Критерии оценки
PO 10.1	Методология управления программами	Необходимо удостоверится в том, что в организации осуществляется поддержка программы проектов, связанных с ИТ инвестициями, путем определения, оценки, расстановки приоритетов, отбора, предложения, управления и контроля над проектами.	• Существует ли в организации методология управления программами проектов?

№	Контроль	Цель контроля	Критерии оценки
PO 10.2	Методология управления проектами	Убедится в том, что в организации разработана и поддерживается методология управления проектами.	• Разработана ли в организации методология управления проектами?
			• Определяет ли методология масштаб и границы управления проектами, а так же конкретные методы, которые могут быть адаптированы для каждого отдельного проекта?
PO 10.3	Подход к управлению проектами	Удостоверится в том, что в организации разработан управленческий подход, адекватный масштабам, сложности и нормативным требованиям, предъявляемым к каждому из проектов.	• Существует ли в организации подход к управлению проектами, включающий: ▪ описание должностных обязанностей исполнителей; ▪ отчетность перед спонсором программы; ▪ управляющий комитет; ▪ проектный офис и руководителя проекта; ▪ механизмы (такие как отчетность и анализ результатов этапов проекта).
			• Все ли ИТ проекты имеют спонсоров с полномочиями, достаточными для самостоятельной реализации проекта?
PO 10.4	Комитет заинтересованных сторон	Необходимо убедится, что при определении и реализации проекта в контексте общей инвестиционной программы заручаются поддержкой и участием заинтересованных сторон.	• Организован ли в организации комитет заинтересованных сторон?
PO 10.5	Представления о масштабах проекта	Необходимо убедится в том, что в организации определены и документально зафиксированы представления о характере и масштабах проекта.	• В организации документально зафиксированы представления о характере и масштабах проекта?
			• Масштабы проекта формально утверждены спонсорами программы и проекта?
PO 10.6	Выделение фаз реализации проекта	Необходимо удостоверится в том, что в организации выделены основные фазы при реализации проекта и заинтересованные стороны проинформированы.	• Определены ли в организации фазы реализации проекта?
PO 10.7	Интегрированный план проекта	Удостоверится, что в организации существует формализованный и утвержденный план проекта.	• Утвержден ли план проекта в соответствии с методологией управления программой и проектом?
PO 10.8	Ресурсы проекта	Убедится в том, что в рамках реализации проекта определены ответственные лица, взаимосвязи, права и критерии оценки в отношении членов проектной группы.	• Определены ли члены официальной проектной команды и ответственные за проект?

№	Контроль	Цель контроля	Критерии оценки
РО 10.9	Управление рисками проекта	Необходимо убедится в том, что в организации устранены или минимизированы специфические для каждого конкретного проекта риски.	• Формализована ли программа управления рисками проекта?
			• Определены ли и документированы риски, угрожающие управлению проектом и его целям?
РО 10.10	План обеспечения качества проекта	Удостоверится в том. что в организации подготовлен план обеспечения качества проекта.	• Подготовлен ли в организации план управления качеством, в котором будет описана система качества проекта и ее реализация на практике?
			• Согласован ли план со всеми сторонами, участвующими в интегрированном плане проекта?
РО 10.11	Контроль над внесением изменений в проект	Убедится в том, что в организации разработана и поддерживается система контроля за внесением изменений для каждого проекта.	• Все ли изменения, касающиеся основ проекта (стоимости, графика, масштабов, качества) были изучены, утверждены и включены в интегрированный план проекта?
РО 10.12.	Планирование обеспечения достаточной уверенности в отношении качества внедряемых систем	Следует удостовериться в том, что в организации определены методы получения достаточной уверенности в отношении качества новых или модифицированных внедряемых систем.	• Определены ли методы получения достаточной уверенности в отношении качества новых или модифицированных внедряемых систем?
РО 10.13	Оценка эффективности проекта, отчетность и мониторинг	Необходимо удостоверится в том, что в организации проводится оценка эффективности проекта.	• Выявляются ли отклонения от плана проекта?
			• Проводиться ли оценка влияния отклонений для проекта и программы в целом и отчетность о результатах перед заинтересованными сторонами?
			• Реализовываются ли и анализируются корректирующие действия, в соответствии с методологией управления программой и проектом?
РО 10.14	Завершение проекта	Необходимо убедится, что по завершению проекта заинтересованные стороны оценили, достиг ли проект поставленных целей и выгод.	• Проводится ли информирование обо всех значительных действиях по достижению запланированных результатов проекта и выгод программы?
			• Документируется ли опыт, полученный в ходе реализации проекта?

4.4.2 AI. Приобретение и внедрение

AI1. Выбор решений по автоматизации

Потребность в новом приложении или функциональности требует эффективного анализа соответствия бизнес требованиям перед приобретением или разработкой. Данный процесс включает в себя определение потребностей, изучение альтернативных источников, технологическое и экономическое обоснование, проведение анализа рисков, затрат и выгод, а также окончательное решение: «разрабатывать» или «покупать ». Все эти меры позволяют организации минимизировать затраты на приобретение и внедрение решений, одновременно гарантируя соответствие поставленным бизнес целям. Оценка процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 15. Контроли ИТ-процесса «Выбор решений по автоматизации».

Таблица 15. Контроли ИТ-процесса «Выбор решений по автоматизации»

№	Контроль	Цель контроля	Критерии оценки
AI 1.1	Определение и поддержка бизнес требований к функциональности	Удостоверится в том, что в организации определены и выстроены приоритеты при выборе решения по автоматизации.	• Определяются ли приоритеты при выборе решения? • Согласовываются ли требования к функциональности решения?
AI 1.2	Результаты анализа рисков	Необходимо убедится, что в организации проводится анализ рисков, связанных с реализацией требований и разработкой решений по автоматизации.	• Проводится ли в организации анализ рисков для угроз безопасности, потенциальных уязвимостей для решения по автоматизации?
AI 1.3	Исследование обоснованности и разработка альтернативного плана действий	Необходимо удостоверится в том, что в организации проводится исследование обоснованности в выборе решения по автоматизации.	• Проводится ли руководством, при содействии ИТ подразделения, оценка обоснованности решения по автоматизации и альтернативные планы действий? • Производится ли анализ затрат и выгод для каждой альтернативы, рассматриваемой для удовлетворения установленным требованиям?
AI 1.4	Требования, обоснование и утверждение	Следует убедиться, что процесс предполагает утверждение требований к функциональности решения по автоматизации со стороны корпоративного спонсора.	• Требования к функциональности утверждаются корпоративным спонсором?

AI2. Приобретение и поддержка программных приложений

Приложения разрабатываются в соответствии с бизнес требованиями. Данный процесс состоит из проектирования, требований к мерам контроля приложений, требований по безопасности, а также, разработки и конфигурирования в соответствии со стандартами. Это позволяет организациям должным образом поддерживать бизнес операции при помощи правильных автоматизированных приложений. Оценка процесса осуществляется путем анализа

эффективности контролей, представленных в Таблица 16. Контроли ИТ-процесса «Приобретение и поддержка программных приложений».

Таблица 16. Контроли ИТ-процесса «Приобретение и поддержка программных приложений»

№	Контроль	Цель контроля	Критерии оценки
AI 2.1	Общий дизайн приложений	Необходимо убедится, что требования в спецификации на приобретение программного обеспечения установлены с учетом направления технологического развития организации и информационной архитектуры.	• Спецификации утверждаются руководством?
			• Проводится ли пересмотр дизайна приложения в случае существенных технических или логических несоответствий, выявленных в процессе разработки или эксплуатации?
AI 2.2	Детальный дизайн приложений	Необходимо удостоверится в том, что в организации подготовлен детальный дизайн приложений и технические требования к программному обеспечению.	• Подготавливается ли детальный дизайн приложения и технические требования к программному обеспечению перед приобретением?
			• Утверждаются ли требования к программному обеспечению?
AI 2.3	Меры контроля приложений	Убедится в том, что в организации внедрены меры контроля приложений.	• Внедрены ли в организации меры контроля приложений?
AI 2.4	Безопасность и доступность приложений	Необходимо убедится в том, что в организации разработаны и утверждены требования к безопасности и доступности приложений.	• Выявляются ли требования к безопасности и доступности приложений в соответствии с выявленными рисками и принятой в организации классификацией данных, информационной архитектурой, архитектурой информационной безопасности и уровнем приемлемых рисков? • Утверждаются ли требования к безопасности и доступности приложений перед приобретением?
AI 2.5	Настройка и внедрение приобретенного программного обеспечения	Следует удостовериться, что в организации проведена настройка и внедрение программного обеспечения в соответствии с бизнес целями.	• Внедрение программного обеспечения проводится в строгом соответствии с утвержденными требованиями?
AI 2.6	Значительные обновления существующих систем	Удостоверится в том, что значительные обновления существующих систем проводятся по тем же процедурам что и процесс разработки.	• Разработаны ли в организации процедуры, определяющие действия при значительных обновлениях существующих систем? • Соответствуют ли данные процедуры тем же процедурам процесса разработки, как и в случае с полностью новыми системами?
AI 2.7	Разработка программных приложений	Следует убедиться в том, что программное обеспечение разработано в соответствии с проектными спецификациями, стандартами разработки и документации, требованиями системы обеспечения качества и	• Разрабатывается ли программное приложение в соответствии с техническими спецификациями?
			• Изучены ли все нормативные и договорные аспекты, применимые к приложениям, разработанные третьими

№	Контроль	Цель контроля	Критерии оценки
		утвержденными стандартами.	сторонами?
AI 2.8	Обеспечение качества приложений	Необходимо удостоверится в том, что в организации реализован план по обеспечению качества приложений.	• Реализован ли на практике план по обеспечению качества?
			• Сторонние производители, поставляющие программные приложения, имеют соответствующие процедуры для проверки, защиты и поддержки целостности программного обеспечения?
AI 2.9	Управление требованиями к приложениям	Убедится, что в организации проводится отслеживание статуса требований к приложениям в процессе проектирования, разработки и внедрения.	• Проводиться ли утверждение требований к приложению в соответствии с установленным процессом управления изменениями ?
AI 2.10	Поддержка приложений	Необходимо убедиться, что в организации разработана стратегия и план поддержки приложения.	• Существует ли в организации стратегия и план поддержки приложения?

AI 3. Приобретение и обслуживание технологической инфраструктуры

Организации имеют процессы, предназначенные для приобретения, внедрения и обновления технологической инфраструктуры. Данные процессы требуют планового подхода к приобретению, поддержке и защите инфраструктуры в соответствии с заранее согласованными технологическими стратегиями, обеспечением среды разработки и тестирования. Оценка процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 17. Контроли ИТ-процесса «Приобретение и обслуживание технологической инфраструктуры».

Таблица 17. Контроли ИТ-процесса «Приобретение и обслуживание технологической инфраструктуры»

№	Контроль	Цель контроля	Критерии оценки
AI 3.1	План приобретения технологической инфраструктуры	Необходимо удостоверится в том, что в организации разработан и утвержден план приобретения, внедрения и поддержки технологической инфраструктуры, .	• Разработан ли в организации план приобретения, внедрения и поддержки технологической инфраструктуры?
AI 3.2	Защита и доступность ресурсов инфраструктуры	Убедится, что в организации внедрены меры внутреннего контроля, безопасности и проверяемые показатели в процессе конфигурирования, интеграции и обслуживания аппаратного и инфраструктурного	• В организации проводиться мониторинг и оценка эксплуатации компонентов инфраструктуры?
			• Содержат ли и донесены ли должностные инструкции сотрудников, разрабатывающие и интегрирующие компоненты инфраструктуры, обязанности при использовании важных компонентов инфраструктуры?

№	Контроль	Цель контроля	Критерии оценки
		программного обеспечения.	
AI 3.3	Обслуживание инфраструктуры	Удостоверится в том, что в организации разработана стратегия и план обслуживания инфраструктуры.	• В организации разработан план обслуживания инфраструктуры?
			• Включает ли план ▪ периодические оценки соответствия технологической инфраструктуры потребностям бизнеса; ▪ управление обновлениями, ▪ стратегии обновления, ▪ риски, оценку уязвимостей; ▪ требования по безопасности?
AI 3.4	Тестовая среда	Необходимо убедится, что в организации созданы тестовая среда и среда разработки.	• В организации существует тестовая среда?
			• В организации существует среда разработки?

AI 4. Обеспечение выполнения операций

Знания о новых системах становятся доступными. Этот процесс требует производства документации и руководств для пользователей и персонала ИТ и проведения обучения правильному использованию приложений и инфраструктуры. Оценка процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 18. Контроли ИТ-процесса «Обеспечение выполнения операций».

Таблица 18. Контроли ИТ-процесса «Обеспечение выполнения операций»

№	Контроль	Цель контроля	Критерии оценки
AI 4.1	Планирование для операционных решений	Удостоверится в наличии разработанного плана по определению и документированию всех технических, операционных и пользовательских аспектов.	• В организации разработан план по определению и документированию всей технической, операционной информации?
AI 4.2	Передача знаний владельцам систем	Необходимо убедится, что в организации проводится передача знаний владельцам ИТ сервисов.	• Подготавливаются, обновляются и передаются руководства для владельцам ИТ сервисов?
AI 4.3	Передача знаний конечным пользователям	Убедится в том, что в организации передаются знания и навыки по использованию ИТ сервисов.	• Подготавливаются, обновляются и передаются руководства для пользователей, являющиеся частью разработки, внедрения и модификации каждой ИС?
AI 4.4	Передача знаний операционному и обслуживающему	Следует удостоверится в том, что в организации осуществляется передача знаний	• Подготавливаются ли и обновляются обучающие материалы для операционного и обслуживающего персонала?

№	Контроль	Цель контроля	Критерии оценки
	персоналу	операционному и обслуживающему персоналу по поддержке и обслуживанию ИТ сервисов.	• Обучается ли персонал согласно определенному плану обучения по поддержке и обслуживанию ИТ сервисов?

AI 5. Поставки ИТ ресурсов

Должны быть обеспечены поставки ИТ-ресурсов, включая персонал, аппаратное и программное обеспечение, услуги. Это требует определения и внедрения процедур поставок, отбора поставщиков, регламентации договорных требований и с процесса приобретения. Соблюдение этих условий дает гарантии того, что организация обладает всеми необходимыми ИТ-ресурсами. Оценка процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 19. Контроли ИТ-процесса «Обеспечение выполнения операций».

Таблица 19. Контроли ИТ-процесса «Обеспечение выполнения операций»

№	Контроль	Цель контроля	Критерии оценки
AI 5.1	Контроль за поставками	Необходимо удостоверится, что в организации разработаны и следуют процедурам и стандартам в области приобретения ИТ инфраструктуры.	• Разработаны ли в организации процедуры и стандарты по закупкам ИТ инфраструктуры, аппаратного и программного обеспечения, а также услуг, необходимых организации, соответствующие общекорпоративному процессу осуществления поставок и стратегии в области приобретений товаров и услуг?
AI 5.2	Управление контрактами с поставщиками	Удостоверится в том, что в организации установлена процедура по заключению, изменению и прекращению контрактов с поставщиками.	• Установлена ли в организации процедура по заключению, изменению и прекращению контрактов с поставщиками, включающая: ▪ правовые, финансовые, организационные, документальные аспекты; ▪ вопросы эффективности, безопасности, интеллектуальной собственности; ▪ прекращения ответственности и обязательств? • Проходят ли контракты согласование со стороны сотрудников по правовым вопросам?
AI 5.3	Выбор поставщиков	Следует удостовериться, что организацией проводится отбор поставщиков в соответствии с рыночной и формализованной практикой.	• Проводится ли в организации оценка поставщиков?
AI 5.4	Приобретение ИТ ресурсов	Убедиться в том, что в организации обеспечивается защита и поддержка интересов организации во всех договорных соглашениях на должном уровне.	• Существует ли план приобретения ИТ ресурсов? • Следует ли приобретение программного и аппаратного обеспечения согласно утвержденной процедуре?

AI 6. Управление внесением изменений

Все изменения, включая обслуживание в аварийных ситуациях и исправления, относящиеся к инфраструктуре и приложениям в среде промышленной эксплуатации, должны управляться и контролироваться формализованным способом. Изменения (включая изменения в процедурах, процессах, системах) должны протоколироваться, оцениваться и санкционироваться до своего внедрения и анализироваться по плановым показателям после реализации. Оценка процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 20. Контроли ИТ-процесса «Управление внесением изменений».

Таблица 20. Контроли ИТ-процесса «Управление внесением изменений»

№	Контроль	Цель контроля	Критерии оценки
AI 6.1	Стандарты и процедуры изменений	Необходимо удостоверится, что в организации определены формализованные процедуры в области управления изменениями.	• В организации установлены процедуры в области управления изменениями для стандартизованной обработки всех запросов (включая обслуживание и обновления) на изменения?
AI 6.2	Оценка последствий, расстановка приоритетов и авторизация	Убедиться, что все изменения категорированы, расставлены по приоритетам и авторизованы.	• Оценены ли возможные последствия внесения изменений?
			• Все запросы на изменения инициированы и контролируются?
			• Авторизованы ли внесенные изменения?
AI 6.3	Аварийные изменения	Удостоверится в том, что в организации установлен процесс внесения аварийных изменений.	• Существует ли в организации документ, описывающий процедуру внесения аварийных изменений?
AI 6.4	Мониторинг и отчетность по статусу изменений	Убедиться, что принятые изменения реализованы в соответствии с планом внесения изменений.	• Проводится ли информирования о статусе принятых, находящихся в процессе и завершенных изменений заинтересованным сторонам? • Все ли принятые изменения реализованы в соответствии с планом внесения изменений?
AI 6.5	Завершение изменений и документирование	Следует убедиться в том, что в организации проводится обновление связанной с изменениями системной и пользовательской документация.	• Постоянно обновляются документация и процедуры по внесению изменений?

AI 7. Внедрение и приемка решений и изменений

Новые системы должны быть готовы к эксплуатации после завершения разработки. Для этого необходимо тестирование в выделенной тестовой среде подходящих тестовых данных, определение инструкций по миграции, планирование выхода версий и внедрение в промышленную эксплуатацию, а также анализ результатов внедрения. Это обеспечит соответствие эксплуатируемых систем ранее сформулированным ожиданиям и требованиям.

Оценка процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 21. Контроли ИТ-процесса «Внедрение и приемка решений и изменений».

Таблица 21. Контроли ИТ-процесса «Внедрение и приемка решений и изменений»

№	Контроль	Цель контроля	Критерии оценки
AI 7.1	Обучение	Необходимо удостоверится в том, что в организации проводится обучение по внесенным изменениям в любой ИС.	• Проводится ли в организации обучение в соответствии с определенным планом обучения по разработке, внедрению или модификации любой информационной системы?
AI 7.2	План тестирования	Следует убедится, что в организации разработан и утвержден план тестирования изменений.	• Утвержден ли в организации план тестирования изменений определяющий роли, обязанности, ожидаемые результаты на входе и выходе системы? • Утвержден ли план заинтересованными сторонами?
AI 7.3	План внедрения	Удостоверится, что в организации разработан и утвержден план внедрения изменений.	• Разработан ли план внедрения/ отмены изменений? • В организации утвержден план внедрения изменений?
AI 7.4	Среда тестирования	Убедится в существовании среды тестирования изменений в организации.	• Создана ли безопасная среда тестирования, содержащая элементы промышленной среды?
AI 7.5	Перенос системы и данных	Удостоверится, что в организации запланирован перенос данных и инфраструктурный переход как часть методов разработки.	• Запланирован ли перенос данных и инфраструктурный переход как часть методов разработки, принятых в организации, включая контрольный журнал, варианты отмены изменений и возвращения в прежнее состояние?
AI 7.6	Тестирование изменений	Следует убедиться, что в организации проводится тестирование до внедрения в эксплуатационную среду.	• Проводится ли тестирование изменений независимо друг от друга в соответствии с определенным ранее планом тестирования? • Включает ли план аспекты, связанные с безопасностью и производительностью?
AI 7.7	Тестирование перед окончательным внедрением	Необходимо убедится, что в организации проводится тестирование изменений перед окончательным внедрением.	• Исправляются ли существенные ошибки, выявленные в процессе тестирования? • Оцениваются ли результаты тестирования заинтересованными сторонами?
AI 7.8	Ввод в эксплуатацию	Удостоверится, что в организации контролируется ввод изменений в среду промышленной эксплуатации в соответствии с планом внедрения.	• Получается ли подтверждение от основных заинтересованных сторон, таких как пользователи, владельцы систем и операционное руководство перед вводом в эксплуатацию?
AI 7.9	Анализ результатов	Убедится в том, что в организации проводится анализ	• Установлены ли в организации процедуры анализа

№	Контроль	Цель контроля	Критерии оценки
	внедрения	результатов внедрения изменений.	результатов внедрения, как элемента плана внедрения?

4.4.3 DS. Эксплуатация и сопровождение

DS 1. Определение и управление уровнем обслуживания

Эффективная коммуникация между руководством ИТ и пользователями услуг становится возможной благодаря документально оформленному соглашению об ИТ-услугах и уровне обслуживания. Этот процесс включает в себя мониторинг и отчетность перед заинтересованными сторонами по достижении заявленного уровня обслуживания. Данный процесс обеспечивает соответствие между ИТ-услугами и связанными с ними бизнес требованиями. Оценка процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 21. Контроли ИТ-процесса «Внедрение и приемка решений и изменений».

Таблица 22. Контроли ИТ-процесса «Определение и управление уровнем обслуживания»

№	Контроль	Цель контроля	Критерии оценки
DS 1.1	Методология управления уровнем обслуживания	Удостоверится, что в организации разработана и поддерживается методология управления уровнем обслуживания.	• Разработана ли методология управления уровнем обслуживания, включающая: ▪ процессы формирования требований к услугам; ▪ определения самих услуг; ▪ соглашения об уровне обслуживания (SLA); ▪ соглашения операционного уровня (OLA); ▪ определение источников финансирования. • Определяет ли методология организационную структуру управления уровнем обслуживания, должностные обязанности, цели и ответственность внутренних и внешних поставщиков и потребителей услуг?
DS 1.2	Определение услуг	Необходимо убедится в том, что в организации ИТ услуги определены.	• Осуществляется ли централизованное хранение ИТ услуг посредством каталога (портфеля) услуг?
DS 1.3	Соглашения об уровне обслуживания	Следует убедиться в том, что в организации сформулированы и заключены соглашения об уровне обслуживания для всех критичных ИТ услуг.	• Соглашения об уровне обслуживания заключены со всеми поставщиками критичных ИТ услуг? • Включают ли в себя соглашения: ▪ обязательства пользователей; ▪ требования по сервисному обслуживанию; ▪ количественные и качественные показатели ▪ оценки уровня обслуживания для заинтересованных сторон; ▪ финансирование и коммерческие условия; ▪ перечень должностных лиц и их обязанностей, включая надзор за исполнением соглашения об уровне обслуживания? • Рассмотрены ли в соглашении такие аспекты, как доступность, надежность, производительность, возможности для роста, уровни поддержки,

№	Контроль	Цель контроля	Критерии оценки
			обеспечение непрерывности, безопасность и ограничения требований?
DS 1.4	Соглашения операционного уровня	Необходимо убедится, что в организации сформулированы соглашения операционного уровня, которые определяют, как технически будут оказываться услуги.	• Соглашения операционного уровня заключены со всеми внутренними подразделениями?
DS 1.5	Мониторинг и отчетность по выполнению соглашений об уровне обслуживания	Необходимо удостоверится, что в организации установлен процесс мониторинга и отчетности по исполнению соглашения об уровне обслуживания.	• Проводится ли мониторинг и отчетность по уровню облуживания заинтересованными сторонами? • Предоставляются ли отчеты в формате, удобном для понимания заинтересованных сторон?
DS 1.6	Рассмотрение соглашений об уровне обслуживания и контрактов	Убедится в том, что в организации регулярно проводиться рассмотрение соглашений об уровне обслуживания.	• Своевременно ли пересматриваются соглашения об уровне обслуживания с поставщиками?

DS 2. Управление услугами сторонних организаций

Задача обеспечения соответствия между услугами, предоставляемыми сторонними организациями (поставщиками и партнерами) и существующими бизнес требованиями нуждается в эффективном процессе управления. Данный процесс заключается в четком определении ролей, обязанностей и ожиданий в рамках соглашений со сторонними организациями, а также в изучении и анализе этих соглашений с точки зрения эффективности и соответствия требованиям. Эффективное управление услугами сторонних организаций минимизирует корпоративные риски, связанные с плохим функционированием поставщиков. Оценка процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 23. Контроли ИТ-процесса «Управление услугами сторонних организаций».

Таблица 23. Контроли ИТ-процесса «Управление услугами сторонних организаций»

№	Контроль	Цель контроля	Критерии оценки
DS 2.1	Определение взаимоотношений с поставщиками	Необходимо удостоверится в том, что все услуги, предлагаемые поставщиками, классифицированы.	• Классифицированы ли услуги, предоставляемые поставщиками по категориям: тип поставщика, значимость и критичность?
DS 2.2	Управление взаимоотношениями с поставщиками	Убедится в том, что в организации формализован процесс управления взаимоотношениями с каждым	• Формализован ли в организации процесс управления взаимоотношениями с каждым поставщиком (например, посредством соглашения об уровне обслуживания)?

№	Контроль	Цель контроля	Критерии оценки
		постащиком.	
DS 2.2	Управление рисками, связанными с поставщиками	Следует убедиться, что в организации проводится процедура по выявлению и минимизации рисков, связанных с возможностями поставщиков не продолжать эффективное оказание услуг безопасным и эффективным образом.	• Соответствуют ли контракты с поставщиками распространенным корпоративным стандартам, нормативным и регулирующим требованиям?
			• Включает ли управление рисками в себя соглашения о неразглашении, договора по условному депонированию (escrow contracts), соответствие требованиям безопасности, альтернативных поставщиков, условия штрафов и бонусов?
DS 2.3	Мониторинг эффективности поставщиков	Удостоверится, что в организации внедрен процесс мониторинга оказания услуг.	• Проводится ли мониторинг предоставляемых услуг сторонней организацией?

DS 3. Управление производительностью и мощностями

Потребность в управлении производительностью и мощностями обуславливает существование процесса регулярного изучения текущего состояния производительности и мощностей ИТ-ресурсов. Данный процесс включает в себя прогнозирование будущих потребностей на основе данных о рабочей нагрузке и требований по хранению и непрерывности. Данный процесс призван обеспечить уверенность в том, что информационные ресурсы, поддерживающие исполнение бизнес требований, будут доступны на постоянной основе. Оценка процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 24. Контроли ИТ-процесса «Управление производительностью и мощностями».

Таблица 24. Контроли ИТ-процесса «Управление производительностью и мощностями»

№	Контроль	Цель контроля	Критерии оценки
DS 3.1	Планирование производительности и мощностей	Убедится, что осуществляется планирование для анализа производительности и мощностей ИТ ресурсов.	• Определены ли требования по доступности и производительности?
			• Разработан ли план по обеспечению непрерывности?
DS 3.2	Текущее состояние производительности и мощностей	Следует убедится в том. что в организацией проводится оценка производительность и мощности ИТ ресурсов.	• Установлен ли процесс по постоянному мониторингу и отчетности по производительности ИТ ресурсов?
DS 3.3	Прогноз производительности и мощностей	Необходимо удостоверится, что в организации ведется регулярное прогнозирование производительности и мощностей ИТ ресурсов.	• Прогнозируется ли уровень нагрузки на ИТ?
			• Осуществляется ли процесс управление ИТ ресурсами?
DS 3.4	Доступность ИТ ресурсов	Удостоверится в том, что организация обеспечена	• Осуществляется ли управление доступностью ИТ ресурсов?

№	Контроль	Цель контроля	Критерии оценки
		требуемыми уровнями производительности и мощности.	• Учитывают ли управление доступностью вопросы, связанные с мощностями и производительностью отдельных ИТ ресурсов?
DS 3.5	Мониторинг и отчетность	Необходимо убедится, что в организации осуществляется постоянный мониторинг производительности и мощностей ИТ ресурсов	• Проводится ли мониторинг производительности и мощностей ИТ ресурсов?
			• Предоставляется ли отчетность по производительности и мощности ИТ ресурсов?

DS4. Обеспечение непрерывности ИТ сервисов

Потребность в обеспечении непрерывности ИТ-сервисов предполагает разработку, поддержку и тестирование планов по непрерывности обслуживания, использование сторонних резервных хранилищ данных и периодическое обучение по плану непрерывности обслуживания. Эффективные процессы обслуживания минимизируют вероятность и последствия существенных перебоев в предоставлении ИТ-услуг для корпоративных функций и процессов. Оценка процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 25. Контроли ИТ-процесса «Обеспечение непрерывности ИТ сервисов»

Таблица 25. Контроли ИТ-процесса «Обеспечение непрерывности ИТ сервисов»

№	Контроль	Цель контроля	Критерии оценки
DS 4.1	Методология непрерывности обслуживания ИТ	Убедится, что в организации разработана методологию непрерывности обслуживания ИТ, которая будет поддерживать управление непрерывностью бизнеса в масштабах организации на постоянной основе.	• В организации разработана методология по непрерывности обслуживания ИТ? • Включает ли в себя методология: ▪ перечень должностных лиц внутренних и внешних поставщиков услуг и их обязанностей; ▪ процессы планирования, в рамках которых вырабатываются правила и форматы документирования, тестирования и выполнения мер по восстановлению после аварийных ситуаций; ▪ планы по непрерывности обслуживания ИТ?
DS 4.2	Планы непрерывности обслуживания ИТ	Удостоверится, что разработаны планы непрерывности обслуживания ИТ, на основе методологии и с целью минимизации возможных последствий крупных прерываний для бизнес функций и процессов.	• В организации разработаны стратегия, подход и план по обеспечению непрерывности ИТ сервисов? • Охватывают ли планы использование руководств пользователей, перечень должностных лиц и их обязанностей, процессы взаимодействия и подходы к тестированию?
DS 4.3	Критические ИТ ресурсы	Необходимо убедится, что в организации сконцентрировано внимание на наиболее критические аспекты плана обеспечения непрерывности обслуживания ИТ.	• Идентифицированы ли в организации критические ИТ ресурсы? • Соответствуют ли время отклика и время на восстановление критических ИТ ресурсов приоритетным потребностям бизнеса?
DS 4.4	Поддержка плана непрерывности	Необходимо удостоверится, что в организации определены и	• Осуществляется ли обновление плана на

№	Контроль	Цель контроля	Критерии оценки
	обслуживания ИТ	исполняются контрольные процедуры по изменениям, с целью поддержки плана непрерывности обслуживания ИТ в актуализированном виде.	постоянной основе?
DS 4.5	Тестирование плана непрерывности обслуживания ИТ	Следует убедиться, что проводиться регулярное тестирование плана, с целью удостовериться в возможности эффективного восстановления ИТ систем, выявить недостатки и убедиться в адекватности плана.	• Осуществляется ли тестирование плана по обеспечению непрерывности ИТ сервисов на постоянной основе?
DS 4.6	Обучение по плану непрерывности обслуживания ИТ	Удостоверится, что все заинтересованные стороны обеспечены возможностью регулярного обучения по плану непрерывности обслуживания ИТ, их ролям и обязанностям в случае инцидента или аварийной ситуации.	• Все ли заинтересованные стороны прошли курсы и смогут своевременно согласно плану среагировать в случае инцидента или аварийной ситуации?
DS 4.7	Распространение плана непрерывности обслуживания ИТ	Необходимо удостоверится, что обеспечена доступность плана по обеспечению непрерывности ИТ сервисов всем заинтересованным сторонам.	• План по обеспечению непрерывности ИТ сервисов доступен и распространен всем заинтересованным сторонам?
DS 4.8	Восстановление ИТ услуг после сбоя	Необходимо убедиться, что в период восстановления ИТ услуг необходимые действия распланированы.	• Разработан ли план восстановления ИТ услуг?
DS 4.9	Сторонние хранилища резервных данных	Убедится, что в организации используются сторонние хранилища для резервного хранения носителей данных, документации и других ИТ ресурсов.	• Установлено ли удаленное/стороннее хранилище для резервного хранения носителей данных, документации и других ИТ ресурсов?
DS 4.10	Анализ по результатам восстановления	Удостоверится, что руководством ИТ подразделения предприняты меры по оценке адекватности плана по успешному восстановлению работы ИТ службы после аварийной ситуации.	• Проводиться ли оценка адекватности плана по успешному восстановлению работы ИТ подразделения после аварийной ситуации?

DS 5. Обеспечение безопасности систем

Обеспечение целостности информации и защита ИТ-активов требуют процесса управления безопасностью. Данный процесс включает в себя установление и поддержку ролей и ответственностей в сфере ИТ-безопасности, политики, стандарты и процедуры. Управление безопасностью также включает проведение мониторинга безопасности и периодическое тестирование с последующей реализацией корректирующих мер в отношении выявленных слабых мест в обеспечении безопасности. Эффективное управление безопасностью позволит защитить все ИТ-активы и минимизировать воздействие на бизнес со стороны инцидентов и

уязвимостей в системе безопасности. Оценка процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 26. Контроли ИТ-процесса «Обеспечение безопасности систем»

Таблица 26. Контроли ИТ-процесса «Обеспечение безопасности систем»

№	Контроль	Цель контроля	Критерии оценки
DS 5.1	Управление ИТ безопасностью	Удостоверится, что управление ИТ безопасностью организовано на максимально возможном уровне.	• Соответствуют ли управление информационной безопасностью требованиям бизнеса? • Проведено ли обучение по вопросам информационной безопасности среди пользователей?
DS 5.2	План по ИТ безопасности	Убедится, что в организации разработан план по ИТ безопасности.	• Разработан ли в организации план по обеспечению ИТ безопасности, включающий ИТ инфраструктуру и корпоративную культуру обеспечения безопасности? • Внедрены ли в организации политики и процедуры в области безопасности? • Проводится ли в организации информирование заинтересованных сторон и пользователей о политиках и процедурах в области безопасности?
DS 5.3	Управление идентификацией	Следует удостовериться, что деятельность в ИТ системах может быть однозначно идентифицирована	• Разработаны ли и регламентированы правила по предоставлению доступа к ИТ ресурсам? • Соответствуют ли права на доступ пользователей к системам и данным определенным и документированным бизнес потребностям и должностным обязанностям? • Доступ пользователей, запрашиваемый руководством, подтвержден владельцем системы и предоставляется уполномоченным лицом в области безопасности?
DS 5.4	Управление учетными записями пользователей	Необходимо убедится, что в организации установлена процедура утверждения предоставляемых прав доступа со стороны владельцев данных или систем.	• Управление учетными записями осуществляется согласно утвержденной политике информационной безопасности? • Внедрены ли процедуру утверждения предоставляемых прав доступа со стороны владельцев данных или систем? • Осуществляется ли регулярный мониторинг всех учетных записей и связанных с ними прав и полномочий?
DS 5.5	Тестирование, надзор и мониторинг в сфере ИТ безопасности	Необходимо удостоверится, что в организации осуществляется тестирование и мониторинг в сфере	• Осуществляется ли в организации регистрация и мониторинг событий?

№	Контроль	Цель контроля	Критерии оценки
		ИТ безопасности.	
DS 5.6	Определение инцидентов в сфере безопасности	Удостоверится, что четко определены характеристики потенциальных инцидентов в сфере безопасности.	• Классифицированы ли инциденты информационной безопасности?
DS 5.7	Защита технологий безопасности	Необходимо убедится, что в организации обеспечена защита от взлома для технологий, связанных с безопасностью.	• Проводилась ли сертификация (аудит) системы информационной безопасности?
DS 5.8	Управление ключами криптозащиты	Необходимо удостоверится, что в организации определены политики и процедуры по управлению ключами криптозащиты.	• Установлены ли в организации политики и процедуры по управлению ключами криптозащиты, включающие определения по выпуску, изменению, отмене, уничтожению, распространению, сертификации, хранению, активации, использованию и архивированию криптографических ключей для обеспечения их защиты от несанкционированного изменения и раскрытия?
DS 5.9	Выявление, предупреждение и устранение последствий от вредоносного программного обеспечения	Убедится, что в организации приняты превентивные, выявляющие и устраняющие меры для защиты информационных систем и технологий от вредоносных программ.	• Определены ли в организации и внедрены превентивные меры по защите от вредоносных программ (вирусов, червей, шпионских программ, спама)?
DS 5.10	Сетевая безопасность	Удостоверится, что в организации применяются технологии обеспечения безопасности и соответствующие процедуры управления для авторизации доступа и контроля информационных межсетевых потоков.	• Установлены ли сетевые экраны отвечающие требованиям безопасности, способные защищать от атак отказа в обслуживании и любого неавторизованного доступа к внутренним ИТ ресурсам?
DS 5.10	Обмен критичными данными	Следует удостоверится, что в организации осуществляется обмен критичными данными только посредством надежного канала или носителя.	• Гарантируют ли существующие методы обмена критичными данными аутентичность содержания, доказательства отправления и получения, а также невозможность отказа от факта обмена данными?

DS 6. Определение и распределение затрат

Потребность в рыночной и объективной системе распределения затрат на ИТ требует точной оценки этих затрат и соглашения с бизнес пользователями. Данный процесс включает в себя создание и применение системы учета, распределения и отчетности по затратам на ИТ для пользователей услуг. Справедливая система распределения дает возможность бизнесу принимать более компетентные решения по использованию ИТ-услуг. Оценка процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 27. Контроли ИТ-процесса «Определение и распределение затрат».

Таблица 27. Контроли ИТ-процесса «Определение и распределение затрат»

№	Контроль	Цель контроля	Критерии оценки
DS 6.1	Определение услуг	Удостоверится, что в организации определены все затраты на ИТ.	• Определяют ли пользователи требования к ИТ услугам? • Связаны ли ИТ услуги с бизнес процессами?
DS 6.2	Бухгалтерский учет в области ИТ	Убедится, что в организации ведется учет и распределение текущих затрат в соответствии с корпоративной моделью затрат.	• Определены ли и внедрены процедуры расчета себестоимости ИТ услуг?
DS 6.3	Моделирование затрат и выставление счетов на оплату	Следует убедиться, что разработана и применяется модель затрат, основанная на определении услуг, которая поддерживает расчет возвратных платежей за каждую услугу.	• Внедрены ли процедуры по выставлению счетов и расчету возвратных платежей?
DS 6.4	Поддержка модели затрат	Необходимо удостоверится, что в организации проводится мониторинг и сравнительный анализ целесообразности модели затрат/выделения средств для поддержания ее соответствия меняющейся бизнес и ИТ деятельности.	• Внедрены ли процедуры по оптимизации модели затрат и выделения средств?

DS 7. Обучение и подготовка пользователей

Эффективное обучение всех пользователей ИТ-систем, включая персонал ИТ, требует определения потребностей в обучении для каждой из групп. В дополнение к определению потребностей данный процесс включает в себя определение и реализацию стратегии эффективного обучения и оценку его результатов. Эффективная программа обучения повышает результативность применения технологий путем сокращения числа ошибок, роста производительности и повышения уровня соответствия ключевым требованиям контроля, таким как показатели безопасности использования ИТ. Оценка процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 28. Контроли ИТ-процесса «Обучение и подготовка пользователей»

Таблица 28. Контроли ИТ-процесса «Обучение и подготовка пользователей»

№	Контроль	Цель контроля	Критерии оценки
DS 7.1	Определение потребностей в образовании	Необходимо удостоверится, что в организации определены потребности сотрудников в образовании в сфере ИТ.	• Определены ли потребности сотрудников в курсах обучения в сфере ИТ? • Создан ли и регулярно обновляется учебный план для каждой целевой группы сотрудников, учитывающий следующие обстоятельства: ▪ текущие и будущие бизнес потребности; ▪ ценность информации как актива; ▪ корпоративные ценности (этические ценности, управление, культуру в области

№	Контроль	Цель контроля	Критерии оценки
			безопасности и т.д.); ▪ внедрение новой ИТ инфраструктуры или программного обеспечения (в том числе пакетов и отдельных приложений); ▪ современные и будущие навыки, уровни компетентности и потребности в сертификации и аттестации, а также переаттестации; ▪ методы организации обучения (в учебных классах либо посредством Интранет), размеры целевой группы и срок обучения?
DS 7.2	Проведение тренингов и обучения	Необходимо убедится, что в организации проводятся обучения и тренинги в области ИТ.	• Существует ли утвержденная процедура согласно организованно проведение обучения? • Ведется ли учет регистрации на обучение, посещаемости и оценок эффективности учебной сессии?
DS 7.3	Оценка результатов обучения	Следует удостовериться, что по завершению курса проводится оценка результатов обучения.	• Проводится оценка тренингов и обучения по следующим критериям: ▪ актуальности; ▪ качества; ▪ эффективности; ▪ уровня усвоения знаний; ▪ затрат и пользы?

DS 8. Управление службой технической поддержки и инцидентами

Своевременное и эффективное реагирование на запросы и проблемы пользователей, требует хорошо организованной и отлаженной службы поддержки и управления инцидентами. Данный процесс включает в себя создание службы поддержки с функциями регистрации инцидентов, анализа инцидентов и тенденций, а также разрешения возникших проблем. Корпоративные выгоды заключаются в росте производительности благодаря быстрому решению запросов пользователей. В дополнение, организация может выявить первопричины (такие как плохое обучение пользователей) благодаря эффективной отчетности службы поддержки. Оценка процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 29. Контроли ИТ-процесса «Управление службой технической поддержки и инцидентами».

Таблица 29. Контроли ИТ-процесса «Управление службой технической поддержки и инцидентами»

№	Контроль	Цель контроля	Критерии оценки
DS 8.1	Служба технической поддержки	Необходимо удостоверится, что в организации создана служба технической поддержки, являющаяся звеном взаимодействия пользователей и ИТ.	• Организована ли в служба технической поддержки пользователей, призванная регистрировать, распределять и анализировать все обращения, докладывать об инцидентах, требованиях оказания услуг и запросах на информацию?
DS 8.2	Регистрация запросов	Следует убедиться, что созданы функции и система, позволяющие учитывать и отслеживать обращения,	• В организации имеются ли процедуры для службы технической поддержки по регистрации заявок

№	Контроль	Цель контроля	Критерии оценки
		инциденты, запросы о поддержке или об информации.	пользователей ИТ услуг?
DS 8.3	Разрешение инцидентов	Удостоверится в том, что разработаны процедуры службы поддержки, предусматривающие управляемое разрешение инцидентов, которые не могут быть ликвидированы незамедлительно.	• В организации имеются ли процедуры, которые определяют процесс эскалации запросов внутри ИТ подразделения, которые не могут быть решены моментально?
DS 8.4	Закрытие инцидента	Убедится, что разработаны процедуры оперативного мониторинга по окончательному разрешению запросов пользователей.	• Имеются ли в организации процедуры по своевременному мониторингу полного выполнения запросов пользователей? • Ведется ли в организации учет и доклад о неразрешенных инцидентах (известных ошибках и временных решениях), чтобы обеспечить надлежащей информацией процесс управления проблемами?
DS 8.5	Отчетность и анализ тенденций	Необходимо убедится в том, что существует возможность оценить эффективность службы поддержки, время ответа на запросы и выявить тенденции или повторяющиеся проблемы.	• Имеются ли процедуры, гарантирующие предоставление соответствующих отчетов о запросах пользователей и их выполнения, время ответа и определения тенденций?

DS 9. Управление конфигурацией

Обеспечение целостности аппаратного и программного обеспечения требует создания и поддержки точного и полного хранилища конфигурационных данных. Данный процесс включает в себя сбор первоначальных данных о конфигурации, создание прототипа, проверку и аудит данных о конфигурации, а также обновление хранилища конфигурационных данных по мере необходимости. Эффективное управление конфигурацией обеспечивает большую доступность систем, минимизирует проблемы, связанные с промышленной эксплуатацией систем и ведет к более быстрому решению проблем. Оценка процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 30. Контроли ИТ-процесса «Управление конфигурацией».

Таблица 30. Контроли ИТ-процесса «Управление конфигурацией»

№	Контроль	Цель контроля	Критерии оценки
DS 9.1	Хранилище конфигурационных данных	Удостоверится, что в организации созданы средства поддержки и централизованное хранилище, в котором должна помещаться вся информация, имеющая отношение к объектам конфигурации.	• Существует ли в организации централизованное хранилище, в котором помещается вся информация, имеющая отношение к объектам конфигурации?

№	Контроль	Цель контроля	Критерии оценки
DS 9.2	Идентификация и обслуживание объектов конфигурации	Необходимо убедится, что в организации разработаны процедуры конфигурации для поддержки управления и документирования всех изменений в хранилище конфигурационных данных.	• Разработана ли в организации процедура конфигурации для поддержки управления и документирования всех изменений в хранилище конфигурационных данных? • Интегрирована ли данная процедура с процессами управления конфигурацией, управления инцидентами и управления проблемами?
DS 9.3	Проверка целостности конфигурации	Необходимо удостоверится, что проводится периодическая проверка конфигурационных данных и подтверждена целостность конфигурации.	• Ведется ли в организации отчетность по проверке целостности конфигураций?

DS 10. Управление проблемами

Эффективное управление проблемами требует выявления и классификации всех проблем, анализа их первопричин и последующего их решения. Процесс управления проблемами также включает в себя формулирование рекомендаций по совершенствованию, поддержке учета проблем и изучение статуса корректирующих действий. Эффективный процесс управления проблемами максимизирует доступность систем, ведёт к повышению уровней обслуживания, сокращению затрат и повышению комфорта и удовлетворенности пользователей. Оценка процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 31. Контроли ИТ-процесса «Управление проблемами».

Таблица 31. Контроли ИТ-процесса «Управление проблемами»

№	Контроль	Цель контроля	Критерии оценки
DS 10.1	Выявление и классификация проблем	Удостоверится в том, что на практике реализованы отчетность и классификацию проблем, которые были выявлены в ходе процесса управления инцидентами.	• Определена ли в организации система управления проблемами? • Классифицированы ли в организации проблем, которые были выявлены в ходе процесса управления инцидентами?
DS 10.2	Отслеживание и разрешение проблем	Следует убедиться в том, что система управления проблемами обеспечена необходимыми средствами по отслеживанию, анализу и определению первопричин всех выявленных проблем.	• Внедрена ли процедура мониторинга и эскалации проблем?
DS 10.3	Закрытие проблем	Необходимо удостоверится в том, что в организации предусмотрена процедура окончательного решения проблемы.	• В организации разработана процедура окончательного решения проблемы в случае подтверждения о ее успешном устранении, либо после соглашения с бизнес пользователями о методах ее альтернативного (обходного) решения?
DS 10.4	Интеграция управления конфигурацией, управления инцидентами	Необходимо убедиться, что в организации существует интеграция процессов управления	• В организации осуществлена интеграция процессов управления конфигурацией, управления инцидентами и проблемами для обеспечения

№	Контроль	Цель контроля	Критерии оценки
	и проблемами	конфигурацией, управления инцидентами и проблемами для обеспечения совершенствования эффективного управления проблемами.	эффективного управления проблемами?

DS 11. Управление данными

Эффективное управление данными требует определение требований к данным. Процесс управления данными также включает в себя создание эффективных процедур управления библиотекой носителей данных, резервным копированием и восстановлением данных, а также надлежащим выводом из эксплуатации (списанием) носителей данных. Эффективное управление данными помогает обеспечить качество, оперативность и доступность корпоративных данных. Оценка процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 32. Контроли ИТ-процесса «Управление данными».

Таблица 32. Контроли ИТ-процесса «Управление данными»

№	Контроль	Цель контроля	Критерии оценки
DS 11.1	Бизнес требования к управлению данными	Следует удостовериться, чтобы все данные, предназначенные для обработки, были получены и обработаны в полном объеме, точно и своевременно, а результаты обработки соответствовали бизнес требованиям.	• Разработана ли в организации процедура по обработке данных?
DS 11.2	Запись и хранение	Необходимо убедится, что определены и реализованы на практике процедуры эффективного и производительного хранения, записи и архивирования данных в соответствии с бизнес целями, корпоративной политикой безопасности и регулятивными требованиями.	• Разработана ли в организации процедура по хранению данных?
DS 11.3	Управление библиотекой носителей данных	Необходимо удостоверится, что в организации определена и реализована на практике инвентаризация архива носителей данных, с целью удостовериться в их исправности и целостности.	• Осуществляется ли инвентаризация архива носителей данных?
DS 11.4	Вывод из эксплуатации (списание)	Удостоверится, что определены и реализованы на практике процедуры по защите важных данных и программ при списании или передаче оборудования и данных.	• Реализованы ли на практике процедуры отвечающие бизнес требованиям по защите важных данных и программ при списании или передачи оборудования и данных?
DS 11.5	Резервное хранение и восстановление	Следует удостовериться, что в организации определены и реализованы на практике процедуры резервного хранения и	• Реализована ли на практике процедура резервного копирования данных и восстановления систем, приложений, данных и документации, соответствующие бизнес требованиям и плану

№	Контроль	Цель контроля	Критерии оценки
		восстановления.	обеспечения непрерывности обслуживания?
DS 11.6	Требования по безопасности к управлению данными	Необходимо убедится, что сформулированы и реализованы на практике политики и процедуры требований по безопасности в отношении управления данными.	• Разработаны ли в организации требования по безопасности к управлению данными в отношении приема, обработки, хранения и вывода данных, соответствующие бизнес целям, корпоративной политике безопасности и регулятивным требованиям?

DS 12. Управление физической безопасностью и защитой от воздействия окружающей среды

Защита компьютерного оборудования и персонала требует хорошего планирования и организации физических объектов. Процесс управления физической средой включает в себя определение физических требований, выбор подходящих объектов, проектирование эффективных процессов мониторинга внешних факторов и управление физическим доступом. Эффективное управление физической безопасностью и защитой от воздействия окружающей среды сокращает перебои в работе организации, вызванные физическими угрозами, связанными с компьютерным оборудованием и персоналом. Оценка процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 33. Контроли ИТ-процесса «Управление физической безопасностью и защитой от воздействия окружающей среды».

Таблица 33. Контроли ИТ-процесса «Управление физической безопасностью и защитой от воздействия окружающей среды»

№	Контроль	Цель контроля	Критерии оценки
DS 12.1	Выбор места и проектирование	Необходимо убедится, что в организации определено помещение для размещения ИТ оборудования, которое должно осуществлять поддержку технологической стратегии.	• Определены ли помещения для размещения ИТ оборудования (коммутационные, серверные)?
DS 12.2	Показатели физической безопасности	Удостоверится в том, что в организации определены и внедрены показатели физической безопасности.	• Установлены ли элементы физической безопасности и меры контроля для помещения ИТ оборудования, включающих: ▪ элементы пожаротушения; ▪ кондиционирования; ▪ защиты от несанкционированного входа; ▪ элементами бесперебойного электрического питания.
DS 12.3	Физический доступ	Убедится, что определены и реализованы на практике процедуры по физическому доступу.	• Определены ли в организации процедуры по физическому доступу в соответствии с бизнес потребностями, включая действия при чрезвычайных ситуациях?
			• Существуют ли процедуры, при которых люди, не являющиеся сотрудниками ИТ подразделения сопровождаются в присутствии члена ИТ подразделения в помещения с ИТ оборудованием?

№	Контроль	Цель контроля	Критерии оценки
DS 12.4	Защита от факторов окружающей среды	Необходимо удостоверится, что в организации реализованы на практике меры по защите от факторов окружающей среды.	• Установлено ли специализированное оборудование и устройства по мониторингу и контролю среды?
DS 12.5	Управление физическими объектами	Необходимо убедится, что в организации проводится управление физическими объектами.	• Установлены ли источники бесперебойного питания для критически важных ИТ систем?

DS 13. Управление операциями по эксплуатации систем

Полная и точная обработка данных требует эффективного управления процедурами обработки данных и тщательного обслуживания оборудования. Данный процесс включает в себя определение политик и процедур операционной деятельности для эффективного управления плановыми заданиями по обработке данных, защите вывода важной информации, мониторингу производительности инфраструктуры и превентивному обслуживанию оборудования. Эффективное управление операциями по эксплуатации систем позволяет поддерживать целостность данных и сокращает простои в работе и операционные затраты на ИТ. Оценка процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 34. Контроли ИТ-процесса «Управление операциями по эксплуатации систем».

Таблица 34. Контроли ИТ-процесса «Управление операциями по эксплуатации систем»

№	Контроль	Цель контроля	Критерии оценки
DS 13.1	Операционные процедуры и инструкции	Удостоверится в том, что операционный персонал ознакомлен со всеми необходимыми операционными задачами.	• Определены ли в организации операционные процедуры и инструкции, включающие передачу выполняемых действий, обновления статуса, операционных проблем, процедуры эскалации и отчетности по текущим обязанностям?
DS 13.2	Определение графика работ	Необходимо убедиться, что составлен график работ, процессов и задач в наиболее эффективной последовательности.	• Составлен ли в организации график работ по эксплуатации систем?
DS 13.3	Мониторинг ИТ инфраструктуры	Необходимо удостоверится, что в организации на практике реализованы процедуры мониторинга ИТ инфраструктуры и относящихся к ней событий.	• Логируются ли и анализируются все ИТ события в системах оргнаизации?
DS 13.4	Важные документы и устройства вывода данных	Убедиться в том, что в организации создана адекватная физическая защита, практика учета и инвентаризации наиболее важных ИТ активов.	• Внедрены ли процедуры применяемые для обеспечения безопасности специальных форм и чувствительных устройств вывода?
DS 13.5	Превентивное обслуживание оборудования	Удостоверится в том, что в организации на практике реализованы процедуры, обеспечивающие оперативную поддержку	• Внедрены ли в организации на практике процедуры, обеспечивающие оперативную поддержку инфраструктуры для сокращения частоты и масштабов сбоев или падения

№	Контроль	Цель контроля	Критерии оценки
		инфраструктуры для сокращения частоты и масштабов сбоев или падения производительности.	производительности?

4.4.4 ME. Мониторинг и оценка

ME 1. Мониторинг и оценка эффективности ИТ

Эффективное управление производительностью ИТ требует мониторинга. Данный процесс включает в себя определение индикаторов эффективности, систематическую и своевременную отчетность об эффективности, а также безотлагательные меры в случае обнаружения отклонений. Мониторинг необходим для уверенности в том, что все операции проводятся в соответствии с принятыми направлениями и политиками. Оценка процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 35. Контроли ИТ-процесса «Мониторинг и оценка эффективности ИТ».

Таблица 35. Контроли ИТ-процесса «Мониторинг и оценка эффективности ИТ»

№	Контроль	Цель контроля	Критерии оценки
ME 1.1	Подход к организации мониторинга	Удостоверится в том, что в организации разработана общая методология мониторинга и подход к определению масштаба, методологии и процесса оценки ИТ решений и оказания услуг.	• Разработана ли методология мониторинга и оценка эффективности ИТ?
ME 1.2	Определение и сбор данных мониторинга	Убедится, что совместно с бизнес подразделениями разработана и утверждена сбалансированная система целей эффективности.	• Утверждена ли в организации система целей эффективности? • Разработаны ли процессы своевременного сбора достоверных данных для отчетности по достижению целей?
ME 1.3	Методика мониторинга	Следует убедиться, что в организации внедрена методика мониторинга эффективности для учета целей и показателей, получения емкой, всесторонней характеристики ИТ	• Внедрена ли методика мониторинга эффективности ИТ? • Совместима ли методика мониторинга эффективности ИТ с корпоративной системой мониторинга?
ME 1.4	Оценка эффективности	Необходимо удостоверится, что в организации периодически проводится проверка текущей эффективности в сравнении с поставленными целями.	• Проводится ли оценка эффективности ИТ в организации? • Проводить ли анализ причин в отношении отклонений по достижению поставленных целей?
ME 1.5	Отчетность перед высшим руководством и Советом директоров	Необходимо убедится, что в организации разработана отчетность перед высшим руководством по вкладу ИТ в развитие бизнеса.	• Предоставляется ли отчетность высшему руководству и Совету директоров по вкладу ИТ в бизнес?

№	Контроль	Цель контроля	Критерии оценки
ME 1.6	Корректирующие действия	Удостоверится, что в организации на практике реализованы корректирующие действия, основанные на данных мониторинга и оценки эффективности.	• Применяются ли в организации корректирующие действия, основанные на результатах мониторинга и оценки эффективности?

ME 2. Мониторинг и оценка системы внутреннего контроля

Установление программы эффективного внутреннего контроля в сфере ИТ требует хорошей организации процесса мониторинга. Данный процесс включает в себя собственно мониторинг и отчетность о случаях исключения из практики, результаты самооценок и анализ, проводимый третьей стороной. Основное преимущество мониторинга системы внутреннего контроля заключается в обеспечении эффективной и результативной деятельности в сфере ИТ и совместимости с требованиями законодательства и регулирующих норм. Оценка процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 36. Контроли ИТ-процесса «Мониторинг и оценка системы внутреннего контроля».

Таблица 36. Контроли ИТ-процесса «Мониторинг и оценка системы внутреннего контроля»

№	Контроль	Цель контроля	Критерии оценки
ME 2.1	Мониторинг методологии внутреннего контроля	Удостоверится в том, что постоянно осуществляется мониторинг, сравнительный анализ и совершенствование среды ИТ-контроля .	• Проводится ли мониторинг эффективности внутренних контролей в ходе обычной операции по управлению и надзорной деятельности, сравнения, примирения и других рутинных действий?
ME 2.2	Надзор	Убедится, что в организации осуществляется мониторинг и оценка эффективности и результативности внутреннего управленческого контроля ИТ.	• Осуществляется ли надзор за системой внутреннего контроля?
ME 2.3	Исключения из мер контроля	Следует удостоверится, что в организации выявляются исключения из требований контроля.	• Подготавливается ли отчетность по исключениям для заинтересованных сторон?
ME 2.4	Контроль самооценки	Необходимо убедится, что организацией проводится оценка полноты и эффективности управленческого контроля над ИТ процессами, политиками и контрактами в рамках постоянной программы самооценки.	• Проводится ли организацией оценка полноты и эффективности управленческого контроля?
ME 2.5	Аудит системы внутреннего контроля	Необходимо удостоверится, что организацией получены, в случае необходимости, гарантии полноты и эффективности системы внутреннего контроля, с помощью проверок третьей стороны.	• Проводится ли в организации аудит системы внутреннего контроля?

№	Контроль	Цель контроля	Критерии оценки
ME 2.6	Система внутреннего контроля третьих сторон	Следует убедиться, что в организации оценивается система внутреннего контроля внешних поставщиков услуг.	• Проводится оценка системы внутреннего контроля внешних поставщиков услуг?
ME 2.7	Корректирующие действия	Удостоверится, что в организации определены, инициированы, отслеживаются и реализовываются на практике корректирующие действия, вытекающие из оценок системы контроля и отчетности.	• Применяются ли в организации корректирующие действия по системе внутреннего контроля?

ME 3. Обеспечение соответствия внешним требованиям

Эффективный надзор за соответствием внешним требованиям требует установления процесса анализа соответствия требованиям законодательства, регулирующих норм и условий контрактов. Данный процесс включает в себя выявление применимых требований, оптимизацию и оценку результатов, получение уверенности в том, что требования соблюдены, и, наконец, интеграцию отчетности о соответствии ИТ внешним требованиям с корпоративной отчетностью. Оценка процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 37. Контроли ИТ-процесса «Обеспечение соответствия внешним требованиям».

Таблица 37. Контроли ИТ-процесса «Обеспечение соответствия внешним требованиям»

№	Контроль	Цель контроля	Критерии оценки
ME 3.1	Выявление внешних требований законодательства, регулирующих норм и условий контрактов	Следует убедиться, что организацией ведется постоянная работа по выявлению требований национального и международного законодательства, регулирующих норм и других внешних требований, которым должны соответствовать корпоративные ИТ политики, стандарты, процедуры и методики организации.	• Проводится ли выявление внешних требований законодательства, регулирующих норм и условий контрактов?
ME 3.2	Оптимизация результатов проведения в соответствие с внешними требованиями	Удостоверится, что организацией анализируются и корректируются ИТ политики, стандарты, процедуры и методики на предмет соответствия требованиям законодательства, регулирующих норм и условий контрактов.	• Проводится ли работа по соответствию нормативной документации организации с внешними требованиями?
ME 3.3	Оценка соответствия внешним требованиям	Убедится, что организацией подтверждено соответствие ИТ политик, стандартов, процедур и методик требованиям законодательства и регулирующих норм.	• Проводится ли оценка соответствия внешним требованиям нормативной документации организации?
ME 3.4	Положительное	Следует удостовериться в том, что	• Соблюдается ли организацией внешние

№	Контроль	Цель контроля	Критерии оценки
	заключение о соответствии	организацией получено заключение о соответствии и строгом соблюдении положений внутренней политики, вытекающих из внутренних директив и внешних требований законодательства, регулирующих нормы и условия контрактов.	требования законодательства, регулирующих норм и условий контрактов?
ME 3.5.	Интеграция отчетности	Необходимо убедиться, что организацией проводиться интеграция отчетности по соблюдению требований законодательства, регулирующих норм и условий контрактов с аналогичной отчетностью других корпоративных подразделений.	• Проводиться ли организацией интеграция отчетности по соблюдению требований законодательства?

ME 4. Обеспечение корпоративного управления ИТ

Внедрение эффективной методологии корпоративного управления включает в себя определение организационных структур, процессов, лидерства, должностей и обязанностей. Это позволяет удостовериться в том, что корпоративные ИТ-инвестиции соответствуют корпоративной стратегии и целям. Оценка процесса осуществляется путем анализа эффективности контролей, представленных в Таблица 38. Контроли ИТ-процесса «Обеспечение корпоративного управления ИТ».

Таблица 38. Контроли ИТ-процесса «Обеспечение корпоративного управления ИТ»

№	Контроль	Цель контроля	Критерии оценки
ME 4.1	Создание системы корпоративного управления ИТ	Необходимо удостоверится, что в организации обеспечено соответствие системы управления ИТ общекорпоративному управлению и среде контроля.	• Соответствует ли система управления ИТ общекорпоративному управлению и среде контроля?
ME 4.2	Соответствие стратегии	Необходимо убедится, что Совет директоров и высшее руководство понимают стратегические вопросы ИТ, таких как роль ИТ, технологии и возможности.	• Проводится ли руководством оценка соответствия ИТ со стратегией развития организации?
ME 4.3	Вклад ИТ в бизнес	Следует убедиться, что Совет директоров и высшее руководство обеспечено пониманием стратегических вопросов ИТ, таких как роль ИТ, технологии и возможности.	• Проводится ли в организации работа с Советом директоров и существующими органами управления, такими как комитет по ИТ стратегии, для выработки стратегического направления руководства ИТ?
ME 4.4	Управление ресурсами	Удостоверится, что в организации осуществляется надзор за инвестициями, использованием и распределением ИТ ресурсов посредством регулярных оценок	• Осуществляется ли надзор за инвестициями в организации?

№	Контроль	Цель контроля	Критерии оценки
		инициатив и операций в сфере ИТ.	
ME 4.5	Управление рисками	Необходимо убедится, что в организации проведена работа с Советом директоров для определения приемлемого уровня ИТ рисков для организации и были получены разумные гарантии того, что текущие ИТ риски при существующей практике управления ими не превышают установленный Советом директоров уровень.	• Осуществляется ли работа по определению приемлемого уровня ИТ рисков совместно с руководством?
ME 4.6	Управление эффективностью	Следует удостоверится, что намеченные ИТ цели были достигнуты.	• Проводится ли управление эффективностью организации путем достижения поставленных целей?
ME 4.7	Независимая оценка	Убедится, что организацией получена независимая оценка (внутреннюю или внешнюю) соответствия ИТ требованиям законодательства и регулирующих норм, корпоративной политики, стандартов и процедур, общепринятых практик, а также эффективности и результативности ИТ.	• Проводится ли организацией независимая оценка соответствия ИТ требованиям законодательства и регулирующих норм?