CobiT

4-1

РОССИЙСКОЕ ИЗДАНИЕ

Оглавление

Общий обзор

Для многих организаций информация и поддерживающие ее технологии представляют собой самые ценные, хотя и зачастую не до конца понятные активы. Успешные организации осознают те выгоды, которые предлагают информационные технологии и применяют их, повышая собственную ценность для заинтересованных сторон. Эти организации также понимают и управляют связанными рисками, такими как возрастание регулирующих требований и критическая зависимость многих бизнес процессов от информационных технологий (ИТ).

Потребность в уверенности относительно той пользы, которую дают ИТ, управление связанными с ИТ рисками и растущие требования к контролю над информацией в настоящее время понимаются как ключевые элементы корпоративного управления. Ценность, риск и контроль составляют суть корпоративного управления сферой ИТ.

Корпоративное управление сферой ИТ (далее — Управление ИТ) есть ответственность высшего руководства и Совета директоров, которая включает в себя лидерство, организационные структуры и процессы, обеспечивающие соответствие ИТ текущим и стратегическим целям организации.

Более того, управление ИТ интегрирует и структурирует лучшие практики для того, чтобы ИТ организации оказывали помощь в достижении бизнес целей. Управление ИТ позволяет организации пользоваться всеми преимуществами своей информации и тем самым максимизировать выгоду, извлекать прибыли из возможностей и получать конкурентные преимущества. Все это требует методологии для контроля ИТ, которая соответствовала бы требованиям доклада Комитета спонсорских организаций Комиссии Тредуэя (COSO) *«Внутренний контроль — интегрированная методология»,* получившего широкое признание в качестве методологии контроля в области корпоративного управления и управления рисками.

Организации должны удовлетворять стандартам качества, требованиям безопасности и конфиденциальности в отношении собственной информации, равно как и в отношении других активов. Руководство также должно оптимизировать пользование доступными ИТ ресурсами, включающими в себя приложения, информацию, инфраструктуру и персонал. Для того чтобы исполнить эти обязанности, а также достигнуть поставленных целей, высшее руководство должно понимать статус корпоративной ИТ архитектуры и определить, какие методы управления и контроля следует реализовывать на практике.

Издание *«Цели контроля для информационных и смежных технологий»* (COBIT) устанавливает лучшие практики на уровне доменов (групп ИТ процессов) и отдельных процессов и представляет действия в виде управляемой и логичной структуры. Лучшие практики в COBIT основаны на консенсусе экспертов. Они в большей степени ориентированы на контроль, нежели на исполнение. Эти нормы помогут оптимизировать инвестиции в ИТ, обеспечить уверенность в уровне предоставляемых сервисов и выработать показатели, на которые можно будет ориентироваться в случае неблагоприятного развития ситуации.

В сфере ИТ успешное предоставление сервисов в соответствии с требованиями бизнеса предполагает наличие системы или методологии внутреннего контроля. Система контроля COBIT отвечает этим потребностям, поскольку:

- Связана с требованиями бизнеса.
- Организует виды ИТ деятельности в виде понятной процессной модели.
- Определяет основные ресурсы ИТ, на которые должны осуществляться воздействие.
- Определяет цели контроля.

Бизнес ориентация COBIT состоит во взаимосвязи целей бизнеса и ИТ, выявлении показателей и моделей зрелости для оценки достижений, определении соответствующих видов ответственности владельцев бизнес и ИТ процессов. Ориентированный на процессы подход проиллюстрирован в COBIT при помощи модели, подразделяющей 34 отдельных ИТ процесса в четыре домена (группы), упорядочивающей ответственности в области

планирования, построения, исполнения и контроля, обеспечивающей комплексное видение ИТ в целом. Концепции корпоративной архитектуры помогают определить ресурсы, необходимые для успешного выполнения процессов, то есть приложения, информацию, инфраструктуру и персонал.

Вкратце, для того, чтобы обеспечить организацию информацией, необходимой для достижения определенных бизнес целей, необходимо управлять ресурсами ИТ с помощью естественным образом сгруппированных ИТ процессов.

Но как организация может управлять сферой ИТ так, чтобы получать информацию, необходимую для своих корпоративных целей? Как управлять рисками и обеспечивать безопасность тех ИТ ресурсов, от которых организация столь зависима? Как организация может быть уверена в том, что ИТ достигает поставленных целей и поддерживает развитие бизнеса?

В первую очередь руководство нуждается в целях контроля, которые определяют основную цель внедрения политик, планов и процедур, а также в организационных структурах, призванных обеспечить:

- Достижение бизнес целей.
- Предотвращение нежелательных событий или их выявление и исправление последствий.

Во-вторых, в сложных современных условиях, руководство постоянно находится в поиске информации для быстрого и успешного принятия решений в отношении ценности активов, рисков и мер контроля. Что должно быть измерено, и каким образом? Организации нуждаются в объективных критериях оценки своего текущего состояния и тех улучшений, которые им требуются, а также в некотором инструментарии, с помощью которого руководство могло бы оценить эти улучшения. На схеме **1** показаны некоторые из традиционных вопросов и управленческий инструментарий для поиска ответов на эти вопросы, однако приборные панели нуждаются в индикаторах, системы показателей — в самих показателях, а сравнительный анализ — в шкале сравнения.

Схема 1. Вопросы руководства

Ответом на эти требования охарактеризовать и контролировать надлежащий уровень эффективности в сфере ИТ являются следующие определения, которые дает COBIT:

- Сравнительный анализ эффективности и потенциала ИТ процессов, выраженный в виде моделей зрелости, полученных из Модели Зрелости и Потенциала (Capability Maturity Model, CMM), предложенной Институтом по разработке программного обеспечения (Software Engineering Institute).
- Цели и показатели ИТ процессов, необходимые для определения и оценки их результатов и эффективности, основаны на принципах системы сбалансированных бизнес показателей, предложенной Робертом Каштаном и Дэвидом Нортоном.
- **Цели действий** для непосредственного управления ИТ процессами, основаны на целях контроля COBIT.

Оценка возможностей процесса, построенная на моделях зрелости COBIT является ключевой составляющей реализации управления ИТ. После выявления критичных ИТ процессов и мер контроля, модели зрелости помогут ликвидировать обнаруженные пробелы и продемонстрировать результаты руководству. После этого могут быть разработаны планы действий для того, чтобы вывести процессы на желаемый уровень эффективности. Таким образом, COBIT оказывает поддержку управлению ИТ (см. **схему 2),** предоставляя необходимую методологию для обеспечения того, чтобы:

- Сфера ИТ была приведена в соответствие с бизнесом.
- ИТ помогали бизнесу и максимизировали преимущества.
- ИТ ресурсы использовались ответственно.
- Осуществлялось надлежащее управление ИТ рисками.

Оценка эффективности является частью управления сферой ИТ. Оценка эффективности рассматривается в COBIT и включает в себя постановку и контроль целей (достижение которых поддается оценке), которые определяют результаты ИТ процессов и путь достижения этих результатов (потенциал процесса и эффективность). В ходе многих исследований было установлено, что недостатки в области прозрачности затрат на ИТ, определения ценностей и рисков являются одними из основных стимулов к совершенствованию управления сферой ИТ. Тогда как другие области управления являются предметом оценки эффективности, прозрачность достигается в первую очередь с ее помощью.

Схема 2. Ключевые области управления ИТ

- **Соответствие стратегии** делает акцент на связи между планами бизнеса и ИТ; выявлении, поддержке и контроле за ценностным предложением ИТ; а также на соответствии ИТ и бизнес операций.
- **Полезность** представляет собой реализацию ценностного предложения, контроль за тем, чтобы ИТ обеспечивали определенные стратегией преимущества, сосредоточение на оптимизации затрат и подтверждение подлинной ценности ИТ.
- **Управление ресурсами** посвящено вопросам, связанным с управлением критичными ИТ ресурсами, а именно, оптимизацией инвестиций и должному руководству приложениями, информацией, инфраструктурой и персоналом. Ключевые вопросы касаются оптимизации знаний и инфраструктуры.
- **Управление рисками** требует осведомленности высшего руководства в области рисков, четкого понимания корпоративного подхода в их отношении, соответствия требованиям прозрачности в отношении существенных рисков, включения функции управления рисками в практику организации.
- **Оценка эффективности** представляет собой контроль за реализацией стратегии, результатами проектов, использованием ресурсов, эффективностью процессов и сервисным обслуживанием. Для этого применяются, в частности, системы сбалансированных показателей, которые преобразуют стратегию в последовательность действий, результаты которых измеряются иными, по сравнению с бухгалтерским учетом, методами.

Эти области управления ИТ характеризуют круг вопросов, с которыми приходится иметь дело высшему руководству, осуществляя управление ИТ в своих организациях. Оперативное управление использует процессы для организации текущей ИТ деятельности. Методология COBIT предлагает общую модель процессов, которая представляет все процессы как элементы функций ИТ, что делает эту базовую модель понятной для операционного ИТ персонала и бизнес менеджмента. Модель процессов COBIT соотнесена с ключевыми областями управления ИТ и это связывает обязанности операционного персонала с тем, что желает контролировать руководство.

Для достижения эффективного управления руководство требует от операционного персонала, чтобы меры контроля осуществлялись согласно определенной методологии для всех ИТ процессов. Цели контроля, предлагаемые COBIT, организованы по отдельным ИТ процессам; поэтому методология обеспечивает понятную связь между требованиями, предъявляемыми к управлению ИТ, ИТ процессами и мерами контроля ИТ.

В COBIT делается акцент на том, что требуется для достижения адекватного управления и контроля в сфере ИТ на высоком уровне. COBIT соотносится и гармонизируется с другими, более детальными стандартами в сфере ИТ и лучшими практиками. Методология COBIT действует в качестве интегратора этих руководящих материалов, суммируя ключевые цели в рамках единой методологии, которая, в свою очередь, увязана с управлением и требованиями бизнеса.

COSO (и подобные совместимые методологии) обычно принимаются в качестве методологии внутреннего контроля в организациях. COBIT, как правило, является методологией внутреннего контроля в сфере ИТ.

Продукты COBIT имеют трехуровневую организацию (см. **схему 3)** и предназначаются для поддержки:

- Высшего руководства и Советов директоров.
- Бизнес и ИТ менеджмента.
- Профессионалов в области управления, аудита, контроля и безопасности.

Вкратце, продукты COBIT включают:

- *Совещание по вопросам управления сферой ИТ, второе издание* (Board Briefing on IT Governance, 2nd Edition). Помогает высшему руководству осознать, почему важно управление ИТ, что к нему относится и каковы их обязанности по управлению.
- Руководства по управлению/модели зрелости. Помогают определить обязанности, оценить эффективность, провести сравнительный анализ и увидеть упущенные возможности.
- Методология. Организует цели управления ИТ и лучшие практики по доменам и процессам, а также связывает их с требованиями бизнеса.
- Цели контроля. Предлагают полный набор требований высокого уровня на рассмотрение менеджменту для эффективного контроля за каждым ИТ процессом.
- *Руководство по внедрению управления сферой ИТ:* Применение COBIT and VallT TM, второе издание (IT Governance Implementation Guide: Using COBIT andVallTTM, 2ndEdition). Обеспечивает общую последовательность действий при внедрении управления сферой ИТ, используя ресурсы COBIT и Val ITTM.
- *Контрольные практики COBIT:* Руководство по достижению целей контроля для успешного управления сферой ИТ, второе издание (COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition). Объясняет, почему следует реализовать меры контроля на практике и как это сделать.
- *Руководство по обеспечению надежности в сфере ИТ:* применение COBIT (IT Assurance Guide: Using COBIT). Обеспечивает руководство по тому, как COBIT может быть использован для

обеспечения надежности с применением предлагаемых процедур тестирования для всех ИТ процессов и целей контроля.

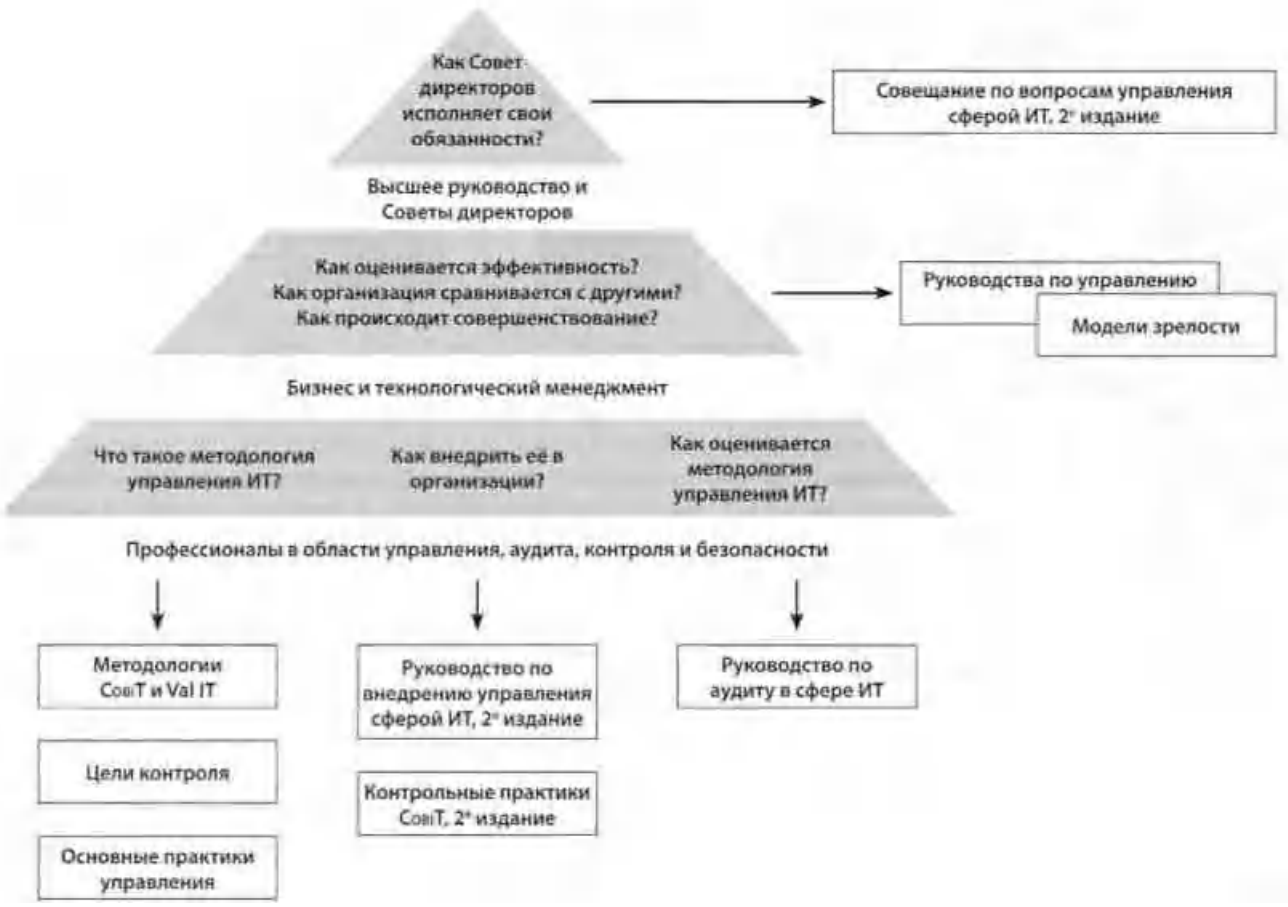


Схема 3. Диаграмма публикаций COBIT

Диаграмма по публикациям COBIT представляет общеприменимые продукты и их основную аудиторию. Существуют также производные продукты по специфическим вопросам (Цели контроля ИТ для Sarbanes-Oxley, второе издание. IT Control Objectives for Sarbanes-Oxley, 2nd Edition), для таких разделов как безопасность (COBIT Основные принципы безопасности. COBIT Security Baseline а также Управление информационной безопасностью: Руководство для Советов директоров и управляющих. Information Security Governance: Guidance for Boards of Directors and Executive Management), или для специфических организаций (Краткое руководство COBIT для малых и средних организаций или для крупных организаций, желающих активизировать внедрение управления ИТ. COBIT Quickstart for small and medium-sized enterprises or for large enterprises wishing to ramp up to a more extensive IT governance implementation).

Диаграмма публикаций COBIT, представленная на **схеме 3,** показывает основные аудитории, их вопросы по управлению ИТ и продукты, которые могут дать ответы на эти вопросы. Также на схеме представлены производные продукты по специфическим вопросам, в частности, по безопасности или для специфических организаций.

Все компоненты COBIT взаимосвязаны, оказывают поддержку для управления, контроля и аудита, как показано на **схеме 4.**

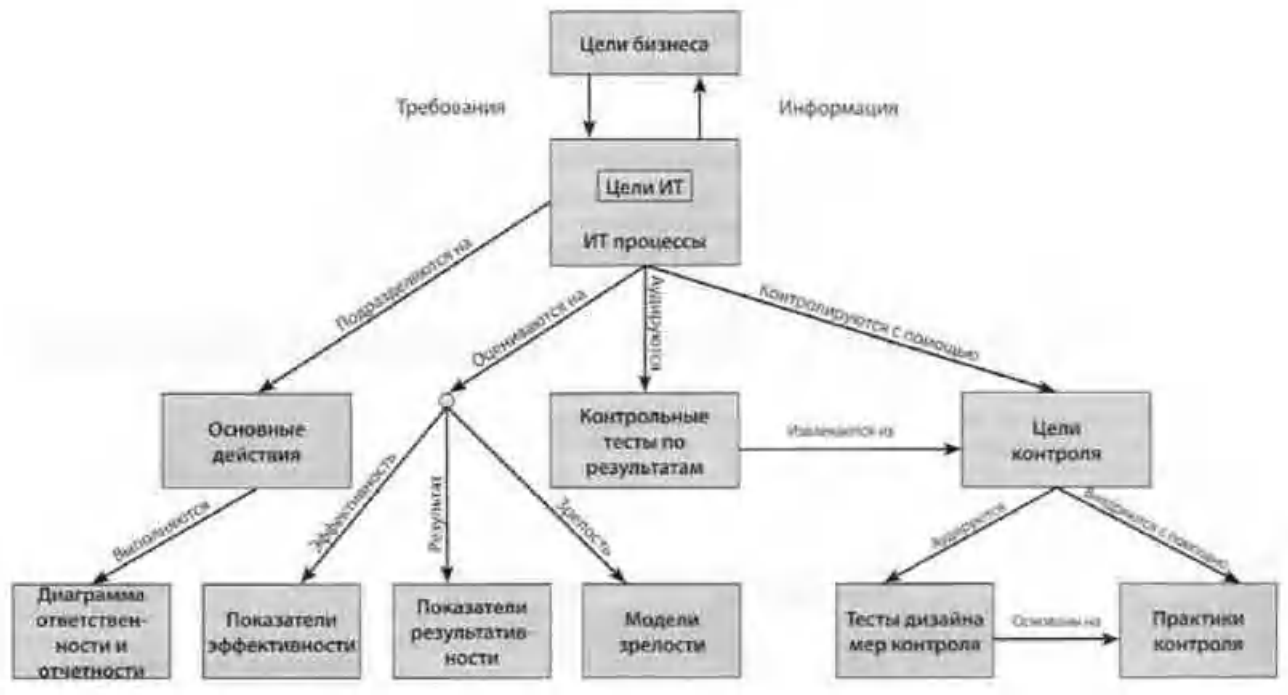


Схема 4. Взаимосвязи компонентов COBIT

COBIT является методологией и инструментарием, который позволяет руководителям устранить недостатки с учетом требований контроля, технических вопросов и бизнес рисков и донести достигнутый уровень контроля до сведения заинтересованных сторон. COBIT дает возможность разрабатывать четкие политики и лучшие практики по контролю ИТ в организациях. COBIT постоянно совершенствуется и гармонизируется с другими стандартами и рекомендациями. В результате COBIT стал интегратором лучших практик в сфере ИТ и зонтичной методологией для управления ИТ, которая помогает понимать и управлять рисками и преимуществами, связанными с ИТ. Сфокусированная на процессах структура COBIT и высокоуровневый, бизнес ориентированный подход обеспечивают комплексное видение ИТ и решений, связанных с этой сферой.

Преимущества внедрения COBIT в качестве методологии управления ИТ включают:

- Лучшее соответствие, основанное на потребностях бизнеса.
- Понятное для менеджмента видение деятельности ИТ.
- Четкость в вопросах владения и ответственности, основанная на процессах.
- Общее соответствие с требованиями третьих сторон и регуляторов.
- Понимание заинтересованных сторон, основанное на общем языке.
- Выполнение требований COSO к контролю в сфере ИТ.

Настоящий документ представляет собой описание методологии COBIT и всех ключевых компонентов COBIT, объединенных в четыре группы и 34 процесса. Вместе с несколькими приложениями это образует удобный справочник по всем основным рекомендациям COBIT.

Наиболее полная и актуализированная информация по COBIT и смежным продуктам, включая онлайн инструменты, руководства по внедрению, примеры из практики, информационные бюллетени и образовательные материалы можно найти на сайте www.isaca.org/cobit.

Методология COBIT

Миссия COBIT:

Исследование, разработка, публикация и продвижение авторитетной, современной, международно-признанной методологии корпоративного управления в сфере ИТ, предназначенной для внедрения в организациях и повседневного использования бизнес менеджерами, специалистами в сфере ИТ и аудиторами.

Потребность в методологии контроля для корпоративного управления ИТ

Методология контроля для корпоративного управления ИТ определяет причины, по которым требуется управление, заинтересованные стороны и, собственно, предмет совершенствования.

Почему

Все в большей степени высшее руководство осознает то существенное воздействие, которое информация оказывает на успешное развитие бизнеса. Руководство надеется на возрастающее понимание того, как работают ИТ и насколько успешно они могут применяться в качестве конкурентного преимущества. В особенности, высшее руководство нуждается в ответах на вопросы о том, как организация может управлять информацией для:

- Наиболее вероятного достижения поставленных целей.
- Эффективного обучения и адаптации.
- Разумного управления рисками.
- Своевременного распознавания новых возможностей и их реализации.

Успешные организации осознают существующие риски, пользуются преимуществами ИТ и принимают меры для того, чтобы:

- Увязать ИТ и бизнес стратегии.
- Убеждать инвесторов и заинтересованные стороны в том, что организация обращает должное внимание на минимизацию ИТ рисков.
- Внедрять ИТ стратегию и ее цели в работу организации.
- Получать отдачу от инвестиций в ИТ.
- Сформировать организационные структуры, способные облегчить внедрение стратегии и ее целей.
- Создать конструктивные взаимоотношения и эффективную взаимосвязь между бизнесом и ИТ, а также с внешними партнерами.
- Оценивать эффективность работы ИТ.

Организации не могут эффективно выполнить следующие задачи без принятия и внедрения методологии корпоративного управления и контроля в сфере ИТ:

- Соответствие требованиям бизнеса.
- Обеспечение прозрачности выполнения этих требований.
- Организация деятельности в виде принятой модели процессов.
- Определение основных задействованных ресурсов.
- Определение целей контроля для руководства.

Более того, методология управления и контроля становится частью лучших практик в области управления ИТ и необходима как для самой организации управления ИТ, так и для соответствия постоянно растущим регулирующим требованиям.

Лучшие практики в сфере ИТ становятся все более значимыми в силу ряда причин:

- Высшее руководство бизнеса и Советы директоров требуют большей отдачи от инвестиций в ИТ. тс есть повышения ценности бизнеса для заинтересованных сторон.
- Выражение обеспокоенности по поводу роста затрат на ИТ.
- Необходимость соответствия регулирующим требованиям в области контроля ИТ в таких вопросах как обеспечение защиты персональных данных и финансовая отчетность (например, американский закон Сарбейнса-Оксли (US Sarbanes-Oxley Act) и соглашение о принципах эффективного банковского надзора Basel II) и в таких специфических отраслях как финансы, фармацевтика и здравоохранение.
- Выбор сервисных организаций, управление аутсорсингом и приобретением услуг.
- Возрастание комплексности ИТ рисков, в частности, сетевой безопасности.
- Предложения в области управления ИТ, которые включают принятие методологий контроля и лучших практик для надзора и повышения качества работы ИТ, роста ценности бизнеса и минимизации бизнес рисков.
- Потребность в оптимизации затрат путем применения, когда это возможно, стандартизированных (а не специально разработанных) подходов к этой проблеме.
- Совершенствование и распространение детализированных методологий, таких как COBIT, «Библиотека ИТ инфраструктуры при Управлении правительственной коммерции Великобритании» (ITIL), стандарты ISO серии 27000 по информационной безопасности, требования к системе управления качеством ISO 9001:2000, «Модель зрелости интеграции» (Capability Maturity Model® Integration, CMMI), «Проекты в контролируемой среде 2» (PRINCE2) и «Свод знаний по управлению проектами» (PMBOK).

• Необходимость для организаций оценить, насколько они соответствуют распространенным стандартам и провести сравнение с конкурентами.

Кто

Методология управления и контроля необходима для удовлетворения специфических потребителей из чиста различных заинтересованных сторон:

• Заинтересованные стороны внутри организации, требующие максимальной отдачи от инвестиций в ИТ:

•S Те, кто принимает решения об инвестициях. **•S** Те, кто определяют требования. **•S** Те, кто пользуется услугами ИТ.

• Внутренние и внешние заинтересованные стороны, которые оказывают ИТ услуги:

•S Те, кто управляют организацией и процессами ИТ. **•S** Те, кто разрабатывает новые возможности. **•S** Те, кто оказывает услуги.

• Внутренние и внешние заинтересованные стороны, которые несут ответственность за контроль и управление рисками:

•S Те, кто несут ответственность за безопасность, защиту персональных данных, контроль и управление рисками. **•S** Те, кто обеспечивают соответствие требованиям. **•S** Те, кто нуждаются или оказывают аудиторские услуги.

Что

Чтобы соответствовать приведенным выше требованиям, методология управления и контроля в сфере ИТ должна:

• Сосредоточиться на потребностях бизнеса, чтобы обеспечивать соответствие между целями бизнеса и ИТ.

• Ориентироваться на процессы, чтобы определить масштаб и степень охвата, а также быть хорошо структурированной, чтобы обеспечить удобство пользования.

• Быть общепринятой с точки зрения согласованности с признанными лучшими практиками и стандартами в сфере ИТ, но независимой от конкретных технологий.

• Предлагать общий язык с помощью терминологии и определений, понимаемыми всеми заинтересованными сторонами.

• Помогать соответствовать регулирующим требованиям через соответствие с общепринятыми стандартами корпоративного управления (например, COSO) и мерами контроля в сфере ИТ, которые ожидают видеть регулирующие органы и внешние аудиторы.

Как COBIT отвечает этим потребностям

Чтобы соответствовать описанным выше потребностям, методология COBIT была разработана как нацеленная на бизнес, ориентированная на процессы, основанная на контроле и управляемая посредством измерения показателей.

Нацеленность на бизнес

Ориентация на бизнес — это лейтмотив COBIT. Методология разработана не только для применения сервис провайдерами ИТ, конечными пользователями и аудиторами, но также (что более важно) для всестороннего руководства менеджменту и владельцам бизнес процессов. Методология COBIT основана на следующем принципе **(схема 5):** для того, чтобы организация обеспечила себя информацией, которая необходима для достижения ее целей, организация должна инвестировать и управлять ресурсами ИТ посредством структурированного комплекса процессов, которые обеспечивают сервисы для предоставления информации.

Управление и контроль над информацией являются центром методологии COBIT и помогают соответствовать требованиям бизнеса.

Протеоднт , - - ИсПбЛи*у»тя

Схема 5. Основной принцип методологии COBIT

Информационные критерии по **COBIT**

Чтобы удовлетворять бизнес целям, информация должна соответствовать определенным контрольным критериям, которые COBIT определят как требования бизнеса к информации. Основанные на общих требованиях качества, доверия и безопасности, определены семь четких, взаимосвязанных критериев информации:

• Полезность характеризует информацию как значимую и имеющую отношение к бизнес процессу, а также получаемую регулярно, корректно, последовательно и в удобном виде.

• Эффективность характеризует получение информации посредством оптимального (наиболее продуктивного и экономичного) использования ресурсов.

• Конфиденциальность имеет отношение к защите важной информации от несанкционированного раскрытия.

• Целостность связана с точностью и полнотой информации, а также с ее обоснованностью в соответствии с корпоративными ценностями и ожиданиями.

• Доступность имеет отношение к наличию информации, когда она необходима в бизнес процессе (в настоящий момент или в будущем). Также это касается защиты необходимых ресурсов и связанных с ними возможностей.

• Соответствие требованиям выражается в соответствии законам, регулирующим актам и условиям контрактов, для которых бизнес процесс является субъектом, то есть внешним требованиям к бизнесу, равно как и внутренней корпоративной политике.

• Достоверность относится к обеспечению надлежащей информацией руководства для выполнения им своих обязанностей.

Цели бизнеса и цели ИТ

В то время как информационные критерии дают общую методику определения бизнес требований к информации, общее определение целей бизнеса и ИТ дает более точное и бизнес-ориентированное понимание и требуется для выявления показателей, с помощью которых можно измерить достижение поставленных целей. Каждая организация использует ИТ для реализации инициатив в сфере бизнеса, которые могут быть представлены как бизнес цели для ИТ. Эти общие примеры могут быть использованы в качестве руководства к определению специфических требований бизнеса, целей и показателей организации.

Для того, чтобы ИТ успешно поддерживали выполнение корпоративной стратегии, должно существовать четкое владение и руководство в исполнении требований со стороны бизнеса (как клиента) и четкое понимание того, что требуется и как это делать, со стороны службы ИТ (как поставщика услуг). На схеме 6 показано, как корпоративная стратегия должна преобразовываться бизнесом в цели, связанные с ИТ инициативами (бизнес цели для ИТ). Эти цели должны вести к четкому определению собственно ИТ целей, которые, в свою очередь, определяют ИТ ресурсы и возможности (корпоративная архитектура ИТ), необходимые для успешного исполнения той части корпоративной стратегии, которая возлагается на ИТ[1].

Как только связанные цели определены, их достижение нужно контролировать, чтобы быть уверенным в том, что текущее положение соответствует ожиданиям. Это достигается с помощью показателей, которые проистекают из самих целей и фиксируются в системе сбалансированных ИТ показателей.

Для понимания заказчиками ИТ сервисов целей ИТ и системы сбалансированных ИТ показателей, все эти цели и связанные с ними показатели должны быть выражены в значимых и понятных бизнесу терминах. В сочетании с эффективными взаимосвязями внутри иерархии целей, это может служить подтверждением той поддержки, которую оказывает ИТ в достижении корпоративных целей.

Как показано на схеме 6, эти стимулы взяты из корпоративного управления бизнесом, изначально более акцентируясь на функциональности и быстроте обслуживания, затем все больше на эффективности инвестиций, доходе на инвестиции (ROI) и соответствии требованиям.

[1] Следует отметить, что определение и внедрение корпоративной архитектуры ИТ также порождает внутренние цели ИТ, которые вносят вклад в достижение бизнес целей, но не следуют из них непосредственно.

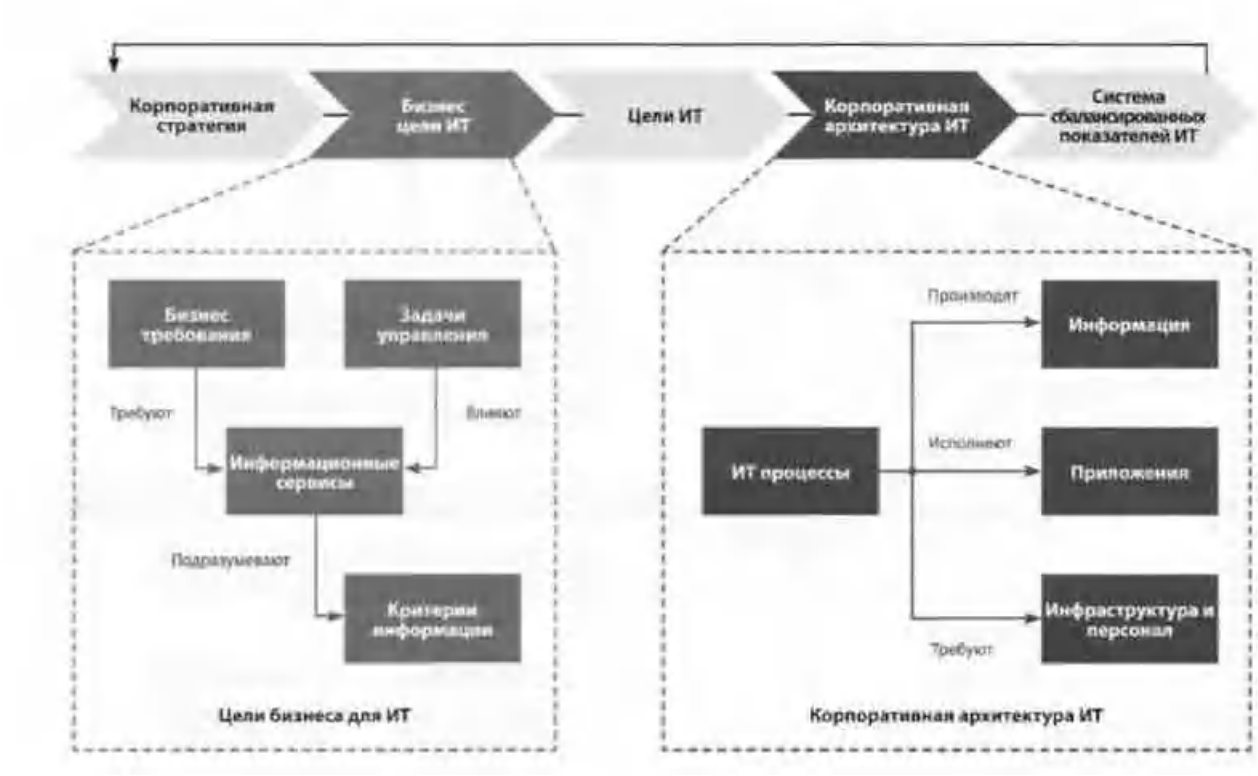


Схема 6. Определение целей ИТ и корпоративная архитектура ИТ

ИТ ресурсы

Организация ИТ стремится к достижению поставленных целей посредством четко определенных процессов, в которых задействуются навыки персонала и технологическая инфраструктура, обеспечивающие выполнение бизнес приложений, с целью предоставления бизнес информации. Эти ресурсы, вместе с процессами, образуют корпоративную архитектуру ИТ, как показано на **схеме 6.**

Чтобы соответствовать бизнес требованиям в сфере ИТ, организации нужно инвестировать в ресурсы, необходимые для создания адекватных технических возможностей (например, системы корпоративного планирования ресурсов (ERP)) для поддержания возможностей бизнеса (например, внедрения эффективного управления каналами поставок), имеющих в результате желаемую отдачу (например, рост продаж и финансовых выгод).

ИТ ресурсы определяются в COBIT следующим образом:

• Приложения — прикладные системы и ручные процедуры для обработки информации.

• Информация — данные в любой форме, введенные, обработанные и выведенные информационными системами в любой используемой бизнесом форме.

• Инфраструктура — это технология и устройства (например, аппаратное обеспечение, операционные системы, системы управления базами данных, сетевое оборудование, мультимедиа, а также та среда, в которой все это находится и поддерживается), которые обеспечивают работу приложений.

• Персонал — люди, необходимые для планирования, организации, приобретения, внедрения, работы, обслуживания, мониторинга и оценки информационных систем и услуг. Персонал может быть внутренним, привлеченным на аутсорсинге или нанятым по контракту в случае необходимости.

На **схеме 7** показано, как бизнес цели для ИТ воздействуют на ИТ ресурсы, которые должны управляться в рамках ИТ процессов для достижения целей ИТ.

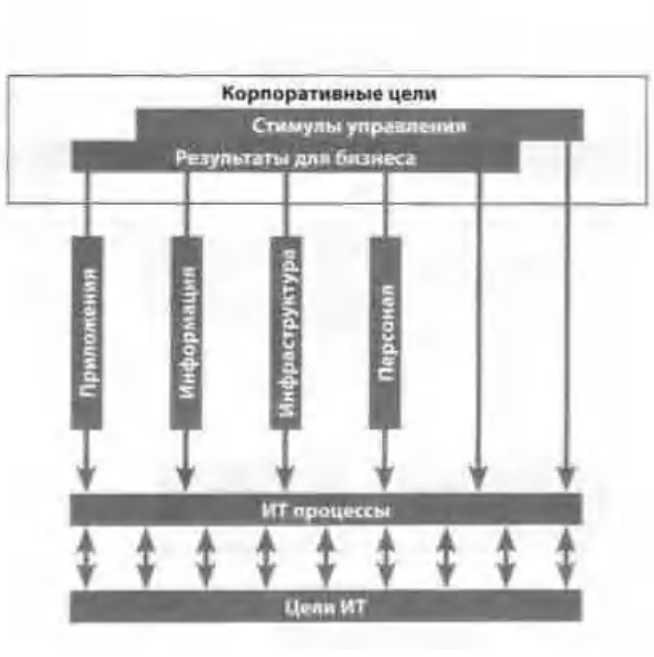


Схема 7. Управление ресурсами ИТ для достижения целей ИТ Ориентация на процессы

COBIT представляет виды деятельности в сфере ИТ в виде типовой модели процессов, состоящей из четырех доменов (групп). Эти домены называются «Планирование и Организация», «Приобретение и Внедрение», «Эксплуатация и Сопровождение» и «Мониторинг и Оценка». Домены отражают традиционные зоны ответственности в сфере ИТ, связанные с планированием, созданием, сопровождением и мониторингом.

Методология COBIT предлагает референтную базовую модель процессов и общий язык для каждого, кто управляет деятельностью ИТ в организации. Соединение операционной модели и общего языка для всех частей бизнеса, вовлеченных в ИТ, является одним из отправных и наиболее важных шагов навстречу хорошему управлению. COBIT также предлагает методологию для измерения и мониторинга эффективности в сфере ИТ, взаимодействия с поставщиками услуг и внедрения лучших практик управления. Модель процессов способствует определению владельцев конкретных процессов, устанавливает ответственность и отчетность.

Чтобы эффективно руководить сферой ИТ, необходимо получить представление о видах деятельности и рисках ИТ, которыми необходимо управлять. Как правило, они укладываются в домены (группы), связанные с планированием, реализацией, обслуживанием и контролем. В методологии COBIT эти домены, как показано на схеме **8,** называются:

• Планирование и Организация (PO) — Определяет направления в отношении внедрения решений (AI) и обеспечения сервисов (DS).

• Приобретение и Внедрение **(AI)** — Обеспечивает внедрение решений и оказание сервисов на их основе.

• Эксплуатация и Сопровождение **(DS)** — Предоставляет решения и делает их применимыми для конечных пользователей.

• Мониторинг и Оценка **(ME)** — Выполняет надзор за всеми процессами, чтобы убедиться в продвижении в верном направлении.

Схема 8. Четыре взаимосвязанных раздела COBIT

Планирование и Организация (PO)

Эта группа процессов охватывает стратегию и тактику и определяет тот путь, с помощью которого ИТ внесет больший вклад в достижение бизнес целей. Реализация стратегического видения должна быть спланирована, донесена до заинтересованных сторон и управляема с различных точек зрения. Должны быть внедрены как правильная организация, так и технологическая инфраструктура. Этот домен отвечает на следующие вопросы управления:

- Согласованы ли ИТ стратегия и корпоративная стратегия?
- Достигает ли организация оптимального использования своих ресурсов?
- В с е л и в организации понимают цели, поставленные перед ИТ?
- Осознаются ли ИТ риски и осуществляется ли управление ими?
- Соответствует ли качество систем ИТ потребностям бизнеса?

Приобретение и Внедрение (AI)

Чтобы воплотить ИТ стратегию, ИТ решения должны быть выявлены, разработаны или приобретены, а также внедрены и интегрированы в бизнес процесс. Кроме того, внесение изменений в существующие системы (равно как и обслуживание последних) относится к этому разделу методологии, так как нужна уверенность в том, что ИТ решения продолжают соответствовать бизнес целям. В этом домене даются ответы на следующие вопросы:

- Предлагают ли новые проекты решения, отвечающие потребностям бизнеса?
- Укладываются ли новые проекты в отведенные сроки и бюджет?
- Будут ли новые системы после своего внедрения работать должным образом?
- Удастся ли внедрить изменения без сбоев в текущих бизнес операциях?

Эксплуатация и Сопровождение (DS)

Этот раздел связан с вопросами текущего предоставления услуг, что включает собственно предоставление услуг, обеспечение безопасности и непрерывности сервисов, поддержку конечных пользователей, управление данными и операционной инфраструктурой. В этом домене рассматриваются следующие вопросы:

- Предоставляются ли ИТ услуги в соответствии с приоритетами бизнеса?

• Оптимизированы ли затраты на ИТ?

• Способен ли персонал использовать ИТ системы эффективно и безопасно?

• Обеспечивается ли в рамках информационной безопасности должный уровень конфиденциальности, целостности и доступности?

Мониторинг и Оценка (ME)

Все ИТ процессы должны регулярно оцениваться на предмет их качества и соответствия требованиям контроля. Данный домен рассматривает вопросы управления эффективностью, мониторинга системы внутреннего контроля, соответствия требованиям регулирующих норм и корпоративного управления. Основные рассматриваемые вопросы:

• Как выявить проблемы, связанные с эффективностью ИТ процессов, пока не стало слишком поздно?

• Может ли менеджмент быть уверен в том, что меры внутреннего контроля результативны и эффективны?

• Как установить обратную связь между эффективностью ИТ и целями бизнеса?

• Обеспечивается ли в рамках информационной безопасности должный уровень конфиденциальности, целостности и доступности?

Внутри этих четырех доменов COBIT выделяет 34 обычно используемых ИТ процесса (их полный список см. в **схеме 22).** В то время как большинство организаций определили зоны ответственности в планировании, реализации, обслуживании и мониторинге в сфере ИТ, и большинство имеют одни и те же ключевые процессы, лишь у немногих организаций могут совпадать структура процессов или же будут задействованы все 34 процесса, описанные в COBIT. COBIT предлагает полный список процессов, которые могут применяться для проверки полноты отдельных видов деятельности и обязанностей, однако не требуется применять их все и, более того, эти процессы могут комбинироваться в соответствии с требованиями каждой конкретной организации.

Для каждого из 34 процессов приводятся бизнес и ИТ цели, которые обеспечивает данный процесс. Также приводится информация о том, как оценивается прогресс в достижении целей, каковы основные виды деятельности и результаты, а также о том, кто является ответственным за достижение результатов.

Методология, основанная на контроле

COBIT определяет цели контроля для всех 34 процессов, равно как и рамочные меры контроля для процессов и приложений.

Процессам нужны меры контроля

Контроль определяется как политики, процедуры, практики и организационные структуры, созданные для обеспечения разумной уверенности в том, что бизнес цели будут достигнуты, нежелательные события предотвращены, а их последствия идентифицированы и исправлены.

Цели контроля ИТ дают полный комплекс требований высокого уровня для руководства по эффективному контролю над каждым ИТ процессом. Цели контроля:

• Являются формулировками управленческих действий по повышению ценности или минимизации риска.

• Включают в себя политики, процедуры, практики и организационные структуры.

• Созданы для обеспечения разумной уверенности в том, что бизнес цели будут достигнуты, нежелательные события предотвращены, а их последствия идентифицированы и исправлены.

Руководство организации должно выбирать решения, соответствующие этим целям контроля путем:

• Отбора тех решений, которые применимы в данной ситуации.

• Выбора тех, которые могут быть реализованы на практике.

• Отбора в зависимости от условий их реализации (частота, диапазон, автоматизация и т. д.).

• Учета риска невозможности реализации.

Помощь может оказать базовая модель контроля, изображенная на **схеме 9.** Она следует принципам очевидной в данном случае аналогии: когда в системе обогрева (процесс) устанавливается значение требуемой температуры (стандарт), система постоянно проводит замеры (сравнения) температуры окружающего воздуха (контрольная информация) и подаст команду (действие) обогревателю вырабатывать больше или меньше тепла.

Схема 9. Модель контроля Операционное руководство использует процессы для организации и управления текущей ИТ деятельностью. COBIT предлагает общую

модель процессов, в которой содержатся все процессы, обычно присутствующие в функциях ИТ. Данная модель носит эталонный характер и понятна операционному ИТ персоналу и руководству бизнеса. Чтобы достичь эффективного управления, меры контроля должны реализовываться операционным менеджментом согласно определенной методологии контроля для всех ИТ процессов. Поскольку цели контроля в COBIT организованы по отдельным ИТ процессам, методология дает четкие связи между требованиями управления ИТ, ИТ процессами и мерами контроля в сфере ИТ.

Каждый из ИТ процессов в COBIT имеет свое описание и набор целей контроля. В целом они являются признаками хорошо управляемого процесса.

Цели контроля обозначаются двухбуквенными сокращениями названий разделов (PO, AI, DS и ME), к которым добавлен номер процесса и номер цели контроля. В дополнение к целям контроля, каждый процесс в COBIT имеет общие требования контроля, которые обозначаются как PC (Process control). Для того чтобы иметь полное представление о требованиях контроля, их нужно рассматривать вместе с целями контроля процесса.

PC1. Цели и задачи процесса

Определить и донести до сведения всех заинтересованных сторон конкретные, измеряемые, исполнимые, реалистичные, ориентированные на результат и своевременные (SMARRT) цели и задачи для эффективного выполнения каждого ИТ процесса. Следует убедиться, что цели и задачи процесса связаны с бизнес целями и обеспечены соответствующими метриками оценки.

PC2. Владение процессом

Определить владельца для каждого ИТ процесса, четко сформулировать его роли и сферы ответственности. Включить, например, ответственность по разработке процесса, взаимодействие с другими процессами, отчетность по конечным результатам, оценку эффективности и поиск возможностей по улучшению.

PC3. Повторяемость процесса

Разработать и реализовать каждый ключевой ИТ процесс таким образом, чтобы он был повторяемым и постоянно приносил ожидаемые результаты. Создать логичную, но гибкую и масштабируемую последовательность действий, которая приведет к желаемым результатам и будет достаточно гибкой для нестандартных ситуаций и экстренных случаев. Использовать последовательные процессы во всех случаях, когда это возможно, и видоизменять их только когда это неизбежно.

PC4. Роли и ответственности

Определить ключевые действия и конечные результаты процесса. Назначить и донести однозначное понимание ролей и ответственностей для эффективного и результативного исполнения и документирования ключевых действий, а также для отчетности по конечным результатам процесса.

PC5. Политики, планы и процедуры

Определить и донести до всех заинтересованных сторон, как политики, планы и процедуры, которые движут ИТ процессом, документируются, пересматриваются, поддерживаются, утверждаются, хранятся, перелаются и используются для обучения. Назначить ответственности для каждого из вышеприведенных видов деятельности и, по мере времени, проверять, исполняются ли они должным образом. Убедиться, что политики, планы и процедуры доступны, правильны, понятны и актуализированы.

PC6. Повышение эффективности процесса

Определить набор показателей, которые позволят оценить результаты и эффективность процесса. Поставить конкретные задачи, которые соответствуют целям процесса и выявить показатели, которые отражают достижение этих целей. Описать, как должен происходить сбор данных. Сравнить текущие показатели с планируемыми и при необходимости действовать с учетом возможных отклонений. Сопоставить показатели, цели и методы в рамках единого подхода к оценке эффективности процессов ИТ.

Меры эффективного контроля снижают риски, повышают вероятность получения выгоды и улучшают эффективность, благодаря сокращению числа ошибок и более последовательному подходу в управлении.

В дополнение, COBIT предлагает примеры для каждого из процессов, которые иллюстрируют (хотя и не предписывают) следующее:

- Входящая информация и результаты процесса в общем виде.
- Действия и рекомендации в отношении ролей и ответственностей, которые отражены в таблице ОУКИ (RACI). В ней показано, кто из должностных лиц является ответственным, утверждающим, консультирующим и информированным.
- Цели ключевых видов деятельности ИТ (основные действия, которые нужно выполнить).
- Показатели.

Помимо оценки того, какие меры контроля необходимы, владельцы процессов должны понимать, какая входящая информация им требуется извне и что ожидают от их процессов другие заинтересованные стороны. COBIT предлагает примеры с исходными данными и результатами для каждого процесса, включая внешние требования в сфере ИТ. Существуют результаты, которые одновременно являются исходными данными для других процессов, они обозначены знаком «ВСЕ» (ALL) в таблицах результатов, но не упоминаются в качестве входящей информации всех процессов. Обычно они включают стандарты качества и показатели результативности, методологию процесса

ИТ, документацию по ролям и ответственностям, корпоративную методологию контроля в сфере ИТ, политики в сфере ИТ, а также персональные роли и ответственности.

Понимание ролей и ответственностей для каждого из процессов является непременным условием эффективного управления. Методология COBIT предлагает таблицу ОУКИ (RACI) для каждого процесса. «Утверждающий» — это своего рода «конечная инстанция», должностное лицо, определяющее направление и утверждающее действия и результаты. Термин «ответственный» относится к лицу, которое несет ответственность за действие, задание. Остальные две роли («консультирующий» и «информированный») призваны контролировать, чтобы в процесс были вовлечены все необходимые лица.

Бизнес и меры контроля в сфере ИТ

Корпоративная система внутреннего контроля воздействует на сферу ИТ на трех уровнях:

• На уровне высшего руководства устанавливаются политики и бизнес цели, а также принимаются решения о том, как задействовать и управлять ресурсами организации для исполнения корпоративной стратегии. Общий подход к управлению и контролю устанавливается Советом директоров и доносится до сведения в организации. Контроль в сфере ИТ направляется политиками и рядом целей высокого уровня.

• На уровне бизнес процесса меры контроля принимаются в отношении специфических видов деятельности. Большинство бизнес процессов автоматизированы и интегрированы с системой ИТ приложений, в результате чего многие меры контроля на этом уровне также автоматизированы. Эти меры контроля известны как контроль приложений. Однако часть мер контроля внутри бизнес процессов остается в виде ручных процедур, таких как авторизация операций, разделение обязанностей и выверка. Поэтому меры контроля на уровне бизнес процессов представляют собой комбинацию мер контроля, осуществляемы вручную (выполняются персоналом) и автоматизированных. Определение и управление обеими видами мер контроля относится к прерогативе бизнеса, хотя при реализации контроля приложений также задействована служба ИТ для поддержки дизайна и разработки.

• Для поддержки бизнес процессов сфера ИТ предоставляет услуги, зачастую общие для многих бизнес процессов, поскольку многие ИТ процессы задействованы в масштабах всей организации, а ИТ инфраструктура способна предоставлять общие для всех пользователей услуги (например, сети, базы данных, операционные системы и хранилища данных). Меры контроля, применяемые для ИТ услуг в целом называются общими мерами контроля ИТ. От надежности выполнения этих мер контроля зависит надежность контроля приложений. Например, плохо налаженное управление внесением изменении может поставить под угрозу (случайно или преднамеренно) надежность автоматизированной проверки целостности.

Общие меры контроля в ИТ и меры контроля приложений

Общие меры контроля включены в состав ИТ процессов и услуг. Примерами являются:

- Разработка систем
- Внесение изменений
- Безопасность
- Компьютерные операции (операции по эксплуатации систем).

Меры контроля, включенные в состав приложений, поддерживающих бизнес процесс, обычно называют мерами контроля приложений. Примерами являются:

- Полнота
- Точность
- Достоверность
- Авторизация
- Разделение обязанностей.

COBIT относит разработку и внедрение автоматизированных мер контроля приложений к ответственностям ИТ и рассматривает их в разделе «Приобретение и Внедрение» на основе бизнес требований, определенных согласно информационным критериям COBIT, как показано в **схеме 10.** Операционное управление и обязанности по контролю приложений относятся не к ИТ, а к владельцу процесса со стороны бизнеса.

Поэтому обязанности в отношении мер контроля приложений являются от начала до конца совместной ответственностью бизнеса и ИТ и разделяются следующим образом:

Бизнес отвечает за:

- Определение функциональных и контрольных требований.
- Применение автоматизированных сервисов. ИТ

отвечает за:

- Автоматизацию и внедрение функциональных и контрольных требований.
- Осуществление контроля с целью обеспечения целостности мер контроля ИТ приложений.

Следовательно, ИТ процессы в COBIT охватывают общие меры контроля ИТ и только отдельные аспекты разработки в мерах контроля приложений; ответственность за определение и операционное применение этих мер контроля возлагается на бизнес.

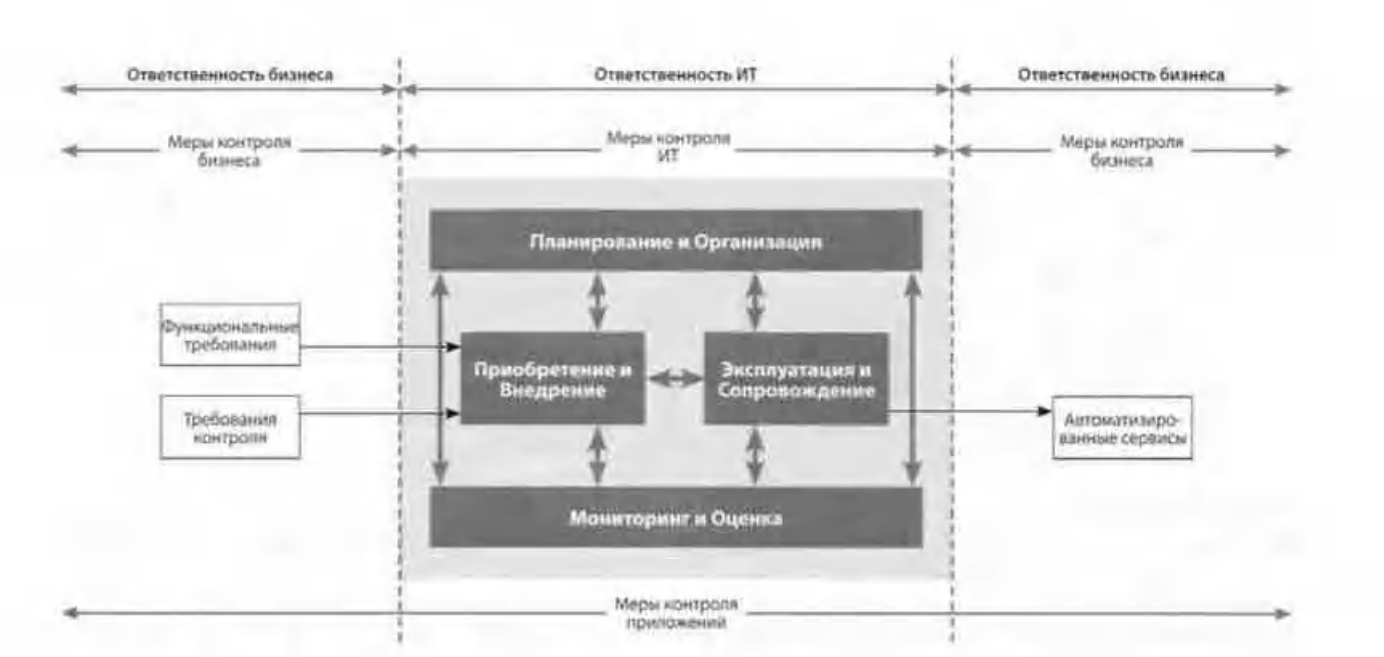


Схема 10. Сферы корпоративного, общего контроля и контроля приложений

В приведенном ниже перечне содержатся рекомендуемые цели для контроля приложений. Они обозначаются по номеру контроля приложения AC (Application control).

AC1. Подготовка исходных данных и авторизация

Следует убедиться, что исходные документы подготовлены уполномоченным и квалифицированным персоналом согласно установленным процедурам, с учетом адекватного разделения обязанностей, относящихся к созданию и утверждению данных документов. Ошибки и пропуски должны быть сведены к минимуму в процессе ввода с помощью надлежащей формы ввода. Выявить ошибки и иные отклонения от нормы таким образом, чтобы их можно было документировать и исправить.

AC2. Сбор исходных данных и ввод

Установить так, чтобы ввод данных выполнялся своевременно уполномоченным и квалифицированным персоналом. Исправление ошибок и повторный ввод данных (которые были первоначально введены с ошибками) должен выполняться с исполнением требований авторизации на всех необходимых уровнях. Следует по возможности сохранять оригиналы, с которых осуществлялся ввод данных в течение достаточного периода времени.

ЛС3. Проверка точности, полноты данных и аутентичности

Обеспечить точность, полноту и достоверность транзакций. Проверку достоверности данных, редактирование или отсылку назад для корректировки следует осуществлять по возможности близко к источнику исходных данных.

AC4. Целостность и достоверность данных в процессе обработки

Поддерживать целостность и достоверность данных в течение всего процесса их обработки. Обнаружение ошибок в транзакциях не должно нарушать обработку корректных транзакций.

AC5. Согласование и выверка данных на выводе

Установить процедуры и связанные с ними обязанности, чтобы вывод данных, анализ ввода, выверка данных и обработка ошибок осуществлялись при условии авторизации, данные направлялись нужному получателю и были защищены в процессе передачи; чтобы осуществлялись проверки подлинности и точности данных; чтобы выводимые данные использовались.

AC6. Проверка подлинности и целостности транзакций

До передачи данных транзакций между внутренними приложениями и бизнес/операционными подразделениями (внутри или вне организации), проверить правильность адресации, истинность происхождения и целостность. Поддерживать подлинность и целостность данных в процессе передачи или пересылки.

Методология, основанная на показателях

Базовая потребность каждой организации заключается в понимании статуса собственных ИТ систем и решении того, на каком уровне нужно обеспечить управление и контроль над ИТ. Чтобы принять правильное решение, руководство должно задать себе вопрос: «Как далеко следует продвинуться и оправдаются ли затраты?»

Составить объективное представление о собственном уровне эффективности организации не просто. Что должно быть оценено (измерено) и каким образом? Организации должны оценить, во-первых, свое текущее положение, во-вторых, определить, где именно им требуются улучшения и, в-третьих, внедрить инструментарий мониторинга этих улучшений. Для этих целей COBIT предлагает:

- Модели зрелости для проведения сравнительного анализа и выявления необходимых улучшений.
- Цели и показатели эффективности для ИТ процессов, показывающие, насколько процессы отвечают бизнес и ИТ целям, а также применяются для оценки эффективности процессов на основе системы сбалансированных показателей.
- Цели действий для повышения эффективности процессов.

Модели зрелости

Высшее руководство организаций проявляет все возрастающий интерес к тому, насколько хорошо осуществляется управление в сфере ИТ. Соответственно, бизнес практика требует постоянного совершенствования и достижения должного уровня управления и контроля над информационной инфраструктурой. Если попытаться оспорить это утверждение, то сначала придется ответить на вопросы, связанные с балансом преимуществ и затрат:

• Как обстоят дела у наших конкурентов по отрасли, как мы можем оценить себя по сравнению с ними?

• Каковы принятые в отрасли лучшие практики и как мы можем оценить себя на их основе?

• Основываясь на этих сравнениях, можем ли мы сказать, что предпринимаем достаточные усилия?

• Как мы определяем, что требуется для достижения должного уровня управления и контроля над нашими ИТ процессами?

Зачастую трудно дать четкие ответы на эти вопросы. Для того чтобы знать, в чем заключается эффективное руководство, руководству ИТ приходится постоянно проводить сравнительный анализ и применять инструменты самооценки. Исходя из ИТ процессов COBIT, владелец процесса должен быть готов регулярно анализировать продвижение к контрольной цели. Это отвечаеттрем потребностям:

1. Сравнение с целью понять, где находится организация;
2. Принятие эффективного решения по вопросу в каком направлении двигаться;
3. Инструментарий для оценки степени достижения цели.

Модели зрелости для управления и контроля над ИТ процессами основаны на методе оценки организации и содержат пять градаций уровня зрелости: от «несуществующего» (0) до «оптимизированного» (5). Этот подход заимствован из модели зрелости, предложенной Институтом по разработке программного обеспечения (Software Engineering Institute, SEI) для оценки зрелости процесса разработки программного обеспечения. Хотя принципы предложенной SEI модели сохранены, ее реализация в методологии COBIT существенно отличается от первоисточника. Исходная модель была ориентирована на принципы разработки программного обеспечения и формальную оценку уровня зрелости, на основании которой разработчики признавались «сертифицированными». В COBIT предлагается шкала зрелости, аналогичная шкале от SEI. но интерпретируемая в отношении управления ИТ

процессов. На основе этой шкалы даются специфические модели зрелости для каждого из 34 ИТ процессов. Вне зависимости от модели, шкалы градаций не должны быть слишком дробными, так как это затруднит использование, оценку текущего состояния и определение приоритетов для улучшения. Цель модели — не оценка точности выполнения целей контроля.

Уровни зрелости выступают в качестве профилей ИТ процессов, которые организация воспринимает как описания возможного положения дел в настоящем и будущем. Их нельзя трактовать как некие пороговые уровни, переход вверх между которыми возможен только при выполнении всех требований предыдущих уровней. В модели зрелости COBIT (в отличие от модели SEI) не ставится цель точно оценить уровень зрелости или сертифицировать достигнутый уровень. Оценка зрелости в COBIT является результатом профиля процесса, где в той или иной степени присутствуют требования всех уровней, как показано на **схеме 11**.

Схема 11. Возможная модель зрелости для ИТ процесса

Возможная модель зрелости для ИТ процесса. В примере показан процесс, в значительной мере достигающий зрелости на 3 уровне, хотя некоторые проблемы совместимости с требованиями более низких уровней продолжают оставаться, и в то же время присутствуют элементы более высоких уровней: оценка эффективности (4 уровень) и оптимизация (5 уровень).

Это объясняется тем, что при оценке зрелости по моделям COBIT часто бывает, что отдельные требования различных уровней в рамках процесса достигают разных уровней зрелости, несмотря на незавершенность или недостаточность. Эти сильные стороны могут быть внедрены для повышения зрелости в дальнейшем. Например, некоторые элементы процесса могут быть четко определены и, даже, несмотря на незавершенность остальных элементов, будет неправильным утверждать, что процесс не определен в целом.

Используя модели зрелости для каждого из 34 ИТ процессов, руководство может определить:

- Текущую эффективность организации. (Где организация находится сейчас).
- Текущее положение дел в отрасли. (Сравнение).
- Корпоративные цели по совершенствованию. (Где организация желала бы находиться).
- Требуемые меры по совершенствованию от состояния «как есть» к «как должно быть».

Для простоты интерпретации результатов для руководства ниже приведена схема реализации этих принципов **(схема 12).**

Схема 12. Графическое изображение модели зрелости

Уровни зрелости

0 Несуществующий
1 Начальный/Повторяющийся эпизодически и бессистемно
2 Повторяющийся, но интуитивный
3 Определенный
4 Управляемый и измеряемый
5 Оптимизированный

Символы

W Текущее положение организации

Средний показатель для отрасли ^

Цель организации Описания уровней

0 Процессы управления не применимы вообще
1 Процессы используются разово или в отдельных случаях и не организованы
2 Процессы повторяются по образцу
3 Процессы документально оформлены и доведены до сведения заинтересованных лиц
4 Ведется мониторинг процессов в измеряемых показателях
5 Лучшие практики внедрены и автоматизированы Общее

описание уровней модели зрелости приводится в схеме **13.**

0	Несуществующий. Полное отсутствие каких-либо заметных процессов. Организация даже не осознает существование проблем, которые надо решать.
1	Начальный/Повторяющийся эпизодически и бессистемно. Есть свидетельства того, что организация осознает существование проблем и необходимость их решения. Нет никаких стандартизированных процессов, однако существуют подходы, применяемые в отдельных случаях. Организованный подход к управлению отсутствует. Повторяющийся, но интуитивный. Процессы достигли уровня, при котором разные сотрудники, выполняющие одну и ту же задачу, и пользуют сходные процедуры. Не существует формализованного обучения и информирования о принятых в организации процедурах, ответственность за используемые процедуры целиком лежит на сотрудниках. Организация в большой степени зависит от знаний отдельных лиц,
2	вследствие чего велика вероятность ошибок.
3	Определённый. Процедуры стандартизированы, документально оформлены и доводятся до сведения сотрудников организации посредством обучения. Существуют требования следовать формально описанному процессу, однако маловероятно, что отклонения будут обнаружены. Сами процедуры не являются сложными и представляют собой формализованный вариант существующей практики.
4	Управляемый и измеряемый. Существует возможность контроля и оценки степени соответствия принятым процедурам, а также возможность принятия мер в случае, если процессы неэффективны. Процессы постоянно совершенствуются и соответствуют общепринятой практике. Автоматизированные и инструментальные средства по управлению эффективностью процесса используются ограниченно или эпизодически.
5	Оптимизированный. Процессы оптимизированы до уровня лучших практик, они базируются на результатах непрерывного совершенствования и сравнений с другими организациями с использованием моделей зрелости процессов. ИТ используются для комплексной автоматизации документооборота, предоставляя средства повышения качества и эффективности, а также увеличивая способность организации к быстрой адаптации.

Схема 13. Общая модель зрелости процесса COBIT представляет собой методологию управления ИТ процессами с акцентом на контроль. Приведенные выше шкалы должны быть практичными в применении и

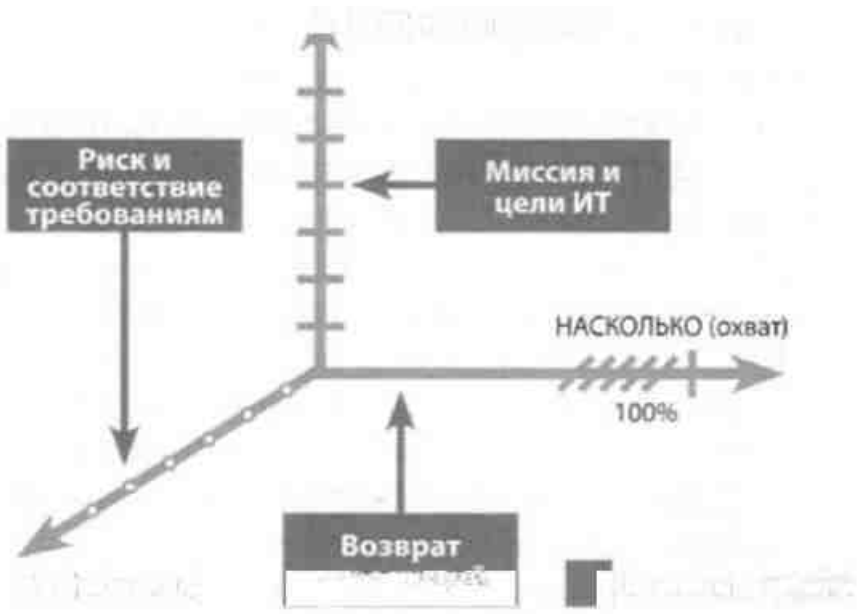
доступными для понимания. Вопросы управления ИТ процессами по существу сложны и субъективны, поэтому использование оценок позволит повысить уверенность, достичь единого мнения среди высшего руководства и побудить к совершенствованиям. Можно проводить оценку, исходя из формулировки уровня модели зрелости, или, более строго, исходя из каждого утверждения внутри этой формулировки. В любом случае, требуется знание ИТ процессов в организации.

Преимущество подхода с использованием моделей зрелости процесса состоит в том, что руководство может сравнительно легко определить уровень своей организации по шкале градаций и, в случае необходимости, повысить эффективность, оценить, какие меры необходимо внедрить. Шкала содержит градации от 0 до 5, поскольку вполне может оказаться так, что процесса не существует вообще. Данная шкала основана на простой модели зрелости процесса и демонстрирует, как тот или иной процесс эволюционирует от уровня «несуществующий» до уровня «оптимизированный».

Тем не менее, управляемость процессом есть не то же самое, что и эффективность процесса. Управляемость, определенная бизнес и ИТ целями, может и не требоваться на одном и том же уровне в масштабах всей сферы ИТ организации (например, процесс может выполняться лишь ограниченным числом систем или подразделений). Оценка эффективности, о чем будет сказано ниже, необходима для того, чтобы определить вклад текущей эффективности организации в работу ИТ процессов.

Хотя правильное применение ИТ управляемости уменьшает степень рисков, организация должна проанализировать, какие меры контроля необходимы для минимизации рисков и получения выгоды с учетом рисков и бизнес целей. Эти меры контроля приводятся в целях контроля COBIT. В Приложении I приведена модель зрелости внутреннего контроля, которая показывает зрелость организации в связи с эффективностью исполнения мер внутреннего контроля. Зачастую такой анализ проводится под воздействием внешних факторов, но в идеале, он должен проводится согласно установлениям процесса P06 «Информирование о целях и направлениях развития ИТ» и ME2 «Мониторинг и оценка системы внутреннего контроля».

Управляемость, охват и контроль — три измерения зрелости процессов, как показано на **схеме 14.**



A КАК (управляемость)

ЧТО ;конгроль) ^^^^^^^^^Ц **| Основные Стимулы**

Схема 14. Три измерения зрелости Модель зрелости процесса позволяет измерить, насколько качественно развиты процессы управления, то есть, какими возможностями они обладают. Уровень развития и возможности процессов управления в первую очередь зависят от целей ИТ и тех потребностей бизнеса, которым они служат. Насколько задействованы их возможности в большой мере зависит от того результата, который организация рассчитывает получить от

своих инвестиций в ИТ. Например, могут быть критичные процессы и системы, требующие повышенного внимания к безопасности, в то время как другие процессы могут быть менее критичными. С другой стороны, степень развития и сложность мер контроля, требуемых для применения в ходе процесса, больше зависит от корпоративной стратегии управления рисками и применимых требований, которым необходимо соответствовать.

Шкала градаций модели зрелости поможет специалистам указать руководству на недостатки в управлении ИТ процессами и поставить цели дальнейшего развития. На выбор уровня зрелости будут влиять бизнес цели, а также условия, в которых функционирует организация и отраслевая практика. В частности, уровень зрелости механизмов управления будет определяться степенью зависимости организации от ИТ, степенью сложности технологии и, что наиболее важно, ценностью информации, которой она располагает.

Стратегическим ориентиром для организации, планирующей улучшить управление и контроль ИТ процессов, может стать анализ новейших международных стандартов и лучшей отраслевой практики. Зарождающаяся сегодня практика завтра сможет стать ожидаемым уровнем эффективности и поэтому очень важно, чтобы это было учтено при планировании развития организации.

Модели зрелости процессов основаны на универсальной качественной модели (см. **схему 13),** в которой с каждым уровнем повышается степень внедрения принципов и соответствующей практики в рамках следующих аспектов:

- Осведомленность и информированность.
- Политики, планы и процедуры.
- Инструментарии и средства автоматизации процесса.
- Навыки и компетенция.
- Ответственность и отчетность.
- Постановка целей и оценка их достижения.

В таблице атрибутов зрелости на **схеме 15** приводятся характеристики управляемости ИТ процессов и описание того, как они эволюционируют от «не существующего» до «оптимизированного» уровня. Эти характеристики могут быть использованы для более детальной оценки, анализа недостатков и планирования усовершенствований.

Резюмируя вышеизложенное, можно сказать, что модели зрелости процессов дают представление об этапах, через которые проходит эволюция управления и контроля ИТ процессов. Модели зрелости:

- Представляют собой набор требований и аспектов, характеризующие разные уровни зрелости.
- Представляют собой шкалу оценок, на которой различия могут быть легко измерены.
- Представляют собой шкалу оценок, удобную для практического сравнения.
- Помогают определить текущее и желаемое состояния.
- Помогают провести анализ недостатков в целях определения того, что необходимо сделать для достижения выбранного уровня.
- Взятые вместе, они создают общее представление о том, как должно быть организовано корпоративное управление ИТ.

Модели зрелости COBIT сконцентрированы на вопросах зрелости, но не охвата или глубины мер контроля. Уровни зрелости — не просто цифры, за которыми надо гнаться и не формальная основа для сертификации определенных труднодостижимых уровней. Напротив, модели зрелости разрабатывались для постоянного применения, а их уровни просто дают представление о том, в правильном ли направлении движется организация. Правильный в конкретном случае уровень определяется типом организации, средой, в которой она работает и стратегией.

Охват, глубина и применение мер контроля представляются решениями, основанными на анализе преимуществ и затрат. Например, высокий уровень обеспечения безопасности, вероятно, необходимо поддерживать только в отношении наиболее критичных ИТ систем

организации. Другим примером может быть выбор между двумя мерами контроля — еженедельным ручным и постоянным автоматизированным.

Наконец, хотя на более высоких уровнях зрелости и возрастает степень управляемости процессами, организации все равно необходимо анализировать, какие механизмы контроля следует применять, основываясь на анализе рисков и результативных факторов. В таком анализе помогут общие бизнес и ИТ цели, формулированные в данной методологии. Механизмы контроля рекомендуются в COBIT исходя из целей контроля и сконцентрированы на том, что, собственно выполняется в рамках процесса. Модели зрелости, в свою очередь, сконцентрированы на том, насколько качественно осуществляется управление процессом. В Приложении I приводится общая модель зрелости, характеризующая среду внутреннего контроля и реализацию мер внутреннего контроля в организации.

Правильная среда контроля возникает, когда все три аспекта зрелости (управляемость, охват и контроль) приведены в соответствие. Повышение уровня зрелости ведет к минимизации рисков и росту эффективности, сокращению числа ошибок, большей предсказуемости процессов и рациональному (с точки зрения затрат) использованию ресурсов.

Оценка эффективности

Цели и показатели эффективности (метрики) определяются в COBIT на трех уровнях:

• Цели и показатели эффективности ИТ, которые определяют, что является вкладом ИТ в достижение бизнес целей и как это измерить.

• Цели и показатели эффективности ИТ процесса, которые определяют, что является вкладом ИТ процесса в достижение ИТ целей и как это измерить.

• Цели и показатель эффективности отдельных видов деятельности (действий), которые определяют, что должно произойти внутри ИТ процесса для достижения требуемой эффективности и как это измерить.

Осведомлённость и информирование	**Политики, планы и процедуры**	**Инструментарий и автоматизация**	**Навыки и компетентность**	**Ответственность и подотчётность**	**Постановка целей и оценка результатов**
1. Осознание необходимости в процессе. Эпизодический обмен информацией о проблемах.	Процессы и практика реагируют на сиюминутные запросы. Процессы и политики не определены.	Есть некоторые инструментальные средства по управлению процессом, которые применяются на настольных компьютерах. Нет плана применения инструментальных средств.	Навыки персонала, необходимые для выполнения процессов, не определены. Нет плана по обучению, формализованное обучение не проводится.	Ответственность и подотчетность не определены. Ответственность берется на себя отдельными людьми по личной инициативе или в силу обстоятельств.	Цели не ясны, оценка результатов не проводится.
2. Осознание необходимости действовать. Руководство обменивается информацией в отношении общих проблем.	Возникают одинаковые и похожие процессы, но управление интуитивно и основано на опыте отдельных людей. Некоторые аспекты процессов повторяемы, могут существовать документация и неформальное понимание политик и процедур.	Общий подход к применению инструментальных средств, основанных на решениях отдельных лиц. Инструментальные средства могут закупаться у внешних поставщиков, однако они, скорее, не используются или используются не правильно.	Определены минимальные требования по навыкам персонала для наиболее критичных процессов. Обучение проводится по мере необходимости, а не на основе согласованного плана, есть неформализованное обучение.	Сотрудник принимает на себя ответственность, и ведет отчетность, даже если это формально не определено. В случае проблемы возникает замешательство, есть тенденция перекладывать ответственность на других.	Определены некоторые цели, происходит оценка по некоторым финансовым показателям, известным только высшему руководству. В отдельных сферах иногда проводится мониторинг.
3. Понимание необходимости действовать. Более формализованное и структурированное информирование.	Внедряются лучшие практики. Определены процессы, политики и процедуры; документированы основные действия.	Есть план применения и стандартизации средств автоматизации процесса. Средства автоматизации управления процессами применяются в	Требования по навыкам определены и документированы для всех областей. Разработан формализованный план обучения, хотя сам	Ответственность и подотчетность определены, назначены владельцы процессов. У владельцев процессов не всегда	Приняты некоторые цели и показатели эффективности, но они не донесены до всех заинтересованных сторон и не четко связаны с бизнес
		соответствии с их основным предназначением, но, вероятно, не по плану или не интегрированы друг с другом.	процесс обучения все еще основан на индивидуальной инициативе.	достаточно полномочий для полного исполнения своих обязанностей.	целями. Проводится (хотя и нерегулярно) оценка эффективности процессов. Приняты принципы системы сбалансированных показателей ИТ, которые интуитивно применяются при анализе первопричин.
4. Полное понимание всех требований. Задействованы зрелые методы и стандартные инструменты информирования.	Процесс доведён до конца; применяются внутренние лучшие практики. Все аспекты процесса документированы и повторяемы. Политики согласованы и приняты руководством. Стандарты разработки и поддержки процессов приняты и внедрены.	Инструментальные средства применяются в соответствии со стандартизированным планом, некоторые инструменты интегрированы друг с другом. Инструментальные средства применяются для автоматизации управления процессом, мониторинга критических действий и мер контроля.	Требования по навыкам постоянно обновляются для всех областей. Для критических областей обеспечена высокая квалификация, приветствуются сертификация. В соответствии с планом внедряются зрелые методики обучения, приветствуется обмен знаниями. К обучению привлечены внутренние специалисты; оценивается эффективность плана обучения.	Ответственность и подотчётность в рамках процессов определены, владельцы процессов полностью справляются с обязанностями. Для позитивной мотивации применяются вознаграждения.	Результативность и эффективность оцениваются, доносятся до исполнителей и увязаны с корпоративной и ИТ стратегиями. В некоторых сферах внедрена система сбалансированных показателей (с рядом известных руководству исключений), стандартизирован анализ первопричин. Возникает постоянное совершенствование.

5. Развитое и ориентированное на перспективу понимание требований. Проактивное	Внедрены стандарты и внешние лучшие практики. Документооборот развит до уровня	Стандартизированные комплексы инструментальных средств применяются по всей организации. Для	Организация поддерживает постоянное совершенствование навыков персонала,	Владельцы процессов полностью уполномочены принимать решения	В результате всеохватного применения системы сбалансированных показателей система

информирование, основанное на анализе тенденций, зрелых методах и применении стандартизированных инструментальных средств информирования. автоматизированного процесса. Процессы,	политики и процедуры стандартизированы, интегрированы и обеспечивают полную управляемость. полного контроля процессов есть полная интеграция связанных друг с	другом инструментов. Инструменты применяются для совершенствования процессов и автоматического нахождения отклонений от нормы. основанное на чётко определённых личных	и бизнес целях. В обучении применяются внешние лучшие практики, концепции и методы. Обмен опытом стал частью корпоративной культуры, внедрены системы, основанные на знании. Для	консультаций привлекаются лидеры отрасли и внешние эксперты. и выполнять действия. Ответственность последовательно делегируется внутри организации.	оценки эффективности ИТ связана с целями бизнеса. Применяется анализ первопричин, возможные исключения повсеместно учтены менеджментом. Практикуется постоянное совершенствование.

Схема 15. Таблица атрибутов зрелости

Иерархия целей выстроена сверху вниз так, что бизнес цель определяет некоторое количество поддерживающих её ИТ целей. ИТ цель достигает результатов в ходе выполнения одного или взаимодействия нескольких процессов. Таким образом, ИТ цели помогают определить различные цели процессов. В свою очередь, каждая цель процесса требует назначения ряда целей конкретных действий. На **схеме 16** показан пример взаимодействия между целями бизнеса, ИТ, процессов и действий.

Схема 16. Пример взаимодействия целей На смену понятиям «ключевой показатель достижения цели» (KGI) и «ключевой показатель эффективности •> (KPI), применявшиеся в предыдущих изданиях COBIT, пришли два других показателя:

• Показатели результативности, прежде «ключевые показатели достижения цели» (KGI), говорят о том, достигнуты ли определенные цели. Эти показатели могут быть измерены только после совершения факта и, поэтому, называются «индикаторами задержки».

• Показатели эффективности, прежде «ключевые показатели эффективности» (KPI), говорят о том, вероятно ли вообще достижение цели. Эти показатели могут быть измерены до получения результата и, поэтому, называются «индикаторами опережения».

На **схеме 17** показаны возможные цели или показатели результативности для приведенного выше примера.

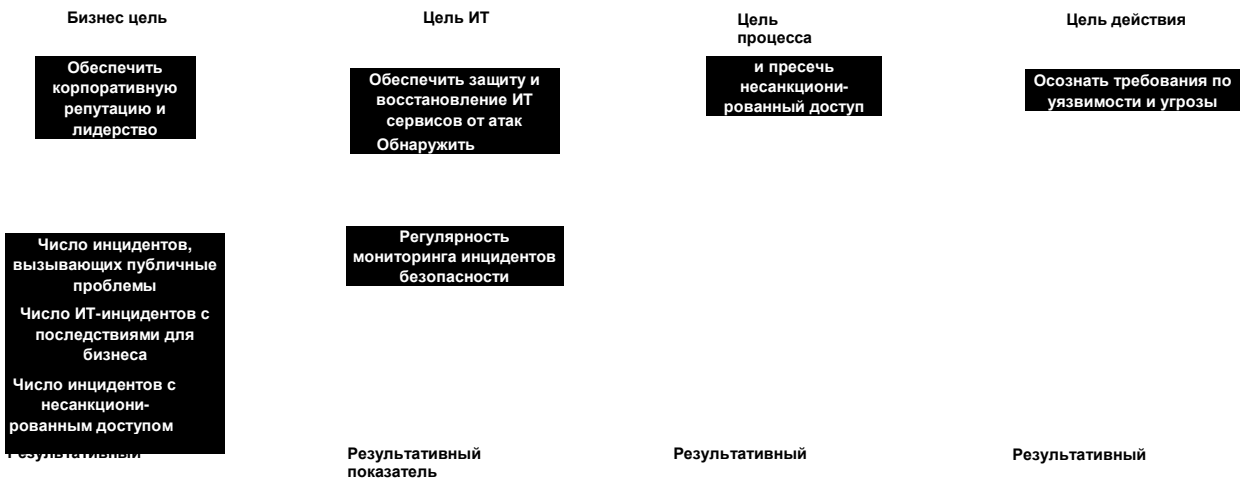


Схема 17. Возможные показатели результативности для примера из схемы 16 Показатели результативности низшего уровня становятся показателями эффективности на более высоком уровне. Что касается примера из **схемы 16,** показатель результативности, говорящий о том, что целью является обнаружение и пресечение несанкционированного доступа, также показывает, что достижение этой цели вероятно обеспечит защиту и восстановление ИТ сервисов от атак. Таким образом, показатель результативности становится показателем эффективности для цели более высокого уровня. На **схеме 18** показано, как показатели результативности становятся показателями эффективности на приведенном выше примере.

Определение показателей результативности информирует руководство (уже постфактум) достигла ли своих целей ИТ функция, процесс или действие. Показатели результативности ИТ функций обычно выражены в терминах информационных критериев:

- Доступность информации, необходимой для бизнес целей.
- Отсутствие рисков, связанных с целостностью и конфиденциальностью.
- Эффективность затрат для процессов и операций.
- Подтверждение надежности, эффективности и соответствия требованиям.

Показатели эффективности определяют, насколько хорошо работают бизнес, служба ИТ и ИТ процессы нал достижением поставленных целей. Они являются индикаторами опережения, показывают, насколько вероятно будут достигнуты цели более высокого уровня. Зачастую они характеризуют наличие необходимых возможностей, практик, навыков и результаты предшествующей деятельности. Например, услуга, которую оказывает ИТ, является как целью для службы ИТ, так и показателем эффективности для бизнеса. Вот почему показатели эффективности иногда называют факторами достижения эффективности, особенно в системе сбалансированных показателей.

Схема 18. Возможные факторы достижения эффективности для примера из схемы 16 Таким образом, предлагаемые показатели одновременно являются показателями результативности, которые характеризуют цель ИТ функции, ИТ процесса или действия и показателями эффективности для бизнес гелей более высокого уровня, ИТ функции, ИТ процесса.

На **схеме 19** показано взаимодействие между целями бизнеса, ИТ процессов и действий, а также различными показателями. Иерархия целей выстроена в верхнем ряду, слева направо. Под каждой целью приведен показатель результативности. Малые стрелки показывают, что показатели результативности являются показателями эффективности для целей более высокого уровня.

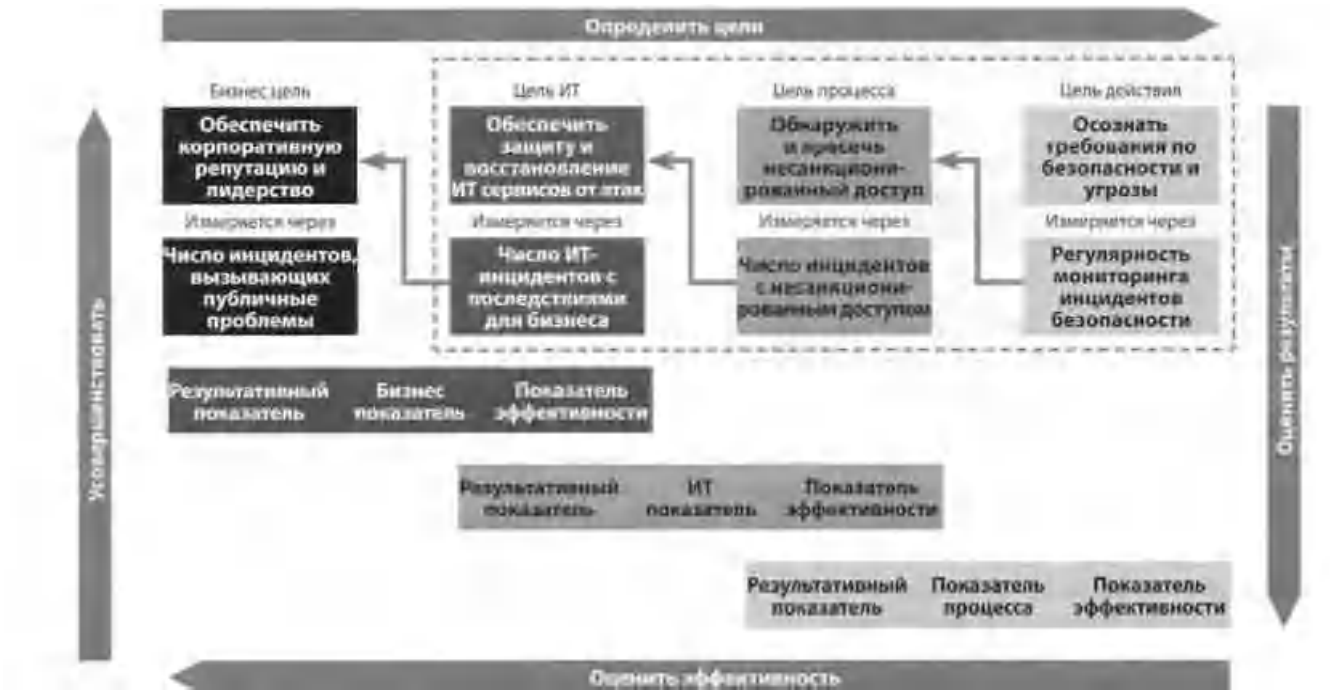


Схема 19. Взаимосвязи между процессами, целями и показателями (DS 5) Данный пример приведен из процесса DS5 «Обеспечение безопасности систем». В COBIT содержатся показатели только для целей ИТ (на **схеме 19** они обозначены пунктиром). Несмотря на то, что они являются также показателями эффективности бизнес целей для ИТ, в COBIT не приводятся показатели эффективности бизнес целей.

Для каждого процесса в COBIT даются цели и показатели, как показано в **схеме 20.**

Показатели разработаны с учетом следующих характеристик:

• Высокая степень проникновения в суть деятельности (уровень детализации показателей не должен превышать уровень усилий по сбору данных).

• Внутренняя сопоставимость (например, процент от общего или количество за период времени).

• Внешняя сравнимость вне зависимости от размера организации или отрасли.

• Лучше, когда есть немного хороших показателей (вероятно, даже один очень значимый, на который осуществляется разнообразное влияние), чем большой набор показателей низкого качества.

• Простота оценки, однако, не путать с целями.

Модель методологии COBIT

Методология COBIT, таким образом, увязывает бизнес требования к информации и управлению с целями сервисной ИТ службы. Модель процессов COBIT позволяет эффективно управлять и контролировать деятельность и ресурсы в сфере ИТ на основе целей контроля. Кроме того, модель процессов позволяет приводить их в соответствие и осуществлять мониторинг, применяя цели и показатели COBIT, как показано на **схеме 21.**

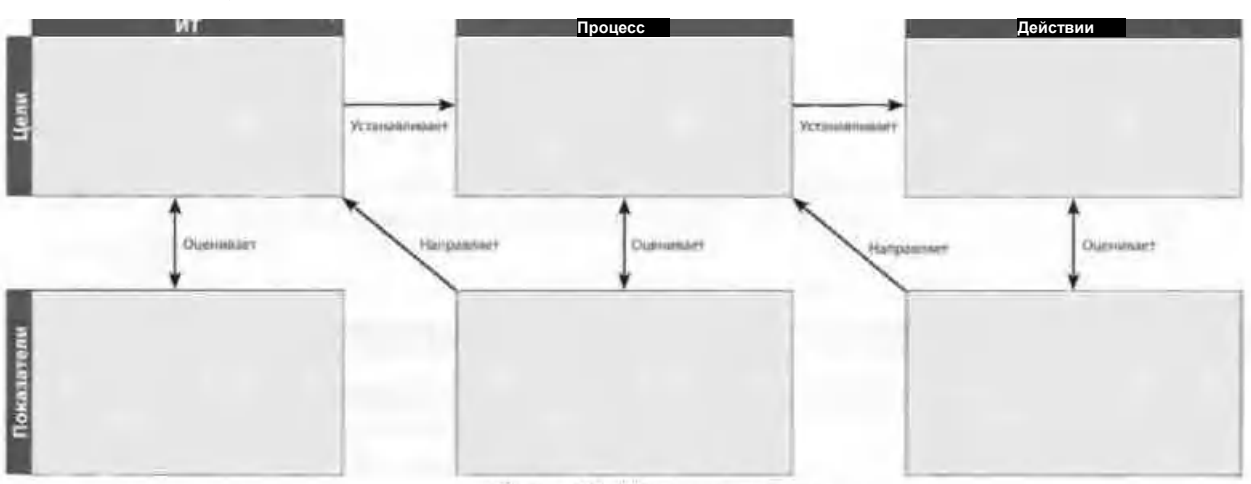


Схема 20. Цели и показатели

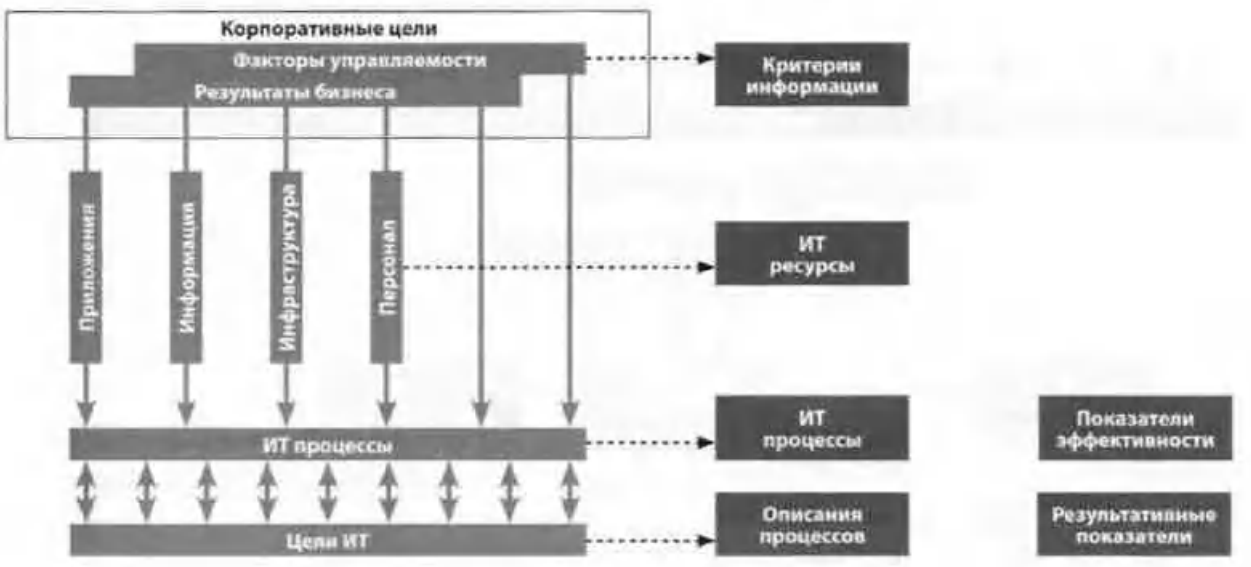


Схема 21. Управление, контроль, соответствие и мониторинг в COBIT

Таким образом, ресурсы ИТ управляются посредством ИТ процессов для достижения целей ИТ, которые, в свою очередь, соответствуют бизнес целям. В этом заключается основной принцип методологии COBIT, как показано на кубе COBIT **(схема 22).**

Схема 22. Куб COBIT

Более детально методология COBIT графически представлена на **схеме 23.** На схеме показана модель процессов, которая включает в себя четыре домена и 34 процесса, управляющих ИТ ресурсами для информационного обеспечения бизнеса в соответствии с бизнес требованиями.

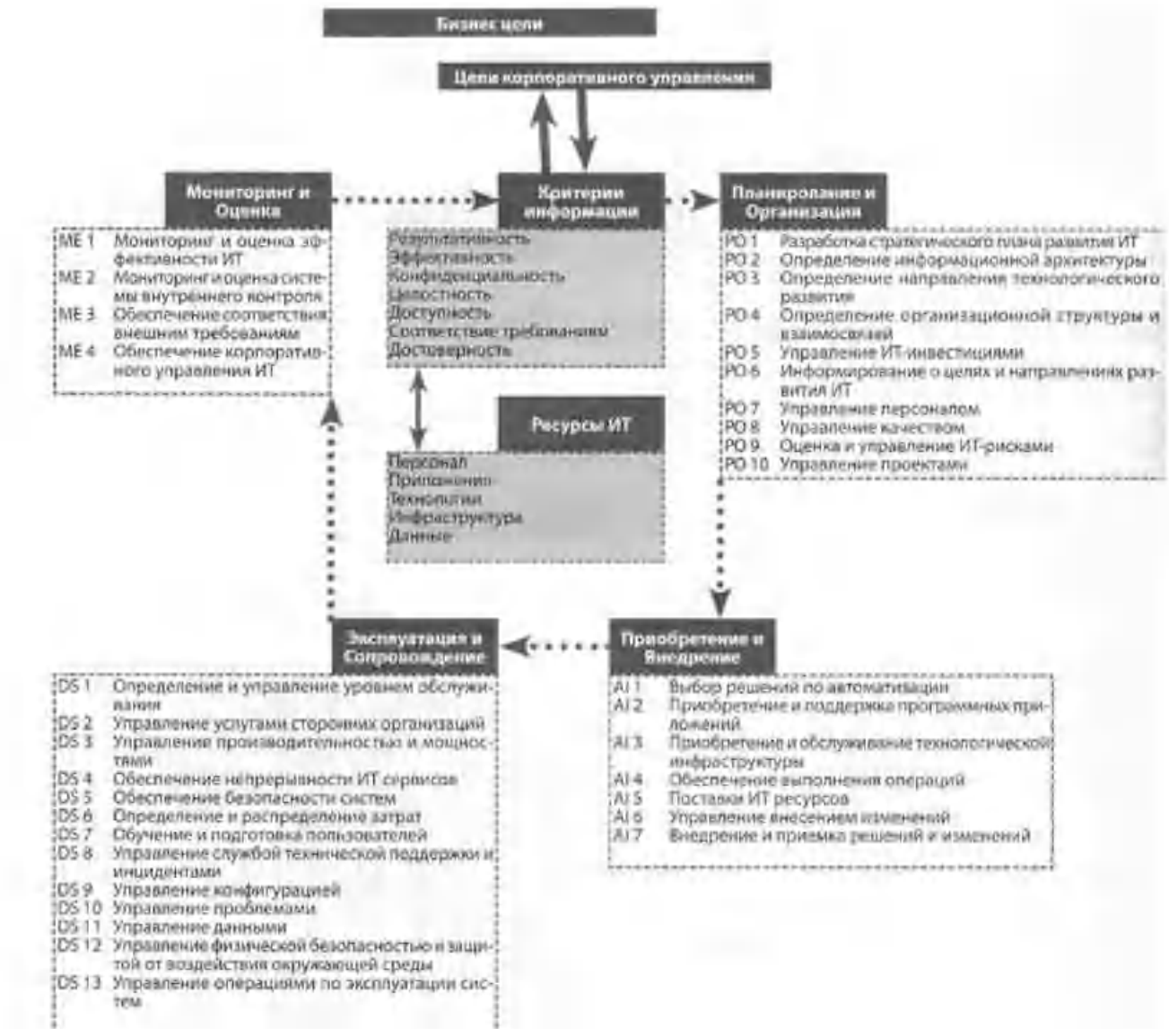


Схема 23. Общая методология COBIT **Общая**

допустимость COBIT

COBIT основан на анализе и гармонизации существующих стандартов в сфере ИТ и лучших практик и соответствует общепринятым принципам управления. COBIT позиционируется как методология высокого уровня, отвечающая бизнес требованиям, охватывающая весь спектр видов деятельности в сфере ИТ и сконцентрированная в большей степени на том, что должно быть достигнуто, нежели как достичь эффективного управления и контроля. Поэтому COBIT выступает как интегратор управленческих практик в ИТ и обращен к высшему руководству, корпоративному и ИТ менеджменту, специалистам в области обеспечения безопасности, контроля и аудита в сфере ИТ. Данная методология разработана для дополнения и совместного применения с другими стандартами и лучшими практиками.

Внедрение лучших практик должно сочетаться с методологией корпоративного управления и контроля, наиболее подходящей для организации и интегрированной с другими применяемыми методами и нормами. Стандарты и лучшие практики не являются панацеей. Их эффективность зависит от того, как они внедрены и актуализированы. Наибольшую пользу они принесут в том случае, когда применяются в комплексе и как отправная точка для совершенствования конкретных процедур. Чтобы рекомендации не отправлялись на полку, а применялись на практике, руководство и персонал должны знать, что нужно делать, как это делать и почему это важно.

Чтобы добиться соответствия лучших практик и требований бизнеса, рекомендуется, чтобы COBIT был внедрен на самом высоком уровне, обеспечив тем самым всеобъемлющую методологию контроля, основанную на модели ИТ процессов, которая подходит практически для любой организации. Специфические практики и стандарты, охватывающие отдельные участки сферы ИТ, могут быть соотнесены с методологией COBIT, тем самым создавая иерархию справочных материалов и рекомендаций.

COBIT адресован нескольким аудиториям:

- **Высшему руководству.** Для получения отдачи от инвестиций в ИТ, уравновешивания рисков и управления инвестициями в зачастую непредсказуемой сфере ИТ.
- **Бизнес-менеджменту организации.** Для обретения уверенности в надлежащем управлении и контроле над ИТ сервисами, предоставляемыми собственной службой ИТ организации или третьими сторонами.
- **ИТ менеджменту.** Для оказания ИТ услуг, требуемых бизнесом и реализации корпоративной стратегии в контролируемых и управляемых условиях.
- **Аудиторам.** Для обоснования собственных заключений и/или консультирования менеджмента по вопросам внутреннего контроля.

COBIT разработан и поддерживается независимым, некоммерческим исследовательским институтом на основе знаний связанных с ассоциацией членов, отраслевых экспертов, профессионалов в области контроля и безопасности. Содержание методологии основано на продолжающихся исследованиях лучших практик в ИТ и постоянно совершенствуется, являясь объективным и практичным ресурсом для всех типов пользователей.

COBIT ориентирован на цели и масштабы управления ИТ, предлагая детальную методологию контроля, соответствие принципам корпоративного управления и, поэтому, приемлем для Советов директоров, высшего руководства, аудиторов и регуляторов.

На **схеме 24** обобщается соотношение различных элементов методологии COBIT и основных разделов (доменов) управления ИТ.

	Цели	Показатели	Практики	Модели зрелости
Соответствие стратегии	П	П		
Результативность		П	В	П
Управление рисками		В	П	В
Управление ресурсами		в	П	П
Оценка эффективности	П	п		В

Схема 24. Методология COBIT и основные разделы управления ИТ П — Приоритетное; В — Второстепенное

Как пользоваться этой книгой

Ориентация внутри COBIT

Для каждого из ИТ процессов COBIT дает описание, вместе с основными целями и показателями **(схема 25).**

Схема 25. Ориентация внутри COBIT Обзор

основных компонентов COBIT

Методология COBIT включает в себя следующие основные компоненты, организованные по 34 ИТ процессам и предлагающие полную картину того, как осуществляется контроль, управление и оценка результатов для каждого процесса. Описание каждого процесса состоит из четырех частей, каждая из которых занимает примерно страницу. Эти части таковы:

• Часть 1 **(схема 25)** — это описание процесса, с кратким изложением его целей в форме «водопада». В этой части также раскрывается связь между процессом, информационными критериями, ресурсами ИТ и разделами (доменами) управления. При этом для лучшего понимания взаимосвязей приоритеты обозначены буквой «П», второстепенные аспекты — буквой «В».

• Часть 2 включает в себя цели контроля для данного процесса.

• Часть 3 включает входящую информацию и результаты процесса, таблицу ОУКИ (RACI), цели и показатели.

• Часть 4 содержит модель зрелости для данного процесса.

На эффективность процесса можно посмотреть и с другой стороны:

- Входящая информация — это то, что владельцу процесса требуется от других.
- Описание целей контроля процесса — это то, что владельцу процесса нужно сделать самому.
- Результаты процесса — это то, что владелец процесса должен в итоге передать другим.
- Цели и показатели показывают, как процесс должен быть оценен / измерен.
- Таблица ОУКИ определяет, что именно и кому делегируется.
- Модель зрелости показывает, что нужно сделать для усовершенствования. В таблице ОУКИ охарактеризована ответственность следующих лиц:

- Генеральный директор, президент
- Финансовый директор
- Высшее руководство
- Директор по ИТ
- Владелец бизнес процесса
- Руководитель службы эксплуатации систем
- Главный архитектор ИТ систем
- Руководитель разработок
- Руководитель службы административной поддержки (для крупных организаций — руководители таких подразделений как служба кадров, бюджетирование или внутренний контроль)
- Руководитель проектного офиса
- Ответственные за соответствие требованиям, аудит, управление рисками и безопасность (имеют обязанности по контролю, но не являются персоналом ИТ).

Некоторые специфические процессы могут иметь включать дополнительных лиц, например, менеджер службы технической поддержки /разрешению инцидентов, как в процессе DS8.

Следует отметить, что, несмотря на то, что методологический материал собирался в ходе серьезного исследования от сотен экспертов, источники и результаты процессов, а также, цели и показатели служат скорее в иллюстративных целях, не являются исчерпывающими и не носят характер предписаний. Они предлагают некую основу экспертного знания, из которой каждая организация может выбрать то, что эффективно применимо для ее собственной корпоративной стратегии и целей.

Пользователи компонентов COBIT

Менеджмент может использовать COBIT для оценки ИТ процессов, основываясь на целях бизнеса и целях ИТ, которые служат для разъяснения целей ИТ процессов, моделей зрелости и оценки эффективности процессов.

Разработчики и аудиторы могут определить применимые требования из целей контроля и обязанности из описаний действий и связанных с ними таблиц ОУКИ.

Все потенциальные пользователи COBIT могут приобрести выгоду от применения общего подхода к управлению ИТ совместно с более детальными стандартами, такими как:

- «Библиотека ИТ инфраструктуры при Управлении правительственной коммерции Великобритании» (ITIL) для оказания услуг.
- «Модель зрелости интеграции» (Capability Maturity Model® Integration, CMMI) для принятия решений.
- ISO 17799 для информационной безопасности.
- «Свод знаний по управлению проектами» (PMBOK) или «Проекты в контролируемой среде 2» (PRINCE2) для управление проектами.

Приложения

В конце книги находятся следующие приложения:
Приложение I. Модель зрелости для среды внутреннего контроля
Приложение И. Глоссарий терминов

Планирование и организация

PO 1. Разработка стратегического плана развития ИТ

Описание процесса

Стратегическое планирование ИТ необходимо для того, чтобы управление всеми ИТ ресурсами было взаимосвязано с корпоративной стратегией и приоритетами. Служба ИТ 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.

Результативность	П
Эффективность	В
Конфиденциальность	
Целостность	
Доступность	
Соответствие требованиям	
Достоверность	

Управление процессом

Разработка стратегического плана развития ИТ.

удовлетворяет следующим бизнес требованиям к ИТ

поддержка или расширение корпоративной стратегии и требований управления при условии прозрачности в отношении преимуществ, затрат и рисков **сосредоточено на**

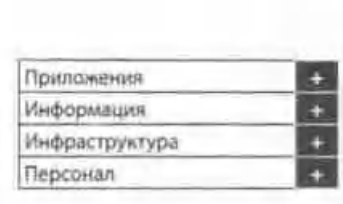
соединении корпоративного и ИТ управления путем преобразования бизнес требований в предложение конкретных услуг и разработке стратегий оказания этих услуг прозрачным и эффективным образом.

достигается с помощью

- Совместной работы с бизнес и высшим руководством по совмещению стратегического планирования ИТ с текущими и будущими потребностями организации.
- Понимания текущих возможностей ИТ.
- Выработки схемы приоритетов бизнес целей, которая охарактеризует количественно бизнес требования.

результаты оцениваются с помощью следующих показателей

- Доля целей ИТ в стратегическом плане ИТ, которые соответствуют стратегическому бизнес плану.
- Доля ИТ проектов в портфеле ИТ проектов, которые отражены в тактических планах ИТ.
- Время задержки между обновлением стратегического плана ИТ и тактических планов ИТ.



Цели контроля

PO 1.1. Управление пользой от ИТ

Необходимо убедиться в том, что корпоративный портфель ИТ инвестиций включает в себя решения, которые обоснованы бизнесом организации. Определить обязательные, поддерживающие и возможные инвестиции, которые отличаются по степени сложности и гибкости распределения средств. ИТ процессы должны обеспечивать эффективную реализацию ИТ компонентов инвестиционных программ и раннее предупреждение о любых отклонениях от выполнения плана, включая изменения по стоимости, графику или функциональности, которые могут повлиять на ожидаемые результаты. ИТ услуги должны предоставляться на основании объективных и имеющих правовой статус соглашений об уровне сервиса. Ответственность по достижению результатов и контролю за затратами должна быть легко предаваемой и проверяемой. Разработать справедливую, прозрачную, повторяемую и сравнимую процедуру бизнес-обоснования, включающую оценку финансовой ценности, а также риска не реализации возможности ожидаемых преимуществ.

PO 1.2. Соответствие между бизнесом и ИТ

Следует установить процессы двустороннего образования и взаимного участия в стратегическом планировании интеграции бизнеса и ИТ. Необходимо образовать связующее звено между бизнесом и ИТ с целью взаимного согласования приоритетов.

PO 1.3. Оценка текущих возможностей и эффективности

Оценить текущие возможности и эффективность решений и услуг для того, чтобы установить отправную очку для сравнения текущей ситуации и будущих требований. Охарактеризовать эффективность в понятиях вклада ИТ в достижение бизнес целей, функциональности, стабильности, сложности, затрат, сильных и слабых сторон.

PO 1.4. Стратегический план ИТ

Разработать стратегический план ИТ, в котором будет определено, при участии всех заинтересованных сторон, как достижение целей ИТ будут способствовать достижению корпоративных целей и каковы связанные с этим затраты и риски. План должен отвечать на вопрос как служба ИТ должна поддерживать связанные с ней инвестиции, услуги и активы. Руководство ИТ должно определить, как планируется достичь поставленных целей, какие методы оценки эффективности должны применяться и какие процедуры должны получить формальное одобрение со стороны всех заинтересованных сторон. Стратегический план ИТ должен включать в себя инвестиционный/операционный бюджет, источники финансирования, стратегию аутсорсинга и закупок, а также нормативные и регуляторные требования. Стратегический план должен быть достаточно детализован, чтобы на его основе могли быть разработаны тактические планы ИТ.

PO 1.5. Тактические планы ИТ

Создать портфель тактических планов ИТ, которые будут вытекать из стратегического плана ИТ. В тактических планах речь должна идти о программе инвестиций, связанных с ИТ,

ИТ услугах и ИТ активах. Тактические планы должны содержать описания необходимых инициатив в области ИТ, требования по ресурсам, а также методы оценки и мониторинга использования ресурсов и достижения преимуществ. Тактические планы должны быть достаточно детализованы, чтобы на их основе могли быть разработаны планы проектов. Необходимо активное управление комплексом тактических планов ИТ и инициатив посредством анализа портфеля проектов и услуг.

РО 1.6. Управление ИТ портфелем

Совместно с руководством организации активно управлять портфелем связанных с ИТ инвестиционных программ, необходимых для достижения стратегических бизнес целей путем определения, оценки, расстановки приоритетов, отбора, инициации разработки, управления и контроля программ. Сюда входят разъяснение ожидаемых результатов бизнеса, проверка того, чтобы цели программ способствовали достижению результатов, понимание масштаба усилий, требуемых для этого, определение ответственности и мер поддержки, выделение проектов внутри программ, распределения ресурсов и бюджета, делегирования полномочий и синхронизации запуска необходимых проектов и программ.

Рекомендации по управлению

Из	Входящая информация
PO 5	Отчеты о затратах и преимуществах
PO 9	Оценка рисков
PO 10	Обновленный портфель ИТ проектов
DS 1	Новые/обновленные требования к услугам, обновленные портфели ИТ услуг
*	Корпоративные стратегии и приоритеты
*	Портфель инвестиционных программ
ME 1	Аспекты эффективности для ИТ планирования
ME 4	Отчет о статусе управления ИТ, корпоративные стратегические указания ИТ

Результаты	В процессы						
Стратегический план ИТ	PO 2, PO 6		PO 6	PO 9	AI 1	DS 1	
Тактические планы ИТ	PO 2	PO 6	PO 9	AI 1	DS 1		
Портфель ИТ проектов	PO 5	PO 6	PO 10	AI 5			
Портфель ИТ услуг	PO 5	PO 6	PO 9	DS 1			
Стратегия аутсорсинга ИТ	DS 2						
Стратегия приобретений в сфере ИТ	AI 5						

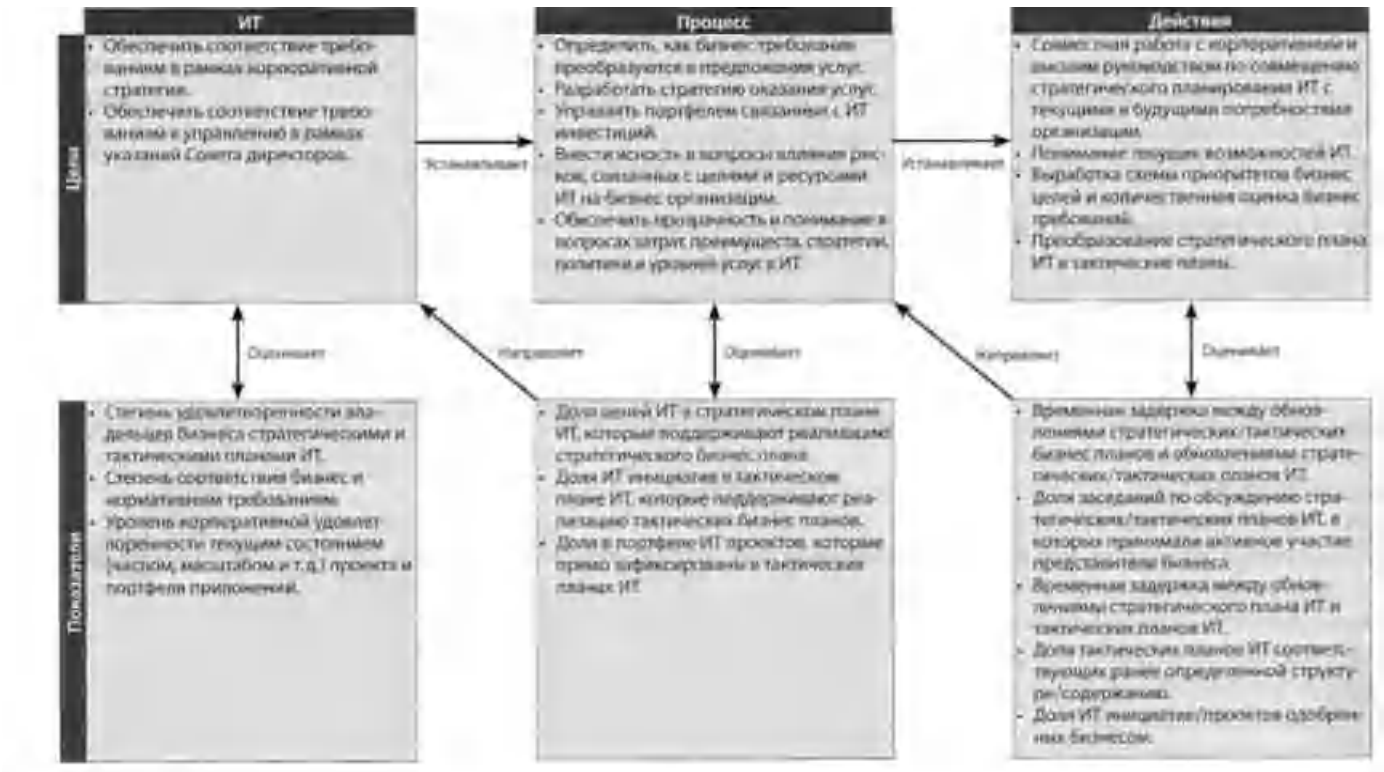
* Источники вне COBIT

Таблица ОУКИ

Действия ↓ Функции →	Президент	Финансовый директор (CFO)	Высшее руководство	Директор по ИТ	Владелец бизнес процесса	Руководитель вычислительной системы	Главный архитектор ИТ системы	Руководитель разработки	Руководитель администрирования ИТ	Руководитель подразделения	Аудит, риски, безопасность
Обеспечить взаимосвязь бизнес целей и целей ИТ	К	И	У/О	О	К						
Определить критические зависимости и текущую эффективность	К	К	О	У/О	К	К	К	К	К		К
Разработать стратегический план ИТ	У	К	К	О	И	К	К	К	К	И	К
Разработать тактические планы ИТ	К	И		У	К	К	К	К	К	О	И
Провести анализ портфеля инвестиционных программ и управлять портфелем проектов и услуг ИТ	К	И	И	У	О	О	К	О	К	К	И

В таблице ОУКИ показано, кто является Ответственным, Утверждающим, Консультирующим и/или Информированным

Цели и показатели



Модель зрелости

Управление процессом *«Разработка стратегического плана развития ИТ»* удовлетворяет следующим бизнес требованиям к ИТ *поддержка или расширение корпоративной стратегии и требований управления при условии прозрачности в отношении преимуществ, затрат и рисков* и соответствует характеристикам:

0. Несуществующий

Стратегическое планирование ИТ не ведется. У руководства нет понимания того, что стратегическое планирование ИТ необходимо для достижения бизнес целей.

1. Начальный/Повторяющийся эпизодически и бессистемно

Потребность в стратегическом планировании ИТ осознана руководством ИТ. Планирование ИТ ведется по мере необходимости в ответ на специфические бизнес требования. Вопросы стратегического планирования ИТ изредка обсуждаются на заседаниях руководства ИТ. Настройка приложений и технологий под потребности бизнеса является реакцией на внешнее воздействие, а не на основании корпоративной стратегии. Оценка стратегического риска не формализована и осуществляется от проекта к проекту.

2. Повторяющийся, но интуитивный

Стратегическое планирование ИТ ведется совместно с бизнес менеджментом по мере необходимости. Обновление ИТ планов происходит по запросам руководства. Стратегические решения принимаются применительно к конкретным проектам без согласования с общей корпоративной стратегией. Риски и выгоды от основных стратегических решений понимаются интуитивно.

3. Определенный

Разработана политика, определяющая когда и как осуществлять стратегическое планирование ИТ. При стратегическом планировании ИТ применяется структурированный подход, который документально оформлен и известен всем сотрудникам. Процесс планирования ИТ разумно обоснован и обеспечивает рациональное планирование. Однако вопрос реализации данного процесса оставлен на усмотрение отдельных руководителей и отсутствуют процедуры его проверки. Общая стратегия развития ИТ включает единообразное определение рисков, которые организация готова принять в качестве новатора или последователя в применении новых технологий. Стратегии развития

финансовых, технических и кадровых ресурсов в области ИТ все больше влияют на закупки новых программных продуктов и технологий. Вопросы стратегического планирования обсуждаются на заседаниях руководства бизнеса.

4. Управляемый и измеряемый

Стратегическое планирование ИТ является стандартной практикой и любые исключения отмечаются руководством. Стратегическое планирование ИТ является четко определенной функцией руководства, при этом ответственность возложена на руководителей высшего звена. Руководство может осуществлять мониторинг процесса стратегического планирования ИТ, принимать взвешенные решения на его основе и измерять (оценивать) его эффективность. Осуществляется разработка как текущих, так и долгосрочных планов, которые при необходимости обновляются. Стратегия развития ИТ и общая корпоративная стратегия становятся все более скоординированными в результате рассмотрения бизнес-процессов, возможных выгод и более эффективного применения приложений и технологий посредством реинжиниринга бизнес-процессов. Имеется хорошо определенный процесс рационального применения внутренних и внешних ресурсов, необходимых для разработки и эксплуатации систем.

5. Оптимизированный

Стратегическое планирование ИТ является документально оформленным, реально осуществляемым процессом, постоянно учитывающим цели бизнеса и приводящим к ощутимой отдаче от инвестиций в ИТ. Вопросы риска и выгод непрерывно корректируются в процессе стратегического планирования ИТ. Разрабатываются и постоянно обновляются долгосрочные реалистичные планы с тем, чтобы отразить изменения в информационных технологиях и новые разработки, связанные с бизнесом. Ведется сравнительный анализ на соответствие понятным проверенным отраслевым нормам; этот анализ интегрирован с процессом формирования стратегии. Стратегический план включает в себя ответ на вопрос о том, как развитие новых технологий может способствовать созданию новых возможностей для развития бизнеса и повышению конкурентоспособности организации.

РО 2. Определение информационной архитектуры

Описание процесса

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.

Управление процессом

Определение информационной архитектуры.

удовлетворяет следующим бизнес требованиям к ИТ

гибкий подход при соответствии требованиям, предоставление достоверной и непротиворечивой информации, а также тесная интеграция приложений и бизнес процессов. **сосредоточено на**

создании корпоративной модели данных которая включает схему классификации данных для обеспечения целостности и непротиворечивости данных.

достигается с помощью

- Обеспечения точности и корректности информационной архитектуры и модели данных.
- Назначения владельцев данных.
- Классификации информации в соответствии с заранее согласованной классификационной схемой.

результаты оцениваются с помощью следующих показателей

- Доля избыточных/дублированных элементов данных.
- Доля приложений не соответствующих методологии построения информационной архитектуры организации.
- Частота операций сверки данных.

Цели контроля

РО 2.1. Модель корпоративной информационной архитектуры

Разработать и поддерживать корпоративную информационную модель для обеспечения разработки приложений и деятельности по поддержке принятия решений, а также соответствия планам развития ИТ, описанным в процессе РО 1. Модель должна способствовать оптимизации создания, применения и совместного использования информации бизнесом, причем в целостной, гибкой, функциональной, эффективной с точки зрения затрат средств и времени, безопасной и устойчивой к ошибкам форме.

РО 2.2. Справочник корпоративных данных и правила представления данных

Следует вести справочник корпоративных данных, включающий в себя правила представления данных. Данный справочник должен способствовать совместному использованию элементов данных приложениями и системами, предлагать общее понимание данных для ИТ и бизнес пользователей, а также предотвращать создание несовместимых элементов данных.

РО 2.3. Схема классификации данных

Разработать схему классификации, которая будет применяться повсеместно в организации, основанную на критичности и значимости корпоративных данных (например, общедоступные, конфиденциальные, строго секретные данные). Данная схема должна включать сведения о владельцах данных; определения уровней безопасности данных и защитных контрольных мер; краткие требования по хранению и уничтожению данных, критичности и значимости. Схема должна использоваться как основа для применения таких мер контроля как контроль доступа, архивация или шифрование.

РО 2.4. Управление целостностью

Определить и внедрить процедуры по обеспечению целостности и совместимости всех данных, хранящихся в электронной форме, таких как базы, хранилища и архивы данных.

Рекомендации по управлению

Из	Входящая информация
PO 1	Стратегические и тактические планы ИТ
AI 1	Анализ осуществимости бизнес требований
AI 7	Обзор результатов внедрения
DS 3	Сведения о производительности и мощности
ME 1	Вклад эффективности в планирование ИТ

Результаты	В процессы						
Схема классификации данных	AI 2						
Оптимизированный план бизнес систем	PO 3	AI 2					
Справочник данных	AI 2	DS 11					
Информационная архитектура	PO 3	DS 5					
Незначимые классификации данных	DS 1	DS 4	DS 5	DS 11	DS 12		
Классификации и инструменты	*						

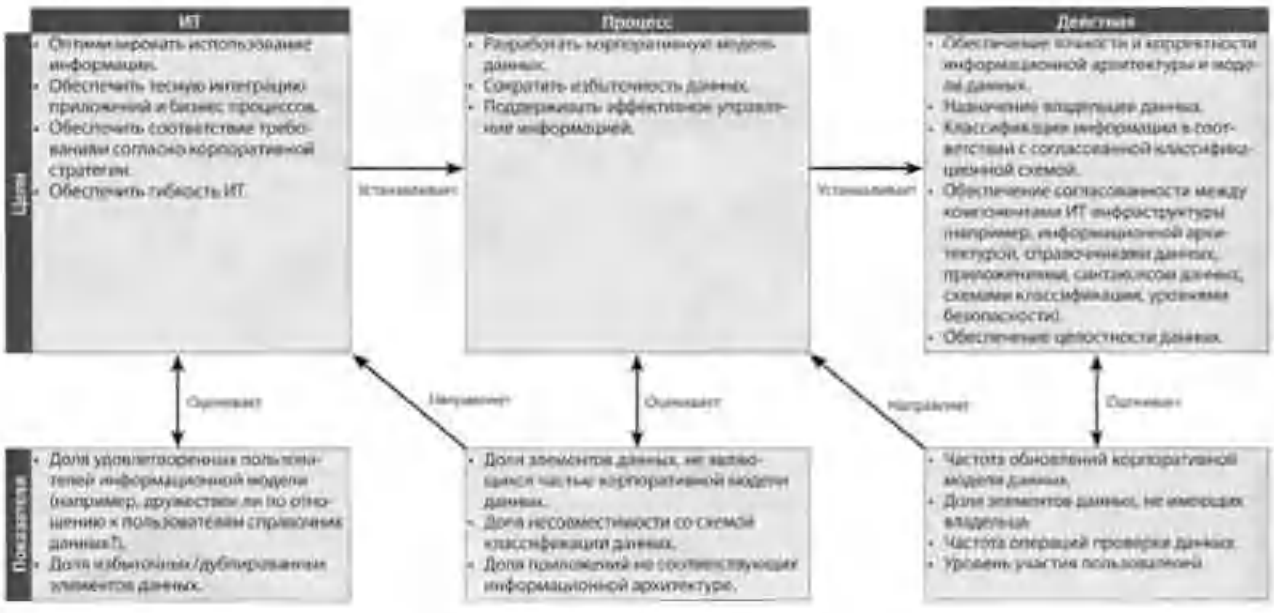
* Завершенные виды COBIT

Таблица ОУКИ

Действия ↓ / Функции →	Президент	Финансовый директор	Высшее руководство	Директор по ИТ	Владелец бизнес процесса	Руководитель эксплуатации систем	Главный архитектор ИТ системы	Руководитель разработок	Руководитель администрации ИТ	Руководитель проектного офиса	Аудит, риски, безопасность
Создать и поддерживать корпоративную информационную модель		К	И	У	К		О	К	К		К
Создать и поддерживать корпоративные справочники данных				И	К		О/У	О			К
Разработать и поддерживать схемы классификации данных	И	К	У	К	К	И	К	К			О
Обеспечить владельцев данных процедурами и инструментами для классификации информационных систем	И	К	У	К	К	И	К	К			О
Применять информационную модель, справочники данных и схемы классификации для оптимизации бизнес систем	К	К	И	У	И		О	К			И

В таблице ОУКИ показано, кто является Ответственным, Утверждающим, Консультирующим и/или Информированным

Цели и показатели



Модель зрелости

Управление процессом *«Определение информационной архитектуры»* удовлетворяет следующим бизнес требованиям к ИТ *гибкий подход при соответствии требованиям, предоставление достоверной и непротиворечивой информации, а также тесная интеграция приложений и бизнес процессов* и соответствует характеристикам:

0. Несуществующий

Не осознается важность информационной архитектуры для данной организации. В организации отсутствуют знания, опыт и ответственность, необходимые для ее разработки.

1. ***Начальный/Повторяющийся эпизодически и бессистемно***

Руководство признает необходимость информационной архитектуры. Разработка компонентов информационной архитектуры осуществляется от случая к случаю. Определения относятся скорее к данным, чем к информации и обусловлены предложениями поставщиков приложений. Информирование заинтересованных сторон о необходимости информационной архитектуры проводится непоследовательно и бессистемно.

2. ***Повторяющийся, но интуитивный***

Развивается процесс формирования информационной архитектуры. Некоторыми сотрудниками соблюдаются, хотя и неформальные и интуитивные, процедуры. Персонал приобретает навыки в результате практического опыта и многократного применения методов и приемов. Разработка компонентов информационной архитектуры осуществляется отдельными сотрудниками на основе тактических требований.

3. ***Определенный***

Важность информационной архитектуры осознана и признана, назначены ответственные за ее реализацию и об этом информированы заинтересованные стороны. Соответствующие процедуры, инструментальные средства и методы, пусть и несложные, стандартизированы, документально оформлены и являются частью процесса неформального обучения. Разработаны базовая политика в отношении информационной архитектуры, включая некоторые стратегические требования, однако соблюдение политик и стандартов реализуется непоследовательно. Учреждена формально определенная функция (группа) администрирования данных, устанавливающая внутрикорпоративные стандарты и начинающая информировать руководство о внедрении и использовании информационной архитектуры. Начинают применяться автоматизированные инструментальные средства управления данными, однако процессы и правила их использования определяются предложениями поставщиков программных средств базы данных. Разработан формализованный план обучения, но передача опыта все еще основана на индивидуальной инициативе.

4. ***Управляемый и измеряемый***

Разработка и реализация информационной архитектуры полностью поддерживается формализованными приёмами и методами. Введена отчетность в отношении эффективности разработки данной архитектуры, проводится измерение степени ее реализации. Широко используются вспомогательные автоматизированные инструментальные средства, но они еще не интегрированы. Выявлены основные показатели и организована система их оценки. Процесс определения информационной архитектуры является упреждающим и сосредоточен на рассмотрении перспективных потребностей бизнеса. Группа администрирования данных активно участвует во всех разработках приложений с целью обеспечения совместимости. Полностью реализован автоматизированное хранилище данных (репозитарий), внедряются более сложные модели данных с целью более эффективного использования информационного содержания баз данных. Информационные системы и системы поддержки принятия решений для руководства эффективно используют имеющуюся информацию.

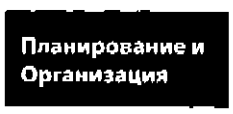
5. ***Оптимизированный***

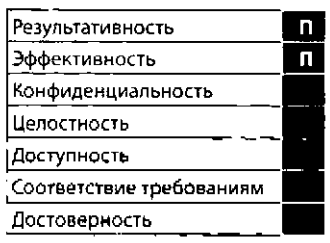
Информационная архитектура единообразно реализована на всех уровнях. Постоянно подчеркивается ее важность для бизнеса организации. Персонал ИТ обладает опытом и навыками разработки и поддержания устойчивой и восприимчивой информационной архитектуры, отвечающей всем бизнес требованиям. Информация, предоставляемая данной архитектурой, широко и единообразно применяется. Повсеместно при разработке и поддержании информационной архитектуры используются лучшие отраслевые практики, включая процесс непрерывного совершенствования. Определена стратегия эффективного использования информации с использованием хранилищ данных, баз данных и методов и извлечения информации. Информационная архитектура непрерывно совершенствуется и учитывается нетрадиционная информация о процессах, организациях и системах.

РО 3. Определение направления технологического развития

Описание процесса

Служба ИТ 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.





Управление процессом

Определение направления технологического развития.

удовлетворяет следующим бизнес требованиям к ИТ

наличие стабильных, эффективных с точки зрения затрат, интегрированных и стандартизованных систем приложений, ресурсов и возможностей, отвечающих текущим и будущим бизнес требованиям. **сосредоточено на**

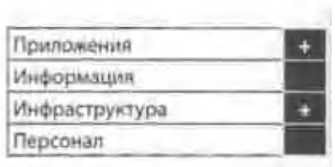
определении и реализации плана развития технологической инфраструктуры, архитектуры и стандартов, которые учитывают и задействуют возможности технологий.

достигается с помощью

- Создания комитета для обсуждения путей развития архитектуры и проверки соответствия требованиям.
- Создания плана технологической инфраструктуры, сбалансированного с точки зрения затрат, рисков и требований.
- Определения стандартов в области технологической инфраструктуры, основанных на требованиях информационной архитектуры.

результаты оцениваются с помощью следующих показателей

- Количество и типы отклонений от плана развития технологической инфраструктуры.
- Частота пересмотра/обновления плана развития технологической инфраструктуры.
- Количество различных технологических платформ в организации.



Цели контроля

РО 3.1. Планирование технологическогоразвития

Следует проводить анализ существующих и возникающих технологий и планировать, какое направление технологического развития будет адекватно реализовывать ИТ стратегию и архитектуру бизнес систем. Также следует определить в плане, какие технологии имеют потенциал для создания новых бизнес возможностей. Кроме того, план должен включать такие аспекты инфраструктуры, как архитектура систем, технологическое направление, стратегии миграции и непрерывность.

РО 3.2. План технологической инфраструктуры

Разработать и поддерживать план технологической инфраструктуры в соответствии со стратегическим и тактическими планами ИТ. План должен основываться на выбранном направлении технологического развития и включать аспекты непрерывности и рекомендации по приобретению технологических ресурсов. В нём должны быть учтены изменения в конкурентной среде, а также аспекты экономии на масштабах инвестиций и затратах на персонал для поддержки информационных систем и улучшение взаимодействия платформ и приложений.

PO 3.3. Текущий анализ перспективных направлений и нормативных требований

Следует осуществлять мониторинг рынка, отрасли, технологий, инфраструктуры, тенденций в области нормативного регулирования. Использовать анализ последствий этих тенденций при разработке плана технологической инфраструктуры.

PO 3.4. Технологическиестандарты

Чтобы обеспечить совместимые, эффективные и безопасные технологические решения в масштабах организации, нужно создать технологический форум для обмена опытом по применению технологий, консультирования по инфраструктурным решениям, имеющимся на рынке, руководства по выбору технологий, оценки совместимости со стандартами. Данный форум должен направлять развитие технологических стандартов и практик, основанных на соответствии требованиям бизнеса, с учетом рисков, а также внешних требований.

PO 3.5. Коллегия по вопросам ИТархитектуры

Следует учредить комитет по вопросам ИТ архитектуры для руководства, консультирования и оценки соответствия требованиям. Комитет должен направлять развитие ИТ архитектуры, при условии соответствия корпоративной стратегии и нормативным требованиям. Эти вопросы связаны также с процессом PO 2 «Определение информационной архитектуры».

Рекомендации по управлению

Из	Входящая информация
PO 1	Стратегический и тактические планы ИТ
PO 2	Оптимизированный план бизнес систем, информационная архитектура
AI 1	Обновления технологических стандартов
DS 1	Сведения о производительности и мощности

Результаты	В процессах						
Технологические возможности	AI 3						
Технологические стандарты	AI 1	AI 3	AI 7	DS 5			
Регулярное обновление современного состояния технологий	AI 1	AI 2	AI 3				
Планы технологической инфраструктуры	AI 3						
Инфраструктурные требования	PO 3						

Таблица ОУКИ

Действия ↓ Функция →	Президент	Финансовый директор	Высшее руководство	Директор по ИТ	Владелец бизнес процесса	Руководитель эксплуатации системы	Главный архитектор ИТ системы	Руководитель разработки	Руководитель администрации ИТ	Руководитель проектного офиса	Аудит, риски, безопасность
Разработать и поддерживать планы технологической инфраструктуры		И	И	У		К	О	К	К		К
Разработать и поддерживать технологические стандарты				У		К	О	К	И	И	К
Публиковать технологических стандартов		И	И	У		И	О	И	И	И	И
Осуществлять мониторинг технологического развития		И	И	У		К	О	К		К	К
Определять будущее стратегическое применение новой технологии ИТ		К	К	У		К	О	К		К	К

В таблице ОУКИ показано, кто является Ответственным, Утверждающим, Консультирующим и/или Информированным

Цели и показатели

Модель зрелости

Управление процессом *«Определение направления технологического развития»* удовлетворяет следующим бизнес требованиям к ИТ *наличие стабильных, эффективных с точки зрения затрат, интегрированных и стандартизованных систем приложений, ресурсов и возможностей, отвечающих текущим и будущим бизнес требованиям* и соответствует характеристикам:

0. Несуществующий

Руководством организации не осознается важность планирования технологической инфраструктуры. Знания и опыт необходимые для разработки такого плана, отсутствуют. Нет понимания того, что планирование изменений в технологиях является критически важным для эффективного распределения ресурсов.

1. Начальный/Повторяющийся эпизодически и бессистемно

Руководство признает необходимость планирования развития технологической инфраструктуры. Разработки компонентов технологии и внедрение новых технологий проводятся бессистемно, от случая к случаю. Выбранный подход к планированию ориентирован на решение оперативных задач и возникающих внешних факторов. Выбор технологических направлений часто осуществляется на основе противоречивых перспективных планов разработки новых продуктов, предлагаемых поставщиками

оборудования, системного программного обеспечения и приложений. Информирование заинтересованных сторон о потенциальном влиянии изменений в технологиях проводится бессистемно.

2. Повторяющийся, но интуитивный

Заинтересованные стороны информируются о необходимости и важности технологического планирования. Имеет место тактическое планирование, ориентированное в большей степени на разработку решений, связанных с техническими проблемами, чем на использование технологии для удовлетворения потребностей бизнеса. Оценка технологических изменений оставлена на усмотрение сотрудников, которые интуитивно следуют однотипным процессам. Персонал приобретает навыки в результате практического опыта и многократного применения методов и приемов. Начинают применяться типовые приемы и стандарты для разработки компонентов инфраструктуры.

3. Определенный

Руководство понимает важность разработки плана развития технологической инфраструктуры. Процесс его разработки достаточно качественный и соответствует стратегическому плану развития ИТ. Имеется определённый и документально оформленный план развития технологической инфраструктуры, о котором информированы заинтересованные стороны, однако реализация его проводится непоследовательно. Выбранное направление развития технологии включает понимание того, в каких областях организация планирует быть лидером в использовании технологии с учетом рисков и стратегии своего развития. Основные поставщики выбираются, исходя из того, чтобы их долгосрочные планы разработки новых технологий и продуктов были совместимы с направлением технологического развития организации. Существует формализованная программа обучения, персонал информирован о функциях и обязанностях.

4. Управляемый и измеряемый

Руководство обеспечивает разработку плана развития технологической инфраструктуры. ИТ персонал обладает опытом и навыками необходимыми для разработки плана развития технологической инфраструктуры. Учитывается и оценивается потенциальное влияние изменений в существующей технологии и появления новых технологий. Руководство может выявлять отклонения от выполнения данного плана упреждать возникающие проблемы. Назначены ответственные лица за разработку и поддержание плана развития технологической инфраструктуры. Процесс разработки плана является комплексным и учитывает изменения условий. При разработке плана используется накопленные собственные лучшие практики. Стратегия использования кадровых ресурсов разработана в соответствии с выбранным технологическим направлением — благодаря этому ИТ персонал может эффективно управлять изменениями в технологиях. Определены планы внедрения новых технологий. Методы привлечения сторонних организаций и кооперации эффективно используются для получения доступа к необходимым специальным знаниям и навыкам. Руководство проводит оценку рисков, связанных с передовым (или отстающим) применением технологии при разработке новых возможностей для бизнеса или операционной эффективности.

5. Оптимизированный

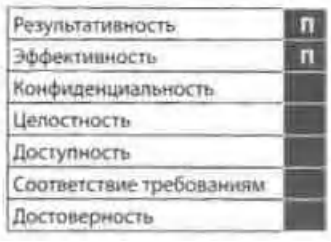
Создан исследовательский отдел для анализа новых и перспективных технологий и сравнительной оценки собственной организации на соответствие отраслевым нормам. План технологической инфраструктуры предлагает выбор направления развития с учетом отраслевых и международных стандартов и разработок, а не на основе предложений поставщиков технологий. Потенциальные последствия изменений в технологии рассматриваются на уровне высшего руководства организации. Новые и скорректированные технологические направления официально утверждаются руководством организации. Разработан устойчивый план развития технологической инфраструктуры, который отвечает требованиям бизнеса и может быть скорректирован для учета изменений в бизнес среде.

Осуществляется непрерывный и регламентированный процесс совершенствования плана. При выборе направлений развития широко применяются лучшие отраслевые практики.

РО 4. Определение ИТ процессов, организационной структуры и взаимосвязей

Описание процесса

Организационная структура ИТ определяется требованиями по кадрам, навыкам, функциям, отчетности, руководству, должностям и обязанностям, надзору. Эта структура включена в методологию ИТ процессов и 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 сообразно 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.



Управление процессом

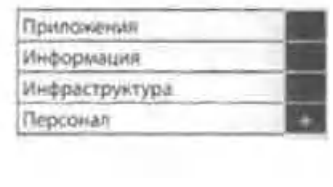
Определение ИТ процессов, организационной структуры и взаимосвязей.

удовлетворяет следующим бизнес требованиям к ИТ

гибкость в соответствии требованиям корпоративной стратегии и управления; определение компетентных контактных лиц. **сосредоточено на**

создании прозрачных, гибких и ответственных организационных структур ИТ, определении и реализации на практике ИТ процессов владельцами и прочими должностными лицами, интегрированными в бизнес и принятие решений. **достигается с помощью**

- Определение методологии ИТ процессов.
- Создание необходимых структурных подразделений и структуры.
- Определение должностных функций и обязанностей. **результаты оцениваются с помощью следующих показателей**
- Доля документированных должностных функций.
- Число подразделений/процессов, которые должны поддерживаться ИТ (в соответствии со стратегией), но не поддерживаются.
- Число ключевых видов деятельности (действий) ИТ, находящихся вне рамок ее организационной структуры.



Цели контроля

РО 4.1. Методология ИТ процесса

Следует определить методологию ИТ процесса для того, чтобы реализовать стратегический план ИТ. Методология должна включать в себя структуру ИТ процесса, взаимосвязи (например, для управления возможными разрывами и взаимными наложениями), владельцев процесса, зрелость, оценку эффективности, совершенствование, соответствие требованиям, качественные цели и планы по их достижению. Данная методология должна обеспечивать интеграцию между процессами, характерными для ИТ, управление корпоративным портфелем, бизнес процессами и процессами

изменения бизнеса. Методология ИТ процесса должна быть интегрирована в систему управления качеством (QMS) и систему внутреннего контроля.

РО 4.2. Комитет по стратегии ИТ

Сформировать комитет по стратегии ИТ на уровне Совета директоров. Данный комитет должен обеспечить управление ИТ как элемента корпоративного управления, иметь соответствующие полномочия, давать рекомендации стратегического характера, анализировать основные инвестиции от лица всего Совета директоров.

РО 4.3. Комитет по управлению ИТ

Сформировать комитет по управлению ИТ (или эквивалентный ему орган), состоящий из исполнительного, бизнес и ИТ руководства для того, чтобы:

- Определить приоритеты инвестиционных программ в области ИТ в соответствии со стратегией бизнеса и приоритетами организации;
- Отслеживать реализацию отдельных проектов и устранять ресурсные конфликты;
- Отслеживать уровень оказания услуг и улучшения в этой области. ***РО 4.4.***

Место службы И Т в организации

Следует включить службу ИТ в организационную структуру организации с учетом значимости ИТ для организации, особенно важности для бизнес стратегии и уровня операционной зависимости от ИТ. Отчетность директора по ИТ (CIO) должна быть адекватной значимости ИТ для организации.

РО 4.5. Организационная структура И Т

Создать внутреннюю и внешнюю организационную структуру ИТ в соответствии с потребностями бизнеса. Также нужно упорядочить процессы, чтобы периодически анализировать организационную структуру ИТ с точки зрения соответствия кадровым потребностям и стратегиям в области аутсорсинга, достигать ожидаемых бизнес целей и учитывать изменения.

РО 4.6. Определение должностных обязанностей и полномочий

Установить и донести до сведения всех заинтересованных сторон должностные обязанности и полномочия персонала ИТ и конечных пользователей; разграничить компетенцию персонала ИТ и руководства конечных пользователей, установить ответственность и подотчетность в соответствии с потребностями организации.

РО 4.7. Ответственность за обеспечение качества ИТ

Назначить ответственнгх лиц по вопросам обеспечение качества и обеспечить группу ответственных соответствующими системами, средствами контроля и информирования. Следует убедиться, что полномочия, статус и состав группы по обеспечению качества соответствуют потребностям организации.

РО 4.8. Ответственность зариск, безопасность и соответствие требованиям

Поставить вопросы о принадлежности и ответственности по корпоративным рискам, связанным с ИТ, на уровне высшего руководства. Определить и назначить ключевых должностных лиц для управления ИТ рисками, включая особую ответственность за информационную безопасность, физическую безопасность и соответствие требованиям. Установить ответственность менеджмента по рискам и безопасности на уровне организации. Дополнительная ответственность менеджмента по безопасности может потребоваться на уровне специфических систем. Получить указания от руководства по вопросам отношения к ИТ рискам и решения в отношении остаточных ИТ рисков.

РО 4.9. Владение данными и системами

Следует снабдить бизнес процедурами и инструментами, позволяющими обеспечить функцию бизнеса как собственника данных и информационных систем. Владельцы должны принимать решения о классификации данных и систем и защищать их в соответствии с принятой классификацией.

РО 4.10. Надзорные функции

Следует реализовать адекватные практики по надзору в области ИТ, чтобы оценить, насколько правильно персонал выполняет свои обязанности, обладает ли достаточными полномочиями и ресурсами для осуществления своей деятельности, а также проводить общий анализ ключевых показателей эффективности.

РО 4.11. Разделение полномочий

Необходимо разделить задачи и ответственность лиц, чтобы сократить возможность для отдельного сотрудника подвергнуть риску какой-либо критический процесс. Следует убедиться, что сотрудники выполняют только регламентированные обязанности, предусмотренные их должностными обязанностями.

РО 4.12. Кадровое обеспечениеИТ

Оценить потребности в кадрах на регулярной основе или по мере существенных изменений в бизнесе, операционной или ИТ среде, чтобы быть уверенным в том, что функции ИТ адекватно и в достаточной мере обеспечены кадровыми ресурсами для реализации целей и задач бизнеса.

РО 4.13. Ключевой персонал ИТ

Определить и назначить ключевых должностных лиц в службе ИТ (в том числе дублирующий персонал) и минимизировать зависимость от одного конкретного сотрудника в исполнении критических функций.

РО 4.14. Политика и процедуры в отношении привлекаемых специалистов

Следует убедиться, что консультанты и персонал, работающий по контракту, занятый обеспечением ИТ функций, ознакомлен и исполняет политику организации по защите информационных активов в соответствии с принятыми на себя договорными обязательствами.

PO 4.15. Взаимосвязи

Установить и поддерживать оптимальную координацию и взаимодействие между службой ИТ и другими 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.

Рекомендации по управлению

Из	Входящая информация
PO 1	Стратегический и тактические планы
PO 7	Политики и процедуры ИТ в отношении кадровых ресурсов, матрица навыков ИТ, описания должностных обязанностей
PO 8	Деятельность по повышению качества
PO 9	Планы действий по минимизации связанных с ИТ рисков
ME 1	Планы корректирующих действий
ME 2	Отчет об эффективности контроля ИТ
ME 3	Каталог нормативных и регулирующих требований, относящихся к оказанию услуг ИТ
ME 4	Улучшения методологии процессов

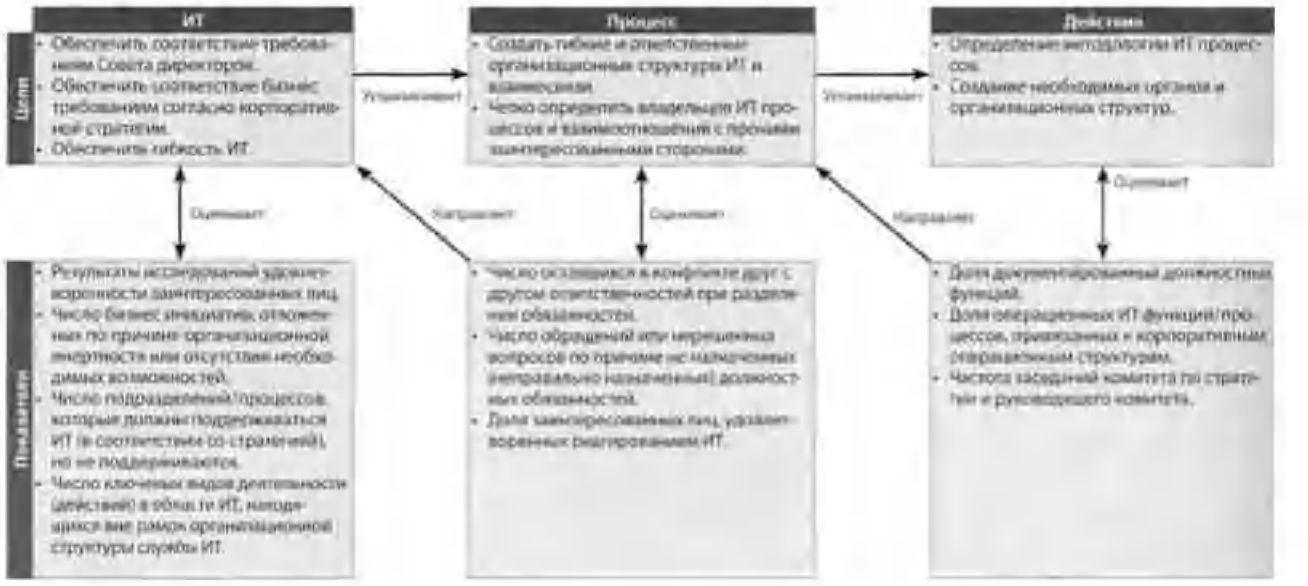
Результаты	В процессах						
Методологии ИТ процессов	ME 4						
Документированные владельцы систем	AI 7	DS 8					
ИТ организация и взаимосвязи	PO 7						
Методологии ИТ процессов, документирование должностных функций и обязанностей	ВСЕ						
Документирование должностных функций и обязанностей	PO 7						

Таблица ОУКИ

Действия ↓ / Функции →	Президент	Финансовый директор	Высшее руководство	Директор по ИТ	Владелец бизнес процесса	Руководитель эксплуатации систем	Главный архитектор ИТ систем	Руководитель разработок	Руководитель администрации ИТ	Руководитель проектного офиса	Аудит, риск, безопасность
Создать организационную структуру ИТ, включая комитеты и связи с заинтересованными сторонами и поставщиками	К	К	И	У		К	К	К	О	К	И
Разработать методологию ИТ процессов	К	К	И	У		К	К	К	О	К	К
Определить владельцев систем		К	К	У	К	О	И	И	И	И	И
Определить владельцев данных		И	У	И	К	И	О	И	И	И	К
Установить и реализовать должностные функции и обязанности в ИТ, включая надзор и разделение обязанностей		И	И	У	И	К	К	К	О	К	К

В таблице ОУКИ показано, кто является Ответственным, Утверждающим, Консультирующим и/или Информированным

Цели и показатели



Модель зрелости

Управление процессом *«Определение ИТ процессов, организационной структуры и взаимосвязей»* удовлетворяет следующим бизнес требованиям к ИТ *гибкость в соответствии требованиям корпоративной стратегии и управления; определение компетентных контактныхлиц* и соответствует характеристикам:

0. Несуществующий

Структура существующей службы ИТ не ориентирована на достижение целей бизнеса.

1. Начальный/Повторяющийся эпизодически и бессистемно

Информационная деятельность и функции службы ИТ осуществляются бессистемно в виде реакции на внешние факторы. ИТ привлекается в бизнес проекты только на завершающей стадии. Служба ИТ считается вспомогательной, отсутствует общая

перспектива ее развития в организации. Есть неявно выраженное понимание необходимости в службе ИТ, однако функции и обязанности не формализованы и не реализованы.

2. ***Повторяющийся, но интуитивный***

Служба ИТ ориентирована на то, чтобы реагировать на потребности бизнеса и сотрудничать с поставщиками с учётом тактических соображений, но отличается непоследовательностью. Обсуждается необходимость в структурированной организации службы ИТ и координации взаимоотношений с поставщиками, однако принимаемые решения по-прежнему зависят от знаний и квалификации ведущих сотрудников. Появляются типовые методы управления службой ИТ и ее взаимоотношениями с поставщиками.

3. ***Определенный***

Существуют определенные функции и обязанности службы ИТ и сторонних организаций. Служба ИТ создана, документально оформлена, о ее существовании доведено до сведения сотрудников организации, деятельность службы ИТ осуществляется в соответствии со стратегией ИТ. Определена система внутреннего контроля. Формализованы взаимоотношения с другими сторонами, включая руководящие комитеты, внутренний аудит и управление поставщиками. Служба ИТ является функционально законченной. Определены функции, которые должны выполняться ИТ персоналом, и те, которые должны выполняться пользователями. Требования к ключевым должностям ИТ персонала и их навыкам определены и удовлетворительны на практике. Существуют формализованные определения отношений между конечными пользователями и третьими сторонами. Разделение функций и обязанностей определено и реализовано на практике.

4. ***Управляемый и измеряемый***

Служба ИТ с упреждением реагирует на изменения и включает все функции, необходимые для удовлетворения потребностей бизнеса. Определены и согласованы вопросы, касающиеся руководства ИТ, принадлежности процессов, отчетности и ответственности. При определении функций службы ИТ применены лучшие внутренние практики. Руководство ИТ обладает необходимыми знаниями и квалификацией для того, чтобы определить, реализовать и осуществлять мониторинг за предпочтительным вариантом структуры службы ИТ и ее взаимоотношениями со сторонними организациями. Стандартизированы контрольные показатели для поддержки бизнес целей и сформулированные пользователями критические факторы успеха. Имеются кадровые возможности для комплектования штата исполнителей проектов и профессионального роста сотрудников. Определено и реализовано рациональное соотношение между внутренними кадровыми ресурсами и специалистами, привлекаемыми со стороны. Организационная структура ИТ адекватна потребностям бизнеса, поскольку предоставляет услуги в соответствии со стратегией развития бизнес процессов, а не в рамках разрозненных технологий.

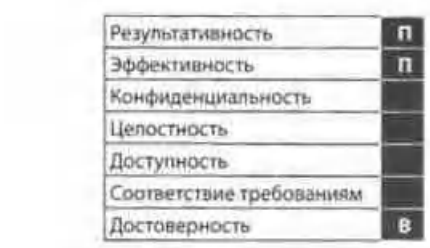
5. ***Оптимизированный***

Организационная структура ИТ является гибкой и адаптивной. Используются лучшие отраслевые практики. Широко применяется технология для содействия в проведении мониторинга эффективности службы ИТ и отдельных процессов. Применяются технологии для поддержки комплексных, географически удаленных друг от друга структурных подразделений. Реализован процесс непрерывного совершенствования.

<u>РО 5. Управление ИТ инвестициями</u>

Описание процесса

Методология 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 иметь 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 (ТСО), реализацию корпоративных преимуществ и получение прибыли на ИТ инвестиции.



Управление процессом

Управление ИТ инвестициями.

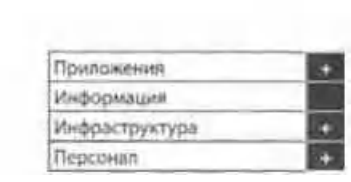
удовлетворяет следующим бизнес требованиям к ИТ

постоянное и наглядное улучшение эффективности затрат в ИТ и участие в повышении прибыльности организации при наличии интегрированных и стандартизованных услуг, соответствующим ожиданиям конечных пользователей. **сосредоточено на** результативных и эффективных решениях по инвестиционным программам в части ИТ, а также планированием и мониторингом ИТ бюджетов в соответствии с ИТ стратегией и инвестиционными решениями. **достигается с помощью**

- Планирования и распределения бюджетов.
- Определения формальных инвестиционных критериев (прибыль на инвестиции (ROI), срок окупаемости, чистая стоимость (NPV)).
- Анализа и оценки динамики пользы для бизнеса по отношению к прогнозам.

результаты оцениваются с помощью следующих показателей

- Доля снижения удельной стоимости оказываемых ИТ услуг.
- Доля отклонений от бюджета относительно общего объема бюджета.
- Доля затрат на ИТ, выраженная в корпоративных и стоимостных показателях (например, рост продаж по причине расширения каналов связи).



Цели контроля

РО 5.1. Методология управления финансами

Разработать и поддерживать методологию управления финансами для управления инвестициями и стоимостью ИТ активов и услуг посредством портфелей ИТ инвестиций, бизнес-планов и ИТ бюджетов.

РО 5.2. Расстановка приоритетов внутри ИТ бюджета

Реализовать на практике процесс принятия решений, имеющий целью расстановку приоритетов при распределении ИТ ресурсов. Увеличивать вклад ИТ в оптимизацию корпоративного портфеля связанных с ИТ инвестиционных программ и других ИТ услуг и активов.

РО 5.3. Формирование бюджета ИТ

Установить и внедрить практику по подготовке бюджета, отражающего приоритеты корпоративного портфеля инвестиционных программ, связанных с ИТ, а также включающего текущие затраты по эксплуатации и обслуживанию существующей инфраструктуры. Данная практика должна применяться при разработке общего бюджета ИТ, а также бюджетов отдельных инвестиционных программ, при особом внимании к их ИТ компонентам. Эта практика также должна найти применение в ходе текущего анализа, доработки и утверждения общего бюджета и бюджетов отдельных инвестиционных программ.

РО 5.4. Управление затратами

Внедрить процесс управления затратами, проводя сравнения текущих затрат и бюджетов. Должен проводиться мониторинг затрат и отчетность по его итогам. Должны своевременно фиксироваться отклонения от бюджета и оцениваться их влияние на реализацию инвестиционных программ. Совместно с корпоративным куратором этих программ должна проводиться корректировка и, в случае необходимости, их пересмотр.

РО 5.5. Управлениепреимуществами

Необходимо реализовать на практике процесс мониторинга преимуществами, получаемых в результате использования возможностей ИТ. Вклад ИТ в бизнес, как в случае компонента связанных с ИТ инвестиционных программ, так и в случае постоянной операционной поддержки, должен быть определен, документирован, согласован и оформлен в виде отчета. Такие отчеты должны анализироваться и, в случае, когда есть возможность увеличить вклад ИТ в бизнес, должны планироваться и предприниматься соответствующие меры. В случаях, когда вклад ИТ в бизнес меняется и оказывает влияние на реализацию инвестиционных программ, программы должны пересматриваться.

Рекомендации по управлению

Из	Входящая информация
PO 1	Стратегический и тактические планы ИТ, портфель проектов и услуг
PO 3	Требования инфраструктуры
PO 10	Обновленные портфель ИТ проектов
AI 1	Обоснование бизнес требований
AI 7	Обзор результатов внедрения
DS 3	План по производительности и мощностям (требования)
DS 6	финансовые документы ИТ
ME 4	Ожидаемая отдача от связанных с ИТ инвестиций для организации

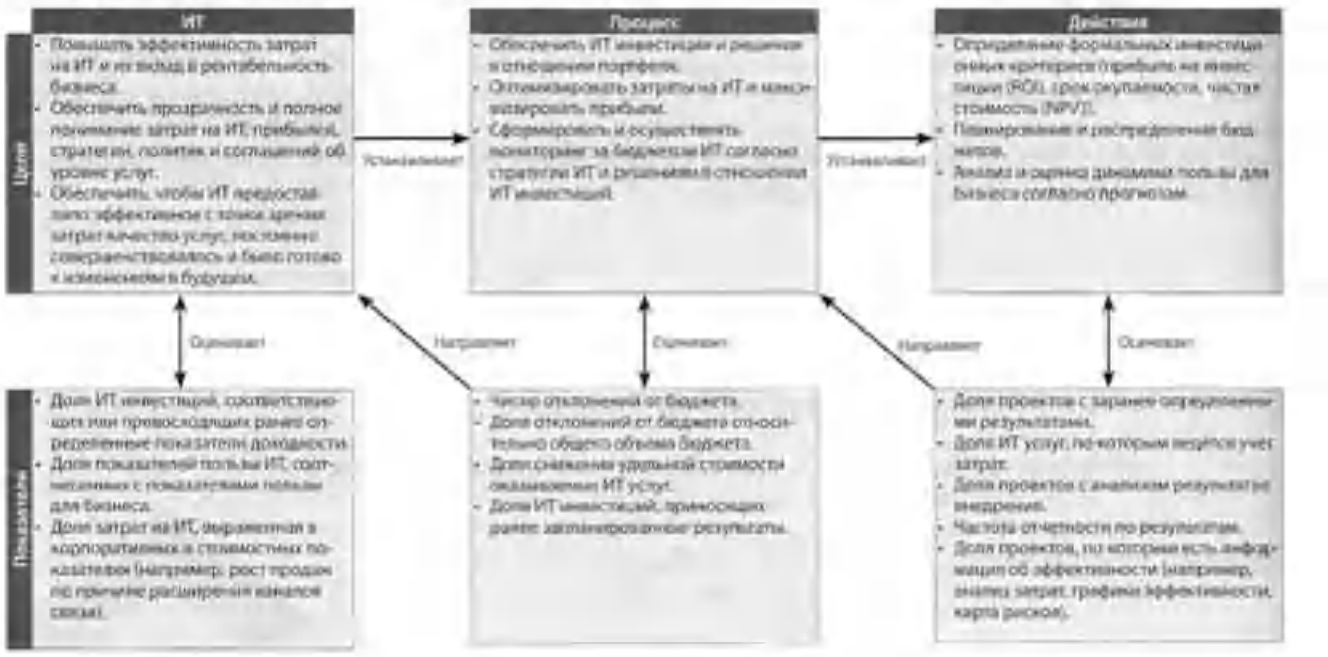
Результаты	В процессы						
Отчеты о затратах и преимуществах	PO 1	AI 2	DS 6	ME 1	ME 4		
Бюджеты ИТ	DS 6						
Обновленный портфель ИТ услуг	DS 1						
Обновленный портфель ИТ проектов	PO 10						

Таблица ОУКИ

Действия ↓ Функции →	Президент	Финансовый директор	Высшее руководство	Директор по ИТ	Владелец бизнес процесса	Руководитель инструмента (систем)	Главный архитектор ИТ систем	Руководитель разработок	Руководитель администрации ИТ	Руководитель проектного офиса	Аудит, риски, безопасность
Осуществлять поддержку портфеля инвестиционных программ	У	О	О	О	К					И	И
Осуществлять поддержку портфеля ИТ проектов	И	К	У/О	У/О	К		К	К		К	И
Осуществлять поддержку портфеля ИТ услуг	И	К	У/О	У/О	К	К				К	И
Разработать и поддерживать формирование бюджета ИТ	И	К	К	У		К	К	К	О	К	
Определить, информировать и осуществлять мониторинг затрат и прибылей от ИТ инвестиций	И	К	К	У/О		К	К	К	О	К	К

В таблице ОУКИ показано, кто является Ответственным, Утверждающим, Консультирующим и/или Информированным

Цели и показатели



Модель зрелости

Управление процессом *«Управление ИТ инвестициями»* удовлетворяет следующим бизнес требованиям к ИТ *постоянное и наглядноеулучшение эффективности затрат в ИТи участие в повышении прибыльности организации при наличии интегрированных и стандартизованных услуг, соответствующим ожиданиям конечных пользователей* и соответствует характеристикам:

0. Несуществующий

Отсутствует осознание важности оптимального выбора инвестиций в ИТ и формирования бюджета. Не проводится мониторинг ИТ инвестиций и затрат.

1. Начальный/Повторяющийся эпизодически и бессистемно

Организация признает необходимость управления инвестициями в ИТ, однако информирование заинтересованных сторон об этом осуществляется непоследовательно.

Формальное назначение ответственнъгх за выбор вариантов инвестирования в ИТ и разработку бюджета осуществляется от случая к случаю. Имеют место разрозненные попытки реализации процесса выбора вариантов инвестирования в ИТ, формирования бюджета и его нерегламентированного документального оформления. Обоснование вариантов инвестиций в ИТ

осуществляется от случая к случаю. Принимаемые решения по бюджету являются реакцией на внешние события и ориентированы на удовлетворение текущих потребностей.

2. Повторяющийся, но интуитивный

Есть неявное понимание необходимости выбора вариантов инвестирования в ИТ и формирования бюджета, о чем проинформированы заинтересованные стороны. Соблюдение процедуры зависит от инициативы сотрудников организации. Появляются типовые методики разработки элементов бюджета по ИТ. Решения по бюджету являются реакцией на внешние события и принимаются с учетом тактических соображений.

3. Определенный

Процессы выбора вариантов инвестирования в ИТ и формирования бюджета достаточно обоснованы и учитывают основные аспекты бизнеса и технологии. Процедура выбора варианта инвестирования и политика в области инвестиций определены, документально оформлены и доведены до сведения персонала. Бюджет на ИТ согласован со стратегическими планами развития ИТ и бизнеса. Процессы разработки бюджета и выбора вариантов инвестирования в ИТ формализованы, документально оформлены, и о них проинформированы заинтересованные стороны. Возникает формализованное обучение, которое, правда, пока основано в основном на индивидуальной инициативе. Имеет место официальное утверждение бюджетов и выбранных вариантов инвестирования в ИТ. Персонал ИТ имеет необходимый опыт и квалификацию для разработки бюджета ИТ и соответствующих рекомендаций по вариантам инвестирования.

4. Управляемый и измеряемый

Ответственность и подотчетность за разработку бюджета и выбор решения по инвестированию возложены на конкретных сотрудников. Выявляются и устраняются бюджетные отклонения. Проводится формализованный анализ прямых и косвенных издержек по текущим операциям, а также предложенных альтернативных вариантов инвестирования с учетом всех затрат на период эксплуатации. При разработке бюджета используется упреждающий и стандартизированный процесс. В инвестиционных планах происходит смещение акцента в затратах с разработки и эксплуатации аппаратных и программных средств на обеспечение системной интеграции и кадровое обеспечение ИТ. Размеры выгод и возврата на инвестиции рассчитываются как в финансовых, так нефинансовых параметрах.

5. Оптимизированный

Для сравнительной оценки затрат и выявления путей повышения эффективности инвестиций применяются лучшие отраслевые практики. В процессе формирования бюджета и выбора вариантов инвестирования используется анализ технологических инноваций. Процесс управления инвестициями постоянно совершенствуется на основе анализа текущей эффективности инвестиций. Инвестиционные решения принимается с учетом тенденций улучшения показателя цена /производительность и появления новых технологий и программных продуктов. Альтернативные варианты финансирования анализируются и оцениваются с учетом существующей структуры капитала организации с использованием формализованных методов оценки. Обеспечивается упреждающее выявление отклонений. При принятии инвестиционных решений учитываются результаты анализа долговременной стоимости владения.

РО 6. Информирование о целях и направлениях развития ИТ

Описание процесса

Руководство разрабатывает корпоративную методологию контроля в сфере ИТ и доносит ее до исполнителей. Программа информирования, принятая и поддержанная руководством, реализуется для объяснения миссии, целей услуг, политики и процедур и т.д. Информирование поддерживает достижение целей ИТ и обеспечивает лучшее понимание ИТ рисков, целей и направления развития. Процесс обеспечивает соответствие законодательству и нормативным требованиям.

Управление процессом

Информирование о целях и направлениях развития ИТ.

удовлетворяет следующим бизнес требованиям к ИТ

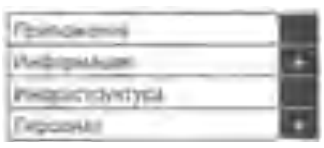
предоставление точной и своевременной информации о текущих и будущих ИТ услугах и связанных с ними рисках и ответственности. **сосредоточено на**

создании четких, понятных и утвержденных политик, процедур, руководств и прочей документации, включенной в методологию контроля в сфере ИТ, для заинтересованных сторон. **достигается с помощью**

- Определении методологии контроля в сфере ИТ.
- Разработки и внедрения ИТ политик.
- Реализации ИТ политик на практике.

результаты оцениваются с помощью следующих показателей

- Количество нарушений в работе бизнеса, вызванных перебоями в работе ИТ.
- Доля заинтересованных сторон, понимающих методологию корпоративного контроля в сфере ИТ.
- Доля заинтересованных сторон, не придерживающихся политик.



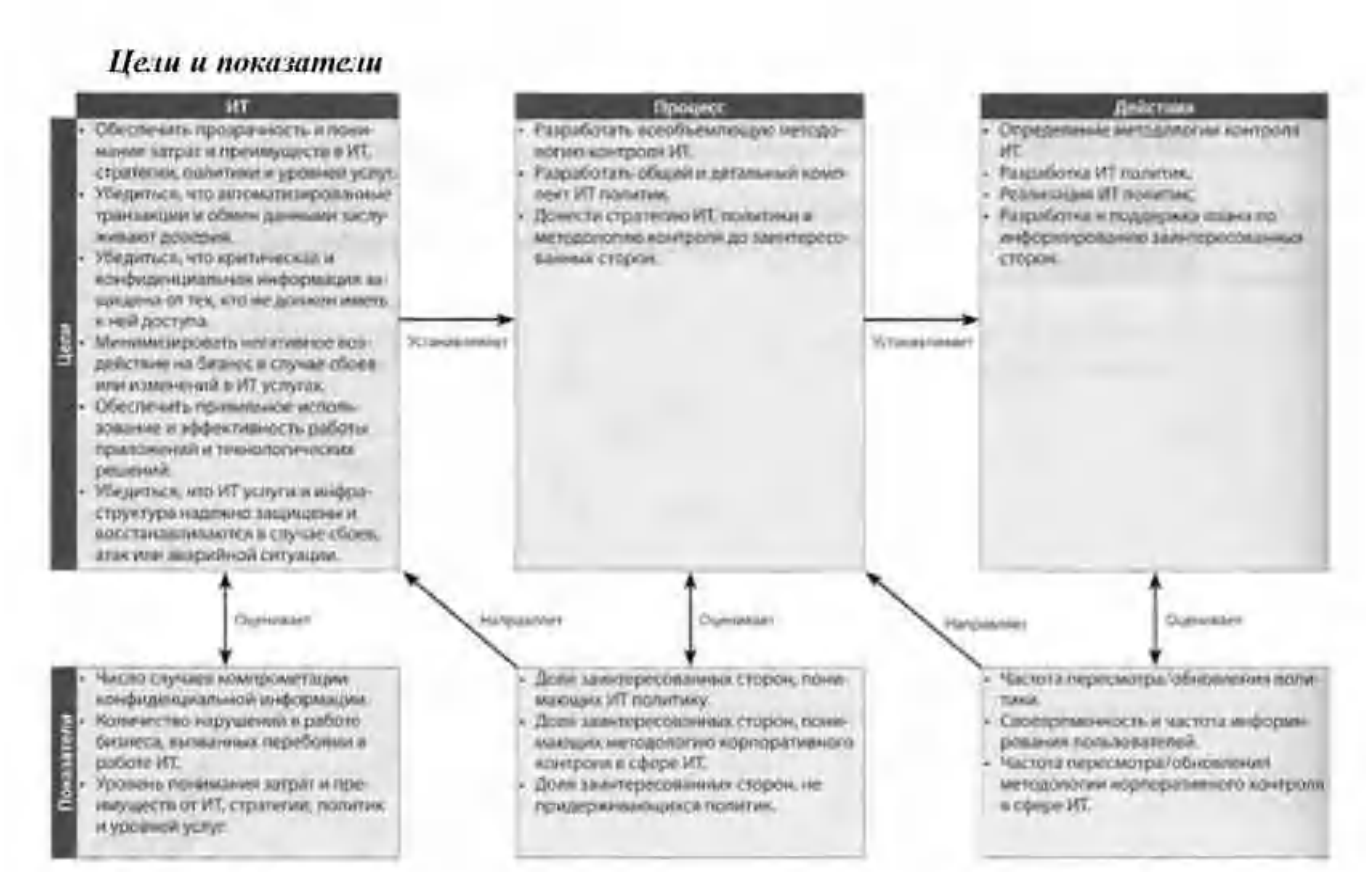
Рекомендации по управлению

Из	Входящая информация
РО 1	Стратегический и тактические планы ИТ, портфель ИТ проектов и услуг
РО 9	Рекомендации/ указания по управлению сигналами с ИТ рисками
МЕ 2	Отчет по эффективности контроля ИТ

Результаты	В процессах					
Корпоративная методология контроля ИТ	ВСЕ					
ИТ политики	ВСЕ					

Таблица ОУКИ

Действия ↓ / Функции →	Президент	Финансовый директор	Высшее руководство	Директор по ИТ	Владелец бизнес процесса	Руководитель эксплуатации систем	Главный архитектор ИТ систем	Руководитель разработки	Руководитель администрации ИТ	Руководитель проектного офиса	Аудит, риски, безопасность
Разработать и поддерживать методологию и среду ИТ контроля	И	К	И	У,О	И	К		К	Л		К
Разработать и поддерживать ИТ политики	И	И	И	У,О		К	А	К	О		К
Информировать о методологии ИТ контроля, ИТ целях и направлениях развития	И	И	И	У,О					О		К



Модель зрелости

Управление процессом *«Информирование о целях и направлениях развития ИТ»* предоставление точной и *своевременной информации о текущих и будущих ИТ услугах и связанных с ними рисках и ответственности* и соответствует характеристикам:

0. Несуществующий

Руководство не определило среду контроля в области ИТ. Отсутствует понимание необходимости реализации совокупности политики, процедур, стандартов и процессов мониторинга за их соблюдением.

1. Начальный/Повторяющийся эпизодически и бессистемно

Руководство восприимчиво к рассмотрению требований к среде контроля в области ИТ. Политика, процедуры и стандарты разработаны и распространяются от случая к случаю как реакция на возникающие проблемы. Процессы разработки, информирования и соответствия требованиям являются неформальными и несогласованными.

2. Повторяющийся, но интуитивный

Существует понимание необходимости создания эффективной системы контроля в области ИТ, но практики преимущественно неформальны. Руководство проинформировало заинтересованные стороны о необходимости использования политик, планов и процедур в области управления и контроля, однако их разработка оставлена на усмотрение отдельных руководителей и бизнес подразделений. Признано, что обеспечение качества является желательной политикой, которой необходимо следовать, однако практики оставлены на усмотрение отдельных менеджеров. Обучение проводится на индивидуальной основе по мере необходимости.

3. Определенный

Руководством разработана, документально оформлена и доведена до сведения заинтересованных сторон полная концепция в области управления качеством и среды контроля, включающая общий подход в отношении политик, планов и процедур. Процесс разработки политик структурирован, осуществляется его поддержка и о нем известно персоналу, а существующие политики, планы и процедуры вполне приемлемы и охватывают

основные вопросы. Руководство осознало важность осведомленности персонала в вопросах информационной безопасности и начало реализацию программ информирования. Организована формально программа обучения персонала для поддержки среды управления информацией, но она реализуется недостаточно строго. Пока ведется разработка методологии и процедур контроля, применяется непоследовательный мониторинг за их соблюдением. Существует общая методология разработки. Стандартизованы и формализованы методики информирования о вопросах информационной безопасности.

4. Управляемый и измеряемый

Руководство принимает ответственность за информирование заинтересованных сторон о политиках внутреннего контроля, делегирует ответственность и выделяет достаточные ресурсы для поддержки системы контроля в случае значительных изменений. Сформирована позитивная упреждающая система контроля в области ИТ, включая обязательство по информированию персонала по вопросам качества и информационной безопасности. Разработан полный комплект политик, планов и процедур, который поддерживается, доводится до сведения персонала и основан на лучших внутренних практиках. Реализована методология внедрения процедур и последующих проверок их соблюдения.

5. Оптимизированный

Среда контроля в области ИТ соответствует общей стратегии развития и перспективным планам и часто анализируется, обновляется и непрерывно совершенствуется. Для применения лучших отраслевых практик руководства процессами управления и информирования персонала привлекаются наиболее опытные собственные и сторонние специалисты. Процессы мониторинга, внутренней оценки и проверки соответствия требованиям широко применяются в масштабе всей организации. Используются соответствующие технологии для сопровождения баз знаний по политике и информированию персонала, а также для оптимизации процесса информирования посредством применения систем автоматизации учрежденческой деятельности и автоматизированных средств обучения.

РО 7. Управление персоналом

Описание процесса

Компетентный персонал нанимается и удерживается для того, чтобы создать и оказывать бизнесу ИТ сервисы. Управление персоналом осуществляется посредством применения определенных и согласованных практик по набору, обучению, оценке эффективности, продвижению и увольнению. 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.

Управление процессом

Управление персоналом.

удовлетворяет следующим бизнес требованиям к ИТ

наём компетентного и мотивированного персонала для создания и оказания ИТ сервисов.

сосредоточено на

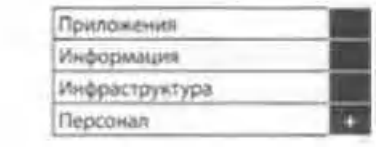
наёме и обучении персонала, мотивации в ясной карьерной перспективе, назначении должностных обязанностей в соответствии с навыками, организации определенного процесса оценки деятельности персонала, создании должностных инструкций и осознании зависимости от человеческого фактора.

достигается с помощью

- Оценки эффективности работы персонала.
- Найма и обучения ИТ персонала для реализации тактических планов ИТ.
- Минимизации риска чрезмерной зависимости от отдельных ключевых ресурсов.

результаты оцениваются с помощью следующих показателей

- Уровня удовлетворенности заинтересованных сторон опытом и навыками ИТ персонала.
- Показателей текучести кадров ИТ.
- Доли ИТ персонала, обладающего сертификатами в сфере их профессиональной деятельности.



Цели контроля

РО 7.1. Наём и удержание персонала

Управлять процессами подбора и найма ИТ персонала в соответствии с общей кадровой политикой и процедурами, принятыми в организации (это относится к наёму, позитивной рабочей среде, введению в курс дел). Реализовать эти процессы на практике, чтобы организация была обеспечена ИТ персоналом, обладающим навыками, необходимыми для достижения бизнес целей.

РО 7.2 Компетентность персонала

Регулярно проводить проверки, чтобы удостовериться в том, что персонал обладает достаточной компетентностью для исполнения своих обязанностей, основанной на образовании, обучении и/или опыте. Определить основные требования к компетентности ИТ персонала и проверять соответствие эти требованиям, применяя, где это уместно, квалификационные тесты и программы сертификации.

РО 7.3 Распределение обязанностей

Определить и осуществлять надзор за ролями и обязанностями, а также компенсационными пакетами персонала, включая требование придерживаться политики и процедур организации, профессионального опыта, и профессиональной этики. Уровень надзора должен соответствовать значимости конкретной должности для организации и масштабу должностной ответственности.

РО 7.4. Обучениеперсонала

Обеспечить сотрудникам ИТ введение в курс дел при наёме и проведение специальных курсов обучения по усовершенствованию знаний, навыков, мер внутреннего контроля и обеспечения безопасности, необходимых для достижения бизнес целей.

РО 7.5. Зависимость от отдельных сотрудников

Минимизировать критическую зависимость от отдельных сотрудников, документируя знания, организовав обмен опытом и планирование на случай увольнений, а также наличие сотрудников-дублеров.

РО 7.6. Проверка персонала на предмет допуска кработе

Включить проверку персонала на предмет допуска к работе в число требований процесса найма. Степень и регулярность таких проверок должны зависеть от значимости и/или критичности конкретной должности и применяться в отношении сотрудников, контрагентов и поставщиков.

РО 7.7. Оценка эффективности работы персонала

Необходимо разработать систему регулярной оценки эффективности работы, достижения индивидуальных целей, производных от бизнес целей, принятых стандартов и должностных обязанностей. Сотрудники должны получать инструктаж по увеличению эффективности своей работы.

РО 7.8. Переход на другую работу и увольнение

Следует предпринять надлежащие действия при переходе сотрудников на другую работу и, особенно, при увольнении. Должна быть налажена передача знаний, перераспределение ответственностей и ликвидация прав доступа для минимизации рисков и обеспечения непрерывного функционирования.

Рекомендации по управлению

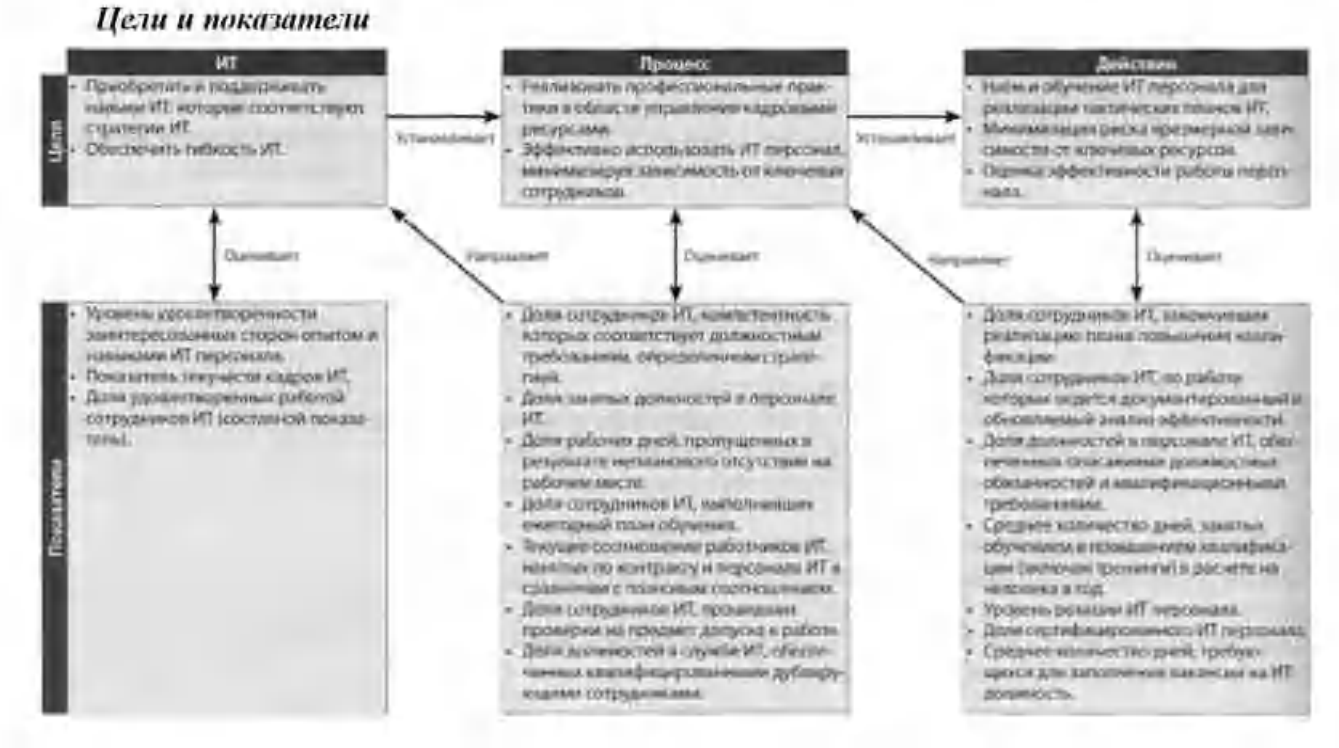
Из	Входящая информация
PO 4	Организационная структура ИТ и взаимосвязи документированных должности и ответственности
AI 1	Обоснованные бизнес требования

Результаты	В процессе						
Политика и процедуры ИТ в отношении кадровых ресурсов	PO 4						
Матрица навыков ИТ	PO 4	PO 10					
Описания должностных обязанностей	PO 4						
Навыки и компетентность пользователей, включая индивидуальное обучение	DS 7						
Спецификации требований к обучению	DS 7						
Должности и ответственности	AI3						

Таблица ОУКИ

Действия ↓ Функции →	Президент	Финансовый директор	Высшее руководство	Директор по ИТ	Владелец бизнес процесса	Руководитель эксплуатации систем	Главный архитектор ИТ систем	Руководитель разработок	Руководитель администрирования ИТ	Руководитель проектного офиса	Аудит, риски, безопасность
Определить навыки ИТ, создать описания должностных обязанностей, уровни оплаты труда и инструментарий сравнения эффективности работы		К		У		К	К	К	О	К	
Реализовать кадровую политику и процедуры применительно к сфере ИТ (поиск, найм, рассмотрение, компенсационный пакет, обучение, оценка, продвижение и увольнение)				У		О	О	О	О	О	К

В таблице ОУКИ показано, кто является Ответственным, Утверждающим, Консультирующим и/или Информированным



Модель зрелости

Управление процессом *«Управление персоналом»* удовлетворяет следующим бизнес требованиям к ИТ *наём компетентного и мотивированного персонала для создания и оказания ИТсервисов* и соответствует характеристикам:

0. Несуществующий

Отсутствует осознание важности согласования управления кадровыми ресурсами ИТ с планированием развития технологии для организации. Нет сотрудников, формально ответственных за управление кадровыми ресурсами ИТ.

1. Начальный/Повторяющийся эпизодически и бессистемно

Руководство признает необходимость управления кадровыми ресурсами ИТ, однако данный процесс не формализован и в большей степени реагирует на внешние факторы. Процесс управления кадровыми ресурсами ИТ ориентирован на решение таких текущих вопросов как наем и управление ИТ персоналом. Растет осознание того влияния, которое

оказывают быстрые изменения в бизнесе, технологии и все более сложные решения на необходимость новых специальных знаний и навыков и уровней компетентности.

2. Повторяющийся, но интуитивный

Господствует тактический подход к наёму и управлению ИТ персоналом, обусловленный скорее потребностями конкретных проектов, чем продуманным соотношением предложений квалифицированных сотрудников внутри организации и на стороне. Осуществляется неформальное обучение новых сотрудников, которые затем проходят обучение по мере необходимости.

3. Определенный

Определен и документирован процесс управления кадровыми ресурсами ИТ. Существует соответствующий план. При наёме и управлении персоналом ИТ используется стратегический подход. Имеется официально утвержденный план обучения персонала, призванный удовлетворить потребности к кадровым ресурсам ИТ. Внедрена программа ротации кадров, предназначенная для совершенствования опыта управления как в технических, так и в бизнес областях.

4. Управляемый и измеряемый

Ответственность за разработку и поддержку плана управления кадровыми ресурсами ИТ возложена на конкретного сотрудника (или группу лиц), обладающих для этого необходимым опытом и квалификацией. Процесс разработки и поддержки плана управления кадровыми ресурсами

ИТ способен адаптироваться к изменениям. В организации стандартизированы критерии, которые позволяют выявлять отклонения от плана, при этом особый акцент уделяется управлению вопросами роста численности и текучести кадров. Налажен мониторинг за динамикой зарплаты и эффективностью работы в сравнении с этими показателями в конкурирующих организациях и лучшими отраслевыми практиками. Управление людскими ресурсами ИТ носит упреждающий характер и учитывает вопросы карьерного роста.

5. Оптимизированный

Существует постоянно обновляемый план управления кадровыми ресурсами ИТ, который отвечает меняющимся требованиям бизнеса. Управление кадровыми ресурсами ИТ интегрировано с планированием развития технологии, обеспечивая оптимальное развитие и использование имеющихся сотрудников ИТ. Управление кадровыми ресурсами ИТ интегрировано и соответствует направлению стратегического развития организации. Компоненты процесса управления кадровыми ресурсами ИТ, такие как система оплаты труда, оценка эффективности работы, участие в отраслевых форумах, передача знаний, обучение и наставничество соответствуют лучшим отраслевым практикам. Перед внедрением в организацию любых новых продуктов и технологических стандартов разрабатываются соответствующие программы обучения.

РО 8. Управление качеством

Описание процесса

Разработана и поддерживается система управления качеством (QMS), 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
того, чтобы ИТ привносил ценности в бизнес, совершенствование и а также постоянное прозрачность для заинтересованных сторон.

Управление процессом

Управление качеством.

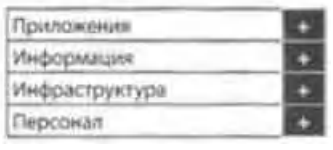
удовлетворяет следующим бизнес требованиям к ИТ

обеспечение постоянного и измеряемого улучшения качества ИТ услуг.

сосредоточено на

определении системы управления качеством, текущем мониторинге эффективности по достижению ранее предписанных целей и внедрении программы постоянного улучшения качества ИТ услуг. **достигается с помощью**

- Определения стандартов и практик обеспечения качества.
- Мониторинга и анализа эффективности внутренних и внешних сервисов в сравнении с определенными стандартами и практиками обеспечения качества.
- Постоянного совершенствования системы управления качеством. **результаты оцениваются с помощью следующих показателей**
- Доля заинтересованных сторон, удовлетворенных качеством ИТ (с учетом значимости их мнений).
- Доля ИТ процессов, формально охваченных наблюдением системы управления качеством на постоянной основе, которые соответствуют конечным целям и задачам обеспечения качества.
- Доля процессов, охваченных системой управления качеством.



Цели контроля

РО 8.1. Системауправления качеством

Создать и поддерживать систему управления качеством, которая обеспечивает стандартизованный, формализованный и постоянно действующий подход в отношении управления качеством и согласована с бизнес требованиями. Система управления качеством должна определять требования и критерии качества; основные ИТ процессы, их последовательность и взаимодействие; политики, критерии и методы для определения, выявления, корректировки и предотвращения несоответствий. Система управления качеством должна определять организационную структуру управления качеством, включающую в себя задачи и должностные обязанности. Все основные подразделения должны разработать собственные планы в соответствии с критериями и политиками и

фиксировать показатели качества. Осуществлять мониторинг и измерение эффективности и адекватности системы управления качеством и совершенствовать ее в случае необходимости.

РО 8.2. ИТ стандарты и практикиуправления качеством

Определить и поддерживать стандарты, процедуры и практические меры в основных ИТ процессах, чтобы организация соответствовала целям системы управления качеством. Внедрить лучшие отраслевые практики в ходе совершенствования управления качества в организации.

РО 8.3. Стандарты в области разработки и приобретения

Принять и поддерживать стандарты для всех видов разработок и приобретений, которые действуют в течение всего времени исполнения процесса и включают приемку его основных этапов в соответствии с ранее утвержденными критериями. Обратить внимание на такие аспекты, как стандарты программирования; соглашения по наименованиям; форматы файлов; схему и стандарты построения справочника данных; стандарты разработки пользовательских интерфейсов; совместимость; производительность систем; масштабируемость; стандарты разработки и тестирований; проверку на соответствие требованиям; планы тестирования; тестирование отдельных модулей, регрессионное и интеграционное тестирование.

РО 8.4. Акцент на потребностях заказчика

Сделать акцент в работе системы управления качеством на определении потребностей заказчиков и нахождении соответствий между ними, ИТ стандартами и практиками. Определить роли и обязанности при разрешении конфликтной ситуации между пользователем/заказчиком и службой ИТ.

РО 8.5. Постоянное совершенствование

Поддерживать и регулярно доносить до персонала общий план повышения качества, который предполагает постоянное совершенствование.

РО 8.6. Оценкауровня качества, мониторинг и обзор

Определить, спланировать и внедрить на практике систему измерений для постоянного мониторинга соответствия требованиям системы управления качеством, а также ценностей, которые должна обеспечивать эта система. Измерение, мониторинг и фиксирование

информации должны осуществляться владельцем процесса для того, чтобы предпринимать корректирующие и превентивные действия.

Рекомендации по управлению

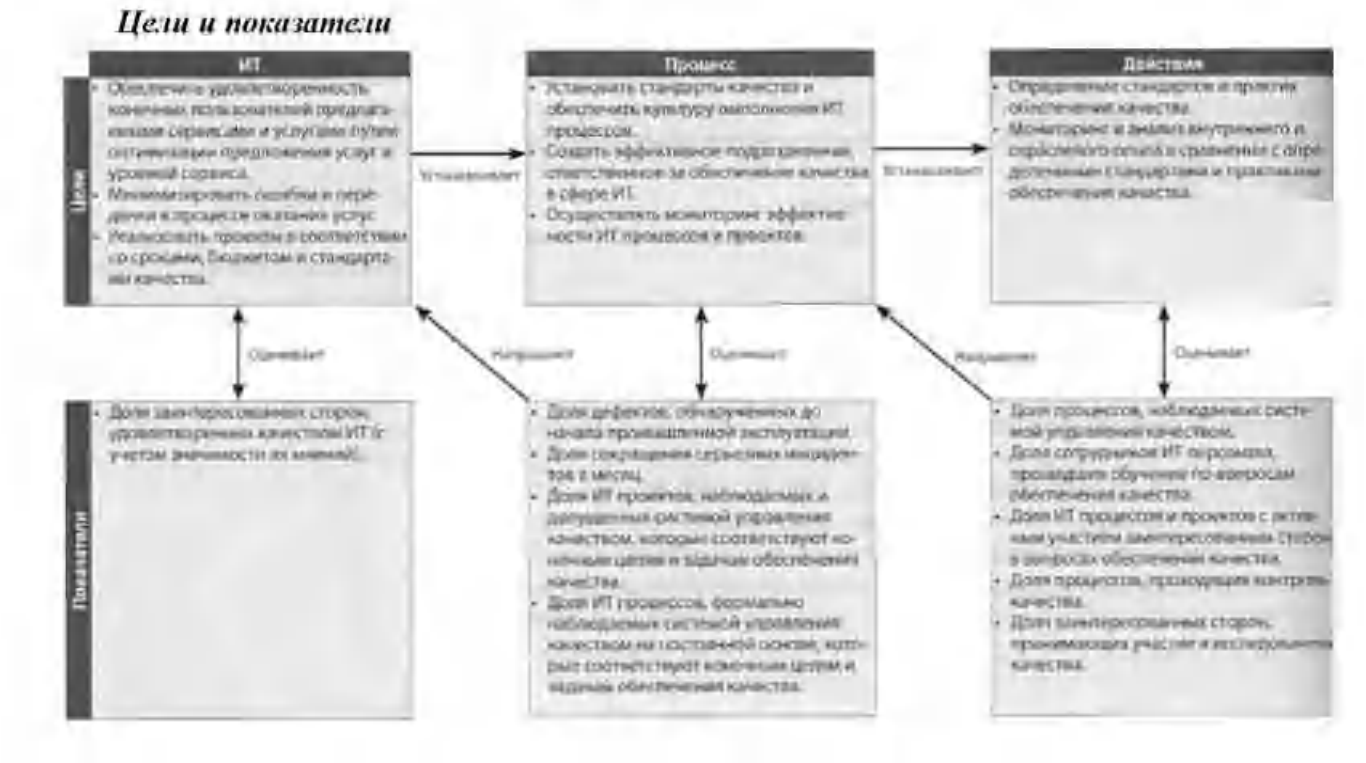
Из	Входящая информация
PO 1	Стратегический план ИТ
PO 10	Детализированные планы проектов
ME 1	Корректирующие планы действий

Результаты	В процессы				
Стандарты в области приобретений	AI 1	AI 2	AI 5	DS 2	
Стандарты в области разработки	PO 10	AI 1	AI 2	AI 3	AI 7
Стандарты и метрики в области качества	ВСЕ				
Действия по повышению качества	PO 8	AI 6			

Таблица ОУКИ

Действия ↓ Функции →	Президент	Финансовый директор	Высшее руководство	Директор по ИТ	Владелец бизнес-процесса	Руководитель инструментальных систем	Главный архитектор ИТ-систем	Руководитель разработки	Руководитель администрации ИТ	Руководитель проектного офиса	Аналитик систем
Определить систему управления качеством	К		К	У/О	И	И	И	И	И	И	К
Создать и поддерживать систему управления качеством	И	И	И	У/О	И	К	К	К	К	К	К
Разработать и информировать внутри организации о стандартах в области качества		И		У/О	И	К	К	К	К	К	К
Создать и поддерживать план постоянного повышения качества				У/О	И	К	К	К	К	К	К
Осуществлять измерение, мониторинг и анализ соответствия целям качества				У/О	И	К	К	К	К	К	К

В таблице ОУКИ показано, кто является Ответственным, Утверждающим, Консультирующим и/или Информированным



Модель зрелости

Управление процессом *«Управление качеством»* удовлетворяет следующим бизнес требованиям к ИТ *обеспечение постоянного и измеряемого улучшения качества ИТ услуг* и соответствует характеристикам:

0. Несуществующий

В организации отсутствует процесс планирования системы управления качеством и методология разработки систем с учетом всего жизненного цикла. Руководители высшего звена и персонал ИТ не осознают необходимости в системе обеспечения качества. Проекты и текущая деятельность никогда не анализируются с точки зрения обеспечения качества.

1. Начальный/Повторяющийся эпизодически и бессистемно

Руководство осознает необходимость в системе обеспечения качества. Начальные попытки предпринимаются отдельными сотрудниками, обладающими определенной квалификацией. Руководство делает неформальные оценки в отношении качества.

2. Повторяющийся, но интуитивный

Внедряется программа управления определения и мониторинга качества в рамках службы ИТ. Деятельность системы управления качеством сосредоточена в ряде инициатив, связанных с ИТ проектами и процессами, но не в масштабах всей организации.

3. Определенный

Существует определенный процесс обеспечения качества, о котором руководство информирует заинтересованные стороны всей организации и в котором участвует руководство конечных пользователей ИТ. Возникает программа обучения вопросам обеспечения качества для всех уровней данной организации. Определены базовые требования в отношении качества, они совместно используются на уровне отдельных проектов и внутри службы ИТ. Возникают общие инструменты и практики управления качеством. Планируются и время от времени проводятся исследования удовлетворенности качеством.

4. Управляемый и измеряемый

Вопросы обеспечения качества рассматриваются во всех процессах, включая те, которые зависят от сторонних организаций. Создается стандартизированная база знаний по показателям

качества. Для обоснования инициатив в области обеспечения качества применяется анализ затраты и выгод. Начинает применяться сравнительный анализ на соответствие отраслевым нормам и стандартам качества, принятым конкурентами. Существует программа обучения вопросам обеспечения качества для всех уровней данной организации. Стандартизован инструментарий системы обеспечения качества и ее практики, периодически проводится анализ первопричин проблем. Регулярно проводятся исследования удовлетворенности качеством. Введена стандартизованная и хорошо структурированная программа оценки качества. Руководство ИТ разрабатывает базу знаний для показателей качества.

5. Оптимизированный

Система обеспечения качества интегрирована во все виды ИТ деятельности. Ее процессы являются гибкими и адаптируемыми к изменениям в ИТ среде. Созданная база знаний в области качества дополнена лучшими отраслевыми практиками. Регулярно проводится сравнительный анализ на соответствие внешним стандартам. Исследования удовлетворенности качеством является постоянным процессом и ведет к анализу первопричин проблем и мерам по совершенствованию качества. Руководство процессом обеспечения качества формализовано.

РО 9. Опенка и управление ИТ рисками

Описание процесса

Создана и поддерживается методология управления рисками. Задача методологии — документирование общего и согласованного уровня ИТ рисков, стратегий минимизации рисков и остаточных рисков. Любое потенциальное воздействие на достижение целей организации, вызванное незапланированным событием должно учитываться, анализироваться и оцениваться. Стратегии 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.

Управление процессом

Оценка и управление ИТ рисками.

удовлетворяет следующим бизнес требованиям к ИТ

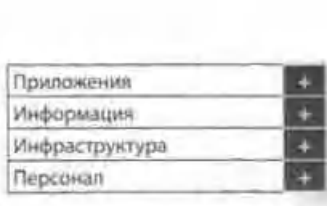
анализ и информирование об ИТ рисках и их потенциальном воздействии на бизнес процессы и цели. **сосредоточено на**

разработке методологии управления рисками, интегрированной в методологию корпоративных и операционных рисков, оценки рисков, минимизации и информирования об остаточных рисках. **достигается с помощью**

- Полного включения управления рисками в процессы управления, как внутри, так и вовне, и его постоянного применения.
- Проведении оценок рисков.
- Выработки предложений и информирования о планах противодействия существующим рискам.

результаты оцениваются с помощью следующих показателей

- Доля критичных целей ИТ, охваченных оценкой рисков.
- Доля выявленных критичных ИТ рисков, в отношении которых разработаны планы действий.
- Доля планов по управлению рисками, утвержденных и принятых к исполнению.



Цели контроля

РО 9.1. Методологияуправлениярисками в сфереИТ

Разработать методологию управления рисками в сфере ИТ, которая соответствовала бы корпоративной методологии управления рисками. ***РО 9.2. Организациярисковой среды***

Организовать среду, в которой будет применяться методология оценки рисков. Этот процесс должен включать в себя определение внутренней и внешней среды для оценки каждого из рисков, задач оценки и критериев в соответствии с которыми риски будут оцениваться.

РО 9.3. Идентификация происшествий

Идентифицировать происшествия (существенную реалистичную угрозу, которая может реализоваться на наиболее уязвимом участке) с точки зрения потенциального негативного воздействия на цели или текущую деятельность организации, включая корпоративные, нормативные, технологические, договорные, кадровые и операционные аспекты. Определить суть последствий и

использовать эту информацию. Документировать и обновлять соответствующие риски в карте рисков.

РО 9.4. Оценкарисков

Проводить регулярную оценку вероятности и последствий всех выявленных рисков, применяя качественные и количественные методы оценки. Вероятность и последствия, связанные с внутренними (присущими природе процесса) и остаточными рисками должны определяться индивидуально, по категориям и на консолидированной основе.

РО 9.5. Реагирование нариски

Разработать и оказывать поддержку процессу реагирования на риски, предназначенному для минимизации рисков эффективными с точки зрения затрат методами на постоянной основе. Процесс реагирования на риски должен определить такие стратегии как избежание, минимизация, разделение или принятие рисков; а также установить связанные с ними ответственности и учитывать предельные уровни допустимых рисков.

РО 9.6. Поддержка и мониторинг плана обработки рисков

Установить приоритеты и спланировать контрольные мероприятия на всех уровнях для реализации должного реагирования на риски, включая определение затрат, выгод и ответственность исполнителей. Согласовать предлагаемые действия и принятие остаточных рисков, а также убедитесь, что назначенные мероприятия имеют своих владельцев. Наблюдать за исполнением планов и отчитываться перед высшим руководством в случае отклонений от плана.

ИЗ-	Вх-вдйЩ-ая информация
P01	Стратегический и тактические планы ИТ, портфель ИТ услуг
РО 10	План по управлению проектными 'рисками
DS2	<Риски в отношении поставщиков
DS4	Результаты гестов по обеспечению иепрерыснсн: ги ИТ серьисоп
СЙ5	Угрозы и уязвимости со стороны безопасности_____
ME	Ретрскпектинный анализ зенден-ции рисков и инцидентом
ME 4	Корпоративный подход («аппетит') к принятию ИТ рис кои

Результаты			В процессы				
Оценил рисков	P01	И4		DS 12 ME 4			
Отчетность в отношении рисков	ME 4						
Рукшчэдин.! гк) управлений рисками и сфере ИТ	РОб						
Планы действий в отношении Существую* щих ИТ рисков	P04	AIB					

Таблица ОУКИ

Функции —

Действия^_____

Оргавизовать **управление** рисками **(например, Оценки** рисков!

Обеспечить» понимание с ip<iiej ических целей бизнеса _____

Обеспечить понимание целей бизнес процессов_____

Опсн-цслин. внутренние цепи ИТ и иркшизоваш рисковую среду

Опрсделизь инциденты, связанные с цепями (некоторые инциденты относятся кбизнесу [бизнес —

У1; некотрр!;^: к ИТ 1ИТ — У, 6и)н« — JJJJ_____**

Оценить риски, связанные с инцидентами _____ _____

Оценить и выбрать меры реагирования на риски

Расставить приоритеты и «планировать контрольные мероприятия

Утвердит» и бюджетировать план обработки рисков

Осуществлять поддержку и мониторинг исполнения плана обработки рисков

В таблице ОУКИ показано, кто является Ответственным, Утверждающим, Консультирующим и/или Информированным

Цели и показатели

Поддерживать достижение ИТ целей.
Уточнить степень корпоративного воздействия рисков на ИТ цели и ресурсы
Осуществлять учет и защиту всех ИТ активов.

Устанавливав-

Уточнить и минимизировать вероятность и масштабы ущерба от ИТ рисков. Создать эффективные с точки зрения затрат планы обработки критичны» ИТ рисков.

Устанавливает

Полная интеграция управления рисками в процессы управления.
Проведение регулярных оценок рисков при участии высшего руководства и ключевых сотрудников. Выработка предложений и информи рование о планах противодействия существующим рискам.

Оценивает

Направляет

Оценивает

Доля критичных целей ИТ, охваченных оценкой рисков. Доля оценок ИТ рисков, интегрированных в рамкам подхода к оценке ИТ рисков.
направляет

Оценивает

Доля выявленных критических ИТ инцидентов, которые подверглись оценке.
Число вновь выявленных ИТ рисков (в сравнении с предыдущим периодом).
- **Число существенных инцидентов, слу чиашихся вследствие не выявленных рисков.**
- **Доля выявленных критичных ИТ рисков, в отношении которых разработаны планы действий.**

Доля ИТ бюджета, затраченного на мероприятия по управлению рисками (оценку и минимизацию).
Частота анализа процесса управления рисками.
Долн утвержденных оценок рисков.
Число отчетов по мониторингу рисков, подготовленных с утвержденной пери-ОДичнОСТьЮ-
Доля выявленных ИТ инцидентов в ходе оценки рисков. Доля планов по управлению рисками, утвержденных и принятых к исполнению

Модель зрелости

Управление процессом *«Оценка и управление ИТ рисками»* удовлетворяет следующим бизнес требованиям к ИТ *анализ и информирование об ИТ рисках и их потенциальном воздействии на бизнес процессы и цели* и соответствует характеристикам:

0. Несуществующий

Не проводится оценка рисков в отношении процессов и бизнес решений. Организация не учитывает возможные последствия для бизнеса, связанные с уязвимостями в системе

безопасности и неопределенностями проектов разработки. Процесс управления рисками не рассматривается как имеющий отношение к принятию решений по ИТ и оказанию ИТ услуг.

1. Начальный/Повторяющийся эпизодически и бессистемно

На ИТ риски обращают внимание от случая к случаю. Проводятся неформальные оценки рисков, определяемые каждым отдельным проектом. Как правило, оценки рисков иногда включаются отдельно в план выполнения проекта, но ответственность за их проведение редко возлагается на конкретных менеджеров. Специфические риски, относящиеся к ИТ, такие как безопасность, достоверность и целостность, иногда учитываются при выполнении отдельных проектов. Информационные риски, влияющие на текущую операционную деятельность, иногда обсуждаются на совещаниях руководства. Если риски учитываются, то меры по их минимизации непоследовательны. Возникает понимание того, что ИТ риски важны и должны учитываться.

2. Повторяющийся, но интуитивный

Рекомендации по управлению

Реализация существующего подхода к оценке рисков на практике отдана на усмотрение отдельных руководителей проектов. Оценка рисков общего уровня обычно проводится только для крупных проектов или при решении возникших проблем. Начинается внедрение процессов минимизации выявленных рисков.

3. Определенный

Политика управления рисками в масштабе организации определяет, когда и как проводить оценки рисков. Оценка рисков выполняется в соответствии с определенным и документально оформленным процессом. Обучение по проблемам управления рисками доступно всему персоналу. Решения в рамках процесса управления рисками и обучения оставлены на усмотрение сотрудников. Разработанная методология является убедительной и вполне приемлемой и гарантирует, что основные риски для данного бизнеса будут выявлены. Процесс минимизации основных рисков, как правило, начинает реализовываться только после выявления рисков. Описания должностных обязанностей включают разделы по управлению рисками.

4. Управляемый и измеряемый

Оценка и управление рисками являются стандартными процедурами. Об отклонениях в процессе управления рисками информируется руководство ИТ. Ответственность за управление рисками возложено на высшее руководство организации. Оценка и минимизация рисков проводятся на уровне отдельных проектов и также регулярно в отношении деятельности ИТ в целом. Руководству даются рекомендации по изменениям корпоративной среды и среды ИТ, которые могли бы значительно повлиять на сценарии рисков. Руководство может контролировать текущее состояние организации с точки зрения рисков и принимать взвешенные решения в отношении того риска, который оно готово принять. Все выявленные риски имеют номинальных владельцев, а высшее руководство и руководители службы ИТ определили уровни риска, которые, по их мнению, являются допустимыми. Руководство службы ИТ разработало стандартизованные меры оценки рисков и соотношений риск-прибыль. Руководство предусматривает в бюджете средства для финансирования проектов управления операционными рисками с тем, чтобы регулярно проводить коррекцию оценок рисков. Сформирована база данных по управлению рисками, началась автоматизация части процессов управления рисками. Руководство службы ИТ вырабатывает стратегии минимизации рисков.

5. Оптимизированный

Оценка рисков доведена до уровня, когда в масштабе организации реализован структурированный и хорошо управляемый процесс. Лучшие практики применяется в масштабе всей организации. Процедуры сбора данных, анализа и отчетности в области управления рисками значительно автоматизированы. Используются рекомендации ведущих специалистов в этой области, служба ИТ принимает участие в работе отраслевых групп по обмену опытом. Процесс управления рисками полностью интегрирован в бизнес и ИТ деятельность, широко распространен, и в нем принимают широкое участие пользователи ИТ

услуг. Руководство выявляет случаи и принимает меры, когда важные операционные и инвестиционные решения в сфере ИТ принимаются без учета плана управления рисками. Руководство постоянно ведет оценку стратегий минимизации рисков.

РО 10. Управление проектами

Описание процесса

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 результатов по этапам, 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.

Результативность	П
Эффективность	П
Конфиденциальность	
Целостность	
Доступность	
Соответствие требованиям	
Достоверность	

Управление процессом

Управление проектами.

удовлетворяет следующим бизнес требованиям к ИТ

получение результатов проектов согласно принятым ранее срокам, бюджету и уровню качества. **сосредоточено на**

определении подхода к управлению программами и проектами, который применим в сфере ИТ и обеспечивает участие и мониторинг рисков и результатов со стороны заинтересованных сторон. **достигается с помощью**

- Определения и применения методологии управления проектами и программами.
- Разработки руководств по управлению проектами.
- Управления каждым проектом, включенным в портфель проектов. **результаты оцениваются с помощью следующих показателей**
- Доля проектов, соответствующих ожиданиям заинтересованных сторон (с учетом значимости их мнений в отношении сроков, бюджета и соответствий требованиям).
- Доля проектов, в отношении которых проведен анализ результатов после внедрения.
- Доля проектов, соответствующих стандартам и практике в области управления проектами.

Приложения	+
Информация	
Инфраструктура	+
Персонал	+

Цели контроля

РО 10.1. Методологияуправления программами

Осуществить поддержку программы проектов, связанных с ИТ инвестициями, путем определения, оценки, расстановки приоритетов, отбора, предложения, управления и контроля над проектами. Следует убедиться, что проекты соответствуют целям программ. Координировать деятельность и взаимосвязи между различными проектами, управлять участием проектов в достижении запланированных результатов программы и разрешать конфликты, вызванные ресурсными требованиями.

РО 10.2. Методологияуправления проектами

Разработать и поддерживать методологию управления проектами, которая определяет масштаб и границы управления проектами, а так же конкретные методы, которые могут быть адаптированы

для каждого отдельного проекта. Методология и методы должны быть интегрированы в программу управления процессами.

РО 10.3. Подход к управлению проектами

Разработать управленческий подход, адекватный масштабам, сложности и нормативным требованиям, предъявляемым к каждому из проектов. Структура управления проектами может включать описание должностных обязанностей исполнителей и отчетность перед спонсором программы, самих спонсоров, управляющий комитет, проектный офис и руководителя проекта, а также механизмы, посредством которых каждый из них реализует свои задачи (такие как отчетность и анализ результатов этапов проекта). Необходимо убедиться в том, что все ИТ проекты имеют спонсоров с полномочиями, достаточными для самостоятельной реализации проектов в рамках общей стратегической программы.

РО 10.4. Комитет представителей заинтересованных сторон

Следует заручиться поддержкой и участием заинтересованных сторон в определении и реализации проекта в контексте общей инвестиционной программы, связанной с ИТ. ***РО 10.5. Представления о масштабах проекта***

Определить и документально зафиксировать представления о характере и масштабах проекта, для того, чтобы утвердить среди заинтересованных сторон общее понимание о проекте и его связях с другими проектами в рамках общей инвестиционной программы ИТ. Данное определение должно быть формально утверждено спонсорами программы и проекта до начала работ.

РО 10.6. Выделение фазреализации проекта

Выделить основные фазы при реализации проекта и проинформировать заинтересованные стороны об этом. Основанием для определения фаз должны служить программные руководящие решения. Выделение последующих фаз должно происходить на основе анализа и утверждения результатов предыдущей фазы, переоценки требований и бизнес обоснований, а также анализа хода реализации программы. В случае наложения фаз реализации проекта утверждение результатов должно проводиться совместно спонсорами проекта и программы.

РО 10.7. Интегрированный план проекта

Следует иметь формализованный и утвержденный интегрированный план проекта (охватывающий бизнес и ресурсы ИТ), чтобы направлять ход реализации проекта и осуществлять контроль в течение всего срока его исполнения. Действия и взаимозависимости различных проектов в рамках одной программы должны быть осознаны и документально зафиксированы. План проекта должен корректироваться в течение всего срока реализации проекта. План проекта и внесенные в него изменения должны быть одобрены и утверждены в соответствии с методологией управления программой и проектом. ***РО 10.8. Ресурсы проекта***

Определить ответственных лиц, взаимосвязи, права и критерии оценки в отношении членов проектной группы, определить подход к наёму и назначению компетентных сотрудников и/или контракторов проекта. Для достижения целей проекта, в соответствии с корпоративной практикой закупок, должны планироваться и осуществляться необходимые закупки продуктов и услуг.

РО 10.9. Управлениерисками проекта

Устранить или минимизировать специфические для каждого конкретного проекта риски посредством систематического планирования, определения, анализа, мониторинга и контроля определенных областей или событий, которые обладают нежелательным потенциалом. Риски, угрожающие управлению проектом и его целям, должны быть определены и централизованно документированы.

РО 10.10. План обеспечения качества проекта

Подготовить план управления качеством, в котором будет описана система качества проекта и ее реализация на практике. План должен быть изучен и согласован всеми сторонами, участвующими в интегрированном плане проекта.

РО 10.11. Контроль за внесением изменений в проект

Разработать систему контроля за внесением изменений для каждого проекта, чтобы все изменения, касающиеся основ проекта (стоимости, графика, масштабов, качества) были изучены, утверждены и включены в интегрированный план проекта в соответствии с методологией управления программой и проектом.

РО 10.12. Планирование обеспечения достаточной уверенности в отношении качества внедряемых систем

Методы получения достаточной уверенности в отношении качества новых или модифицированных внедряемых систем должны быть определены еще на начальной стадии управления проектом и включены в интегрированный план. Нужно добиться уверенности в том, что характеристики безопасности внутреннего контроля отвечают установленным требованиям.

РО 10.13. Оценкаэффективности проекта, отчетность и мониторинг

Следует оценивать эффективность проекта по охвату, срокам реализации, качеству, затратам и рискам. Выявлять все отклонения от плана. Следует оценивать влияние отклонений для проекта и программы в целом и отчитываться о результатах перед заинтересованными сторонами. Необходимо рекомендовать, реализовывать и анализировать корректирующие действия, в соответствии с методологией управления программой и проектом.

РО 10.14. Завершение проекта

Следует требовать, чтобы по завершению проекта заинтересованные стороны оценили, достиг ли проект поставленных целей и выгод. Определить и проинформировать о всех значительных действиях по достижению запланированных результатов проекта и выгод программы, а также выявить и документировать опыт, полезный для будущих проектов и программ.

Рекомендации по управлению

РО 1 Портфель ИТ проектор
one Юбновлениый портфель ИТ [5] .проектов
Матрица навыков ИТ
РО Стандарты разработки
7 AI 7 Обзор результатов внедрения

	В процессе						
Отчеты об эффективмоои проема	**ME1**						
Плои управления рисками проекта	**га 9**						
Руководящиеукамния по проекту	**AI1-A17**						
Детальные планм проемов	**Р0 8**	**АП_А17**					
Обновленный портфель ИТ проектов	**РО 1**	**РО 5**					

Таблица ОУКИ

Действия ↓ Функции →	Президент	Финансовый директор	Высшие руководители	Директор по ИТ	Владелец бизнес процесса	Руководитель эксплуатации систем	Главный архитектор ИТ систем	Руководитель разработок	Руководитель администрации ИТ	Руководитель проектного офиса	Аудит, риски, безопасность
Определить методологию управления проектами/программами для ИТ инвестиций	К	К	У	О						К	К
Создать и поддерживать методологию управления ИТ проектами	И	И	И	У/О	И	К	К	К	К	О	К
Организовать и вести мониторинг ИТ проектов, измерений и системы управления	И	И	И	О		К	К	К	К	У/О	К
Создать описания проектов, план-графиков, планов качества, бюджетов, планов информирования и управления рисками			К	К	К	К	К	К	К	У/О	К
Обеспечить участие заинтересованных сторон проекта	И		У	О	К						К
Осуществлять эффективный контроль над проектами и внесениями изменений в проекты			К	К		К	К	К		У/О	К
Определить и реализовать методы анализа результатов проекта			И	К				И		У/О	К

В таблице ОУКИ показано, кто является Ответственным, Утверждающим, Консультирующим и/или Информированным

Цели и показатели

Модель зрелости

Управление процессом *«Управление проектами»* удовлетворяет следующим бизнес требованиям к ИТ *получение результатов проектов согласно принятым ранее срокам, бюджетуи уровню качества* и соответствует характеристикам:

0. Несуществующий

Не применяются методы управления проектами, и организация не учитывает последствия для бизнеса, связанные с плохим управлением проектами и неудачами при разработке проектов.

1. Начальный/Повторяющийся эпизодически и бессистемно

Решение о применении методов управления проектами в рамках ИТ оставлено на усмотрение отдельных ИТ менеджеров. Недостаточны степень приверженности руководства и ответственность за выполнение проектов. Важные решения по управлению проектами принимаются без участия руководства пользователей или мнения заказчиков. Участие заказчиков и пользователей в разработке проектных заданий для информационных проектов ограничено или отсутствует вообще. Нет четкой организации в рамках информационных проектов. Не определены функции и обязанности. Плохо определены (если вообще определены) план-графики и основные этапы в реализации проектов. Не отслеживаются сроки выполнения и затраты по проектам, а последние не сравниваются с утвержденными бюджетами.

2. Повторяющийся, но интуитивный

Высшее руководство осознает необходимость управления ИТ проектами и информируют об этом персонал. Организация находится в процессе разработки и применения некоторых процедур и методов от проекта к проекту. В ИТ проектах не формализованы технические и бизнес цели. Участие заинтересованных сторон в управлении ИТ проектами ограничено. Разработаны первичные рекомендации по многим аспектам управления проектами, однако их применение оставлено на усмотрение отдельных менеджеров проектов.

3. Определенный

Процесс и методология управления ИТ проектами внедрены в организацию и о них проинформирован персонал. Проектные задания для ИТ проектов разрабатываются с учетом соответствующих технических и бизнес целей. Высшее руководство организации и службы ИТ начинает участвовать в управлении ИТ проектами. В рамках службы ИТ создано подразделение по руководству проектами, определены функции и обязанности исполнителей. Осуществляется мониторинг ИТ проектов, утверждены и корректируются этапы выполнения, план-графики и процедуры оценки хода работ и выполнения бюджета. На основе личной инициативы отдельных сотрудников проводится обучение по вопросам управления проектами. Определены процедуры управления качеством и работы по результатам внедрения систем, однако пока они широко не применяются ИТ менеджерами. Управление проектами начинает осуществляться в виде управления группами (портфелями) проектов.

4. Управляемый и измеряемый

Руководство требует, чтобы после завершения проектов проводилось рассмотрение их формальных и стандартизированных показателей и извлеченных из их выполнения уроков. Уровень

управления проектами измеряется и оценивается в рамках всей организации, а не только в пределах службы ИТ. Усовершенствования, вносимые в процесс управления проектами, оформляются документально и доводятся до сведения заинтересованных сторон, а члены проектной группы при этом повышают свою квалификацию. Руководство службы ИТ внедряет организационную структуру управления проектами, имеющую документированные должностные обязанности, ответственности и критерии оценки эффективности работы персонала. Определены критерии оценки выполнения плановых показателей каждого контрольного этапа. До, в процессе и после реализации проектов проводится оценка и управление затратами и рисками. Все в большей степени ИТ проекты учитывают цели всей организации, а не только сугубо информационные задач. Существует последовательная и активная поддержка реализации проектов со стороны высшего руководства и заинтересованных сторон. Подразделение по управлению проектами и служба ИТ готовят программы обучения по вопросам управления проектами для персонала.

5. Оптимизированный

Внедрена и встроена в практику деятельности всей организации проверенная методология управления проектами на всем жизненном цикле. Осуществляется постоянный анализ и использование лучших практик. Сформулирована и внедрена ИТ стратегия в отношении аутсорсинга на этапах разработки и эксплуатации. Ответственность за проекты и программы, от начала до анализа их результатов, возложена на проектный офис. Планирование проектов и программ в масштабе организации позволяет наилучшим образом использовать ресурсы пользователей и ИТ-ресурсы для поддержки стратегических инициатив.

Приобретение и внедрение

AI 1. Выбор решений по автоматизации

Описание процесса

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.

Управление процессом

Выбор решений по автоматизации

удовлетворяет следующим бизнес требованиям к ИТ

преобразование требований бизнеса в отношении функциональности и контроля в эффективный дизайн автоматизированных решений. **сосредоточено на**

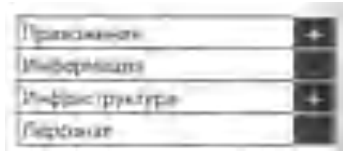
определении технически обоснованных и эффективных с точки зрения затрат решений.

достигается с помощью

- Определения бизнес и технических требований.
- Проведения исследования обоснованности в соответствии со стандартами разработки.
- Утверждения (или отмены) требований и результатов технико-экономического обоснования.

результаты оцениваются с помощью следующих показателей

- Доля проектов, в которых не были достигнуты заявленные выгоды по причине неверных оценок осуществимости.
- Доля технико-экономических обоснований, утвержденных владельцем бизнес процессов.
- Доля пользователей, удовлетворенных реализованной функциональностью.



Цели контроля

AI 1.1. Определение и поддержка бизнес требований к функциональности

Определить и выстроить приоритеты, уточнить и согласовать бизнес требования к функциональности, охватывающие весь перечень инициатив, необходимых для достижения ожидаемых результатов программы ИТ инвестиций.

AI 1.2. Результаты анализа рисков

Выявить, документировать и проанализировать риски, связанные с реализацией бизнес требований и разработкой решений в рамках общекорпоративного процесса разработки требований.

AI 1.3. Исследование обоснованности и разработка альтернативного плана действий

Провести исследование обоснованности для проверки возможности реализации требований. Корпоративное руководство, при содействии службы ИТ, должно оценить обоснованность и альтернативные планы действий, а также выработать рекомендации со стороны бизнеса.

AI 1.4. Требования, обоснование иутверждение

Следует убедиться, что процесс предполагает утверждение со стороны корпоративного спонсора и подписание им бизнес требований к функциональности, а также результатов исследования обоснованности на заранее определенных ключевых этапах. Корпоративный спонсор должен принять окончательное решение с учетом сделанного выбора и подхода к приобретению.

Рекомендации по управлению

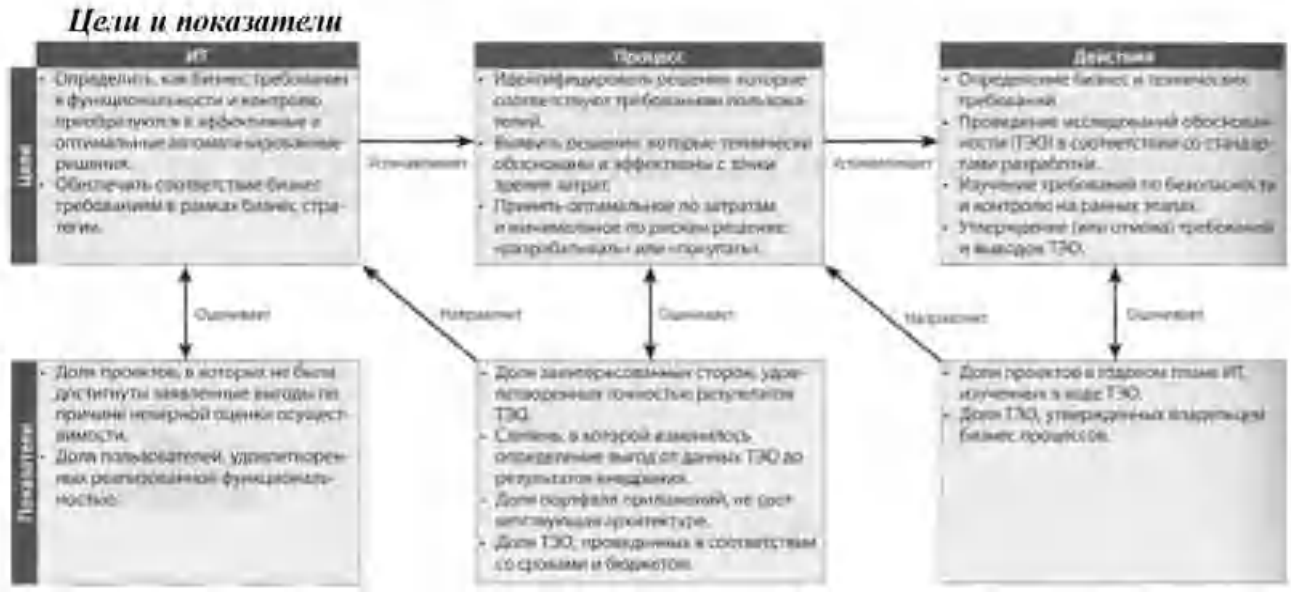
Из	Входящая информация
PO 1	Стратегический и тактические планы ИТ
PO 3	Регулярные обновления состояния технологий; технологические стандарты
PO 6	Стандарты в области приобретения и разработки
PO 10	Рекомендации по управлению проектами и детальные планы проектов
AI 6	Описание процесса управления изменениями
DS 1	Соглашения об уровне сервисов
DS 3	Требования плана по эффективности и объему

Результаты	В процессы						
Обоснование бизнес требований (ТЭО)	PO 2	PO 5	PO 7	AI 2	AI 3	AI 4	AI

Таблица ОУКИ

Действия ↓ Функции →	Президент	Финансовый директор	Высший руководитель	Директор по ИТ	Владелец бизнес процесса	Руководитель инструкций системы	Главный архитектор ИТ систем	Руководитель разработок	Руководитель администрации ИТ	Руководитель проектного офиса	Другие должности
Определить бизнес требования в отношении функциональности и технические требования			К	К	О	К	О	О		У/О	И
Обеспечить процессы по сбору и целостности требований				К		К		И		У/О	К
Определить, документировать и анализировать риски в бизнес процессах			У/О	К	О	О	К	О		О	К
Оценить осуществимость реализации предлагаемых бизнес требований			У/О	О	О	К	К	К		О	К
Оценить операционные ИТ преимущества предлагаемых решений		И	О	У/О	О	И	И	И	И	О	
Оценить преимущества для бизнеса от предлагаемых решений			У/О	О		К	К	К		О	
Разработать процесс утверждения требований			К	У		К	К	К		О	К
Утвердить и подписать предлагаемые решения		К	У/О	О	О	К	К	К	И	О	К

В таблице ОУКИ показано, кто является Ответственным, Утверждающим, Консультирующим и/или Информированным



Модель зрелости

Управление процессом *«Выборрешений по автоматизации»* удовлетворяет следующим бизнес требованиям к ИТ *преобразование требований бизнеса в отношении функциональности и контроля в эффективный дизайн автоматизированных решений* и соответствует характеристикам:

0. Несуществующий

Организация не нуждается в выявлении функциональных или операционных требований к процессам разработки, внедрения или модификации решений, относящихся к системам, услугам, инфраструктуре, программным средствам и данным. Организация не интересуется имеющимися на рынке технологическими решениями, потенциально пригодными для ее деятельности.

1. Начальный/Повторяющийся эпизодически и бессистемно

Осознается необходимость сформулировать требования и идентифицировать технологические решения. Группы сотрудников совместно обсуждают потребности на неформальном уровне, требования лишь изредка документируются. Решения идентифицируются отдельными сотрудниками на основе ограниченной информации о рынке или в ответ на предложения поставщиков. Структурированный анализ или исследования имеющихся технологий проводятся в незначительном объеме.

2. Повторяющийся, но интуитивный

Различные подходы к поиску ИТ решений, основанные на интуиции, существуют и разнятся в рамках организации. Решения выбираются неформально, на основе опыта и знаний сотрудников службы ИТ. Успех каждого проекта зависит от квалификации нескольких ведущих сотрудников. Качество документации и принимаемых решений меняется в значительных пределах. Применяется неструктурированный подход к определению требований и поиску технологических решений.

3. Определенный

Существует четкий, структурированный подход при выборе ИТ решений. Данный подход требует рассмотрения альтернативных вариантов с учетом бизнес или пользовательских требований, технологических и экономических возможностей, оценок рисков и других факторов. Процесс выбора ИТ решений применяется в рамках некоторых проектов на основе таких факторов, как решения, принятые участниками проекта, количество времени, уделяемого руководством, а также масштаб и приоритеты исходного

бизнеса-требования. Для определения требований и выбора ИТ решений применяются структурированные подходы.

4. Управляемый и измеряемый

В большинстве проектов существует и применяется утвержденная методология определения и оценки ИТ решений. Проектная документация обладает хорошим качеством, каждый этап процесса должным образом утверждается. Требования хорошо сформулированы и соответствуют предварительно установленным структурам. Изучаются альтернативные решения, в том числе с помощью анализа затрат и выгод. Методология является понятной, хорошо определенной и поддающейся оценке. Существует четко определенное взаимодействие между руководством ИТ и корпоративным руководством в вопросах определения и оценки ИТ решений.

5. Оптимизированный

Методология определения и оценки ИТ решений непрерывно совершенствуется. Методология приобретений и внедрения обладает гибкостью, делающей ее пригодной для использования как в крупных, так и небольших проектах. Эта методология поддерживается внутренней и внешними базами знаний, содержащих справочные материалы по технологическим решениям. Данная методология сама формирует документацию по предопределенной структуре, что делает эксплуатацию и техническое обслуживание решений эффективным. Происходит выявление новых возможностей технологии для повышения конкурентоспособности, влияния на перестройку бизнес-процессов и улучшение общей эффективности. Руководство выявляет случаи и принимает меры, когда ИТ решения принимаются без анализа альтернативных технологий или функциональных бизнес требований.

AI 2. Приобретение и поддержка программных приложений

Описание процесса

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.

Результативность	П
Эффективность	П
Конфиденциальность	
Целостность	В
Доступность	
Соответствие требованиям	
Достоверность	В

Управление процессом

Приобретение и поддержка программных приложений.

удовлетворяет следующим бизнес требованиям к ИТ

обеспечение соответствия доступных приложений требованиям бизнеса, при условиях своевременности и разумных затрат. **сосредоточено на**

своевременном и эффективном с точки зрения затрат процессе разработки.

достигается с помощью

- Преобразования требований бизнеса в спецификации разработки.
- Соблюдения стандартов разработки для всех модификаций.
- Разделения работ по разработке, тестированию и сопровождению. **результаты оцениваются с помощью следующих показателей**
- Число проблем в расчете на приложение, приводящих к ощутимым простоям.
- Доля пользователей, удовлетворенных реализованной функциональностью.

Цели контроля

AI 2.1. Общий дизайн приложений

Преобразовать бизнес требования в спецификации общего характера на приобретение программного обеспечения, с учетом направления технологического развития организации и информационной архитектуры. Утвердить спецификации у руководства, чтобы быть уверенным в том, что общий дизайн приложения соответствует требованиям. Провести пересмотр дизайна в случае существенных технических или логических несоответствий, выявленных в процессе разработки или эксплуатации.

AI 2.2. Детальный дизайн приложений

Подготовить детальный дизайн приложения и технические требования к программному обеспечению. Определить критерии приемки этих требований. Утвердить требования, чтобы быть уверенным в том, что они соответствуют общему дизайну приложения. Провести пересмотр дизайна в случае существенных технических или логических несоответствий, выявленных в процессе разработки или эксплуатации.

AI 2.3. Меры контроля приложений и проверяемость

Внедрить меры контроля бизнес-процессов там, где это необходимо, в форме мер контроля программных приложений, чтобы обработка данных была точной, своевременной, санкционированной и проверяемой.

AI 2.4. Безопасность приложений и доступность

Обратить внимание на 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.

AI 2.5. Конфигурирование и внедрение приобретенного программного обеспечения

Провести конфигурирование и внедрить приобретенное программное обеспечение, чтобы оно соответствовало бизнес целям.

AI2.6. Значительные обновления существующих систем

В случае значительных изменений в существующих системах, которые отразятся на текущей архитектуре приложений и/или функциональности, следовать тем же процедурам процесса разработки, как и в случае с полностью новыми системами.

AI 2.7. Разработка программных приложений

Следует убедиться в том, что автоматизированная функциональность разрабатывается в соответствии с проектными спецификациями, стандартами разработки и документации, требованиями системы обеспечения качества и утвержденными стандартами. Проверить, что все нормативные и договорные аспекты выявлены и изучены применительно к приложениям, разработанным третьими сторонами.

AI 2.8. Обеспечение качества приложений

Разработать, обеспечить ресурсами и реализовать на практике план по обеспечению качества с тем, чтобы качество соответствовало определенным требованиям, а также политике и процедурам организации в этой области.

AI 2.9. Управление требованиями к приложениям

Отслеживать статус конкретных требований (включая все отвергнутые требования) в процессе проектирования, разработки и внедрения, проводить утверждение требований в соответствии с установленным процессом управления изменениями.

AI 2.10. Поддержка приложений

Разработать стратегию и план поддержки приложений.

Рекомендации по управлению

Из	Входящая информация
PO 2	Справочник данных, схема классификации данных, оптимизированный план бизнес-систем
PO 3	Регулярные обновления текущего состояния развития технологий
PO 5	Отчеты о затратах и выгодах
PO 8	Стандарты в области приобретения и разработки
PO 10	Рекомендации по управлению проектами, детальные планы проектов
AI 1	Исследование обоснованности бизнес-требований (ТЭО)
AI 6	Описание процесса внесения изменений

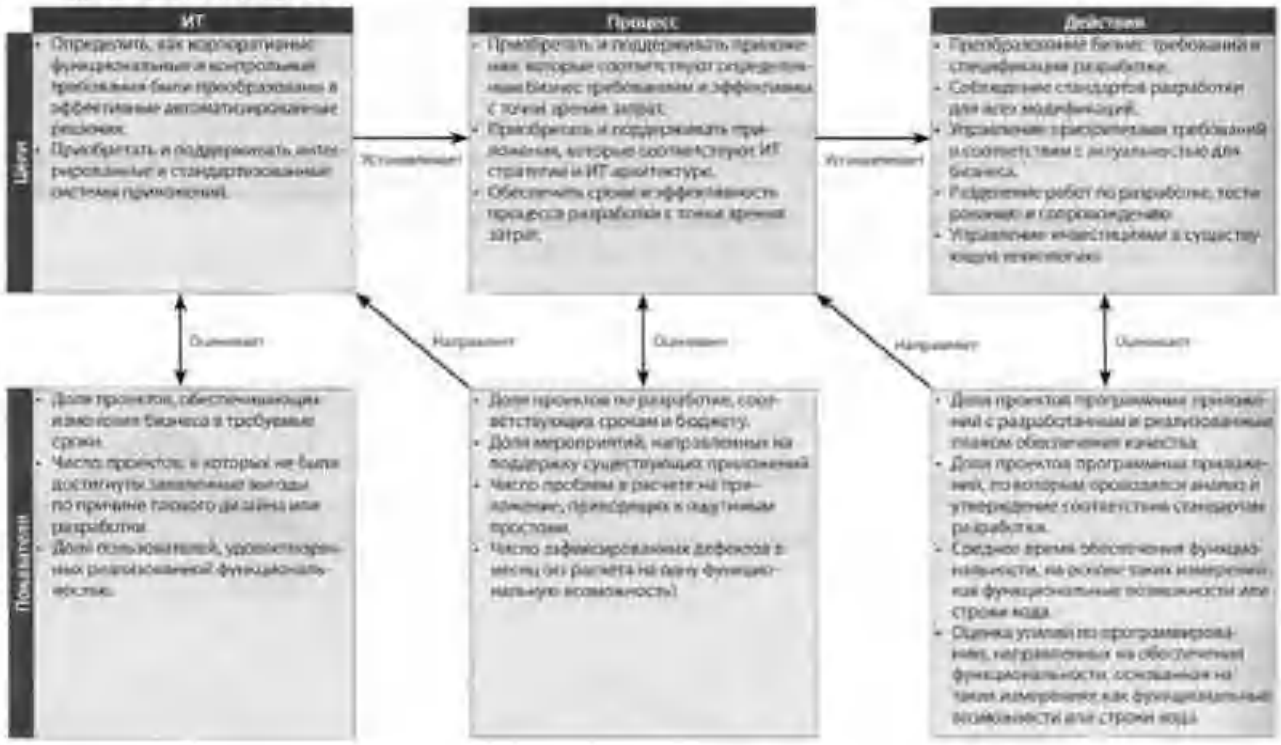
Результаты	В процессы						
Спецификации мер контроля безопасности приложений	DS 5						
Знания в области приложений и программных пакетов	AI 4						
Решения по закупкам	AI 5						
Первоначальные запланированные соглашения об уровне сервиса	DS 1						
Спецификации по доступности, непрерывности и восстановлению	DS 3	DS 4					

Таблица ОУКИ

Действия ↓ / Функции →	Президент	Финансовый директор	Высшее руководство	Директор по ИТ	Владелец бизнес-процесса	Руководитель эксплуатации систем	Главный архитектор ИТ-систем	Руководитель разработок	Руководитель администрации ИТ	Руководитель проектного офиса	Аудит, риски, безопасность
Преобразовать бизнес-требования в спецификации общего дизайна приложений					К		К	У/О		О	К
Подготовить детальный дизайн приложений и технические требования				И	К	К	К	У/О		О	К
Определить меры контроля рамках дизайна приложений					О	К		У/О		О	О
Настроить и внедрить функциональности					К	К		У/О		О	К
Разработать формализованную методологию и процессы управления разработкой приложений				К		К	К	У	К	О	К
Подготовить план обеспечения качества программного обеспечения					И		К	О		У/О	К
Управлять требованиями к приложениям и отслеживать их								О		У/О	
Подготовить план поддержки программных приложений				К		К		У/О		К	

В таблице ОУКИ показано, кто является Ответственным, Утверждающим, Консультирующим и/или Информированным

Цели и показатели



Модель зрелости

Управление процессом *«Приобретение и поддержка программных приложений»* удовлетворяет следующим бизнес требованиям к ИТ *обеспечение соответствия доступных приложений требованиям бизнеса, при условиях своевременности и разумных затрат* и соответствует характеристикам:

0. Несуществующий

Отсутствует процесс разработки и определения требований к приложениям. Обычно приложения приобретаются на основе предложений поставщиков, узнаваемости бренда или знакомства персонала ИТ с конкретными программными продуктами. При этом фактические требования анализируются мало или не рассматриваются совсем.

1. Начальный/Повторяющийся эпизодически и бессистемно

Осознаётся необходимость процесса приобретения и поддержки приложений. Подходы к приобретению и поддержке приложений варьируются от проекта к проекту. Некоторые разрозненные решения, относящиеся к отдельным требованиям бизнеса, как правило, приобретаются независимо друг от друга, что приводит к их неэффективности в эксплуатации и поддержке.

2. Повторяющийся, но интуитивный

Используются различные, но сходные процессы приобретения и поддержки приложений, основанные на опыте и квалификации внутри службы ИТ. Степень успешного применения приложений в значительной степени зависит от опыта и квалификации персонала ИТ. Сопровождение приложений обычно связано с проблемами, особенно при увольнении соответствующих специалистов из данной организации. Вопросам безопасности и доступности при разработке или приобретении программных приложений уделяется незначительное внимание.

3. Определенный

Существует четкий, определенный и понятный процесс приобретения и поддержки программных приложений. Данный процесс соответствует ИТ и корпоративной стратегии. Делаются попытки применения документированных процессов к различным приложениям и проектам. Методологии, как правило, недостаточно гибкие и трудно применимы ко всем случаям, поэтому отдельные этапы могут пропускаться. Работы по поддержке планируются, регламентируются и координируются.

4. Управляемый и измеряемый

Существует формализованная и хорошо понятная методология, которая включает документально оформленный процесс дизайна и разработки технических спецификаций, критерии приобретения программного обеспечения, процесс тестирования и требования к документации. Существуют регламентированные и согласованные механизмы, гарантирующие, что все этапы соблюдаются, а отклонения согласовываются с руководством. Практики и процедуры развиваются и хорошо подходят для организации, используются всеми сотрудниками и применимы к большинству требований, предъявляемых к приложениям.

5. Оптимизированный

Практики приобретения и поддержки приложений соответствуют заранее определенному процессу. Данный подход является компонентно-ориентированным, при этом предварительно заданные стандартизированные приложения согласованы с требованиями бизнеса. Этот подход применяется в рамках всей организации. Методология приобретения и поддержки приложений является достаточно разработанной, обеспечивает быстрое развертывание и высокую степень гибкости и адаптируемости к изменяющимся требованиям бизнеса. Методология приобретения и поддержки приложений непрерывно совершенствуется и поддерживается внутренними и сторонними базами знаний, содержащими справочные материалы и лучшими практиками. Данная методология создает документацию по предопределенной структуре, что делает эксплуатацию и сопровождение эффективными.

AI 3. Приобретение и обслуживание технологической инфраструктуры

Описание процесса

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. В таком случае можно говорить о постоянной технологической поддержке корпоративных приложений.

Управление процессом

Приобретение и обслуживание технологической инфраструктуры.

удовлетворяет следующим бизнес требованиям к ИТ

приобретение и поддержка интегрированной и стандартизованной **ИТ** инфраструктуры.

сосредоточено на

обеспечении подходящих платформ для корпоративных приложений в соответствии с определенной **ИТ** архитектурой и технологическими стандартами. **достигается с помощью**

- Создания плана приобретения технологий в соответствии с технологическим планом инфраструктуры.
- Планирования поддержки инфраструктуры.
- Внедрения мер внутреннего контроля, безопасности и проверяемых показателей.

результаты оцениваются с помощью следующих показателей

- Доля платформ, не соответствующих утвержденной **ИТ** архитектуре и технологическим стандартам.

- Число критичных бизнес процессов, обслуживаемых устаревшей (или устаревающей) инфраструктурой.
- Число компонентов инфраструктуры, которые более не подлежат поддержке (или не будут поддерживаться в недалеком будущем).

Цели контроля

AI 3.1. План приобретения технологической инфраструктуры

Разработать план приобретения, внедрения и поддержки технологической инфраструктуры, который бы соответствовал установленным корпоративным функциональным и техническим требованиям, а также направлению технологического развития организации.

AI 3.2. Защита и доступность ресурсов инфраструктуры

Внедрить меры внутреннего контроля, безопасности и проверяемые показатели в процессе конфигурирования, интеграции и обслуживания аппаратного и инфраструктурного программного обеспечения, чтобы защитить ресурсы и убедиться в доступности и целостности. Нужно четко определить и разъяснить должностные обязанности при использовании важных компонентов инфраструктуры тем сотрудникам, которые разрабатывают и интегрируют компоненты инфраструктуры. Должны проводиться мониторинг и оценка эксплуатации этих компонентов.

AI 3.3. Обслуживание инфраструктуры

Разработать стратегию и план обслуживания инфраструктуры и убедитесь, что изменения находятся под контролем в соответствии с принятой в организации процедурой управления изменениями. Включить в план периодические оценки соответствия потребностям бизнеса, управление обновлениями, стратегии обновления, риски, оценку уязвимостей и требования по безопасности.

AI 3.4. Тестовая среда

Создать среду разработки и тестовую среду для возможности тестирования целостности компонентов инфраструктуры.

Рекомендации по управлению

Из	Входящая информация	Результаты	В процессы
PO 3	План технологической инфраструктуры, стандарты и возможности; регулярное обновление текущего состояния технологии	Решения по закупкам	AI 5
		Конфигурационная система, которая должна быть протестирована/установлена	AI 7
PO 6	Стандарты в области приобретения и разработки	Требования к физической среде	DS 12
		Обновления технологических стандартов	PO 3
PO 10	Рекомендации по управлению проектами и детальные планы проектов	Требования системного мониторинга	DS 3
		Знания в области инфраструктуры	AI 4
AI 1	Обоснования бизнес требований (ТЭО)	Первоначально запланированные соглашения об уровне операционной поддержки	DS 1
AI 4	Описание процесса внесения изменений		
DS 3	Требования плана по эффективности и объему		

Таблица ОУКИ

Действия ↓ / Функции →	Президент	Финансовый директор	Высшее руководство	Директор по ИТ	Владелец бизнес процесса	Руководители эксплуатации систем	Главный архитектор ИТ систем	Руководитель разработок	Руководитель администрации ИТ	Руководитель проектного офиса	Аудит (учет, безопасность)
Определить процедуру процесс приобретений		Я		У		К	Я	Я	О		Б
Обсудить инфраструктурные требования с утвержденными поставщиками		К/И		У	И	О	К	Х	О		Б
Определить стратегию и план поддержки инфраструктуры				У		О	О	О	К		
Конфигурировать компоненты инфраструктуры				У		О	К				Я

В таблице ОУКИ показано, кто является Ответственным, Утверждающим, Консультирующим и/или Информированным

Цели и показатели

Приобретать и поддерживать интегрированную и стандартизованную ИТ инфраструктуру.
Оптимизировать ИТ инфраструктуру, ресурсы и возможности.
Обеспечить гибкость ИТ.

Устанавливает

Процесс

Обеспечить по[illegible]атформы для корпоративных приложений в соответствии с определенной ИТ архитектурой и технологическими стандартами.
Обеспечить надежную и безопасную ИТ | инфраструктуру.

Устанавливает

Действия

Создание плана приобретения технологий в соответствии с технологическим планом инфраструктуры.
Планирование поддержки инфраструктура
Обеспечение инфраструктуры среды разработки и тестирования. Внедрение мер внутреннего контроля, безопасности и проверяемых показателей.

Доля компонентов инфраструктуры приобретенных не в соответствии с процессом приобретения. Число компонентов инфраструктуры, которые более не подлежат поддержке (или не будут поддерживаться в недалеком будущем).

Оценивает

Число критичных бизнес процессов, обслуживаемых устаревшей (или устаревающей) инфраструктурой.

Направляет

Оценивает

Доля платформ, не соответствующих утвержденной ИТ архитектуре и технологическим стандартам. Число различных технологических платформ в организации в расчете на функцию.

Направляет Число и тип аварийных изменений в компонентах	инфраструктуры. Число нереализованных заявок на приобретения.	Среднее время конфигурирования компонентов инфраструктуры.

Модель зрелости

Управление процессом *«Приобретение и обслуживание технологической инфраструктуры»* удовлетворяет следующим бизнес требованиям к ИТ *приобретение и поддержка интегрированной и стандартизованной ИТ инфраструктуры* и соответствует характеристикам:

0. Несуществующий

Управление технологической инфраструктурой не признается как достаточно важный аспект, требующий рассмотрения.

1. Начальный/Повторяющийся эпизодически и бессистемно

В инфраструктуру вносятся изменения для каждого нового приложения без какого-либо общего плана. Хотя есть осознание того, что инфраструктура ИТ имеет важное значение, отсутствует общий непротиворечивый подход. Деятельность по поддержке вызвана реакцией на краткосрочные потребности. Тестирование проводится в среде промышленной эксплуатации.

2. Повторяющийся, но интуитивный

Имеется согласованность между тактическими подходами при приобретении и поддержании инфраструктуры ИТ. Приобретение и поддержка инфраструктуры ИТ не базируется на какой-либо определенной стратегии и не учитывает потребности корпоративных приложений, которые должны поддерживаться. Существует понимание того, что инфраструктура ИТ важна; данное понимание поддерживается некоторыми формальными практиками. Отдельные мероприятия по поддержке запланированы, но нет общего плана и координации. В некоторых случаях существует отдельная среда тестирования.

3. Определённый

Существует ясный, достаточно определенный и в целом понятный процесс приобретения и поддержки инфраструктуры ИТ. Данный процесс поддерживает потребности наиболее важных корпоративных приложений и согласован с корпоративной и ИТ стратегиями, но его применение происходит недостаточно единообразно. Мероприятия по поддержке планируются и координируются. Существуют отдельные среды для промышленной эксплуатации и тестирования.

4. Управляемый и измеряемый

Процесс приобретения и поддержания технологической инфраструктуры развит до уровня, когда он успешно применяется в большинстве ситуаций, последовательно соблюдается и направлен на многократное использование. Инфраструктура ИТ адекватно поддерживает бизнес-приложения. Процесс хорошо организован и работает на опережение. Затраты и время для достижения ожидаемого уровня масштабируемости, гибкости и интеграции отчасти оптимизированы.

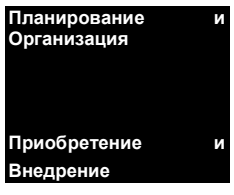
5. Оптимизированный

Процесс приобретения и поддержания технологической инфраструктуры является упреждающим и тесно увязан с наиболее важными корпоративными приложениями и технологической архитектурой. Применяются лучшие практики для принятия решений о выборе технологических решений; организация знает о новейших разработках платформ и системного программного обеспечения. Затраты снижены благодаря рационализации и стандартизации компонентов инфраструктуры и использованию автоматизации. Благодаря высокому уровню технической осведомленности можно определить оптимальные способы упреждающего повышения производительности, включая рассмотрение вариантов аутсорсинга. ИТ инфраструктура рассматривается как важный фактор, способствующий эффективному использованию ИТ.

AI4. Обеспечение выполнения операций

Описание процесса

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.



Результативность

Эффективность

Конфиденциальность

Целостность

Доступность

Соответствие требованиям

Достоверность

Управление процессом

Обеспечение выполнения операций.

удовлетворяет следующим бизнес требованиям к ИТ

обеспечение удовлетворенности конечных пользователей услугами и уровнем сервиса, а также гармоничная интеграция приложений и технологических решений с бизнес-процессами. **сосредоточено на**

обеспечении эффективной пользовательской и операционной документацией и учебными материалами для передачи знаний, необходимых для успешной эксплуатации систем. **достигается с помощью**

- Разработки и распространению документации, способствующей передаче знаний.
- Информирования и обучения пользователей, бизнес-менеджеров, обслуживающего и операционного персонала.
- Разработки учебных материалов.

результаты оцениваются с помощью следующих показателей

- Число приложений, в которых ИТ процедуры гармонично интегрированы с бизнес процессами.
- Доля владельцев бизнес-процессов, удовлетворенных учебными материалами и руководствами по эксплуатации приложений.
- Число приложений, подкрепленных адекватным обучением пользователей и

I **приоритетное** **Ы**

обслуживающего персонала.

Цели контроля

AI 4.1. Планирование для операционных решений

Разработать план по определению и документированию всех технических, операционных и пользовательских аспектов таким образом, чтобы все сотрудники, занятые применением и обслуживанием автоматизированных решений, могли исполнять свои обязанности.

AI 4.2. Передачазнаний бизнес-менеджерам

Передавать знания бизнес-менеджерам, чтобы позволить им осуществлять владение системами и данными, а также исполнять свои обязанности в части пользования ИТ сервисами, обеспечения качества, внутреннего контроля и управления приложениями.

AI 4.3. Передача знаний конечным пользователям

Передавать знания и навыки, чтобы дать возможность конечным пользователям эффективно и оптимально использовать системы для поддержки бизнес-процессов. ***AI 4.4. Передача знаний операционному и обслуживающему персоналу*** Передавать знания и навыки, чтобы дать возможность операционному и обслуживающему персоналу эффективно и оптимально оказывать услуги, поддерживать и обслуживать системы и связанную с ними инфраструктуру.

Рекомендации по управлению

PO10	Рекомендации по управлению проектами и детальные планы проектов
AI 1	Обоснование бизнес требовании ЯЭЙ _____
AI2	Знания в области приложении и пакетов программного обеспе чения _____
A| 3	Знания в области инфраструк ТУРЫ
AI 7	Известные и подтвержденные ошибки
05 7	Запрошенные обновления доку-ментации

Результаты	В процессы					
Руководства для пользователей, сис-темных администраторов, руководства службы технической поддержки	AI7	DS4	DSS	DS 9	DS11	DS 13
Требования по передаче знаний для внедрения решений	DS7					
Учебные матери.шм	DS7					

Таблица ОУКИ

Действия „

Функции —•	ИТ	Руководитель разработок	Аудит, риски, безопасность	Группа внедрения	Департамент обучения
Разрабатывать стратегию эксплуатации решения		О	И	О	К
Разрабатывать методологию передами знаний Разрабатывать руководства по процедурам для конечных пользователей				К	О
Р*i зрэблгыйлть техническую докууенгацию по эксплуатации и поддержке Разрабатывать и проводить обучение		О	К	К	
Оценивать результаты обучения и при необходимости обновлять документацию		К	К		У/О
		О			О
				О	О

В таблице ОУКИ показано, кто является Ответственным, Утверждающим, Консультирующим и/или Информированным

Цели и показатели

Обеспечить правильное использо-вание и эффективность приложений и технологических решений. Обеспечить удовлетворенности конечных пользователей предложением услуг и уровнями сервиса. Обеспечить гармоничную интстра цию приложении и бизнес процессов. Сократить уровень сбоев и передеде-лок в решениях и услугах.

УПЛОШТИПЛ*!

Обеспечить эффективные пользоиа тульские и операционные руководства и обучающие материал и по приложу миям и техническим решениям. Передавать знания, необходимые для успешной работы систем.
Уаараскзткз и распространение дону, ментацни. способствугйшеи передаче знаний.
^нормирование и обучение пользо-вателей, коргзоративного руководства, обслуживающего и операционного персонала.
Разработка обучающих материалов.

число приложении, в которых ИТ процедуры гармонично интегриро-ваны с бизнес-процессами. Доля владельцев бизнес-процессов, уцдалесворенных обучением и coriyu ı вующими материалами
Число инцидентов, вызванных недостаточной гилькиигельской и операционной документацией и обучением. Число запросов на обучение, удовлетворяемых службой поддержки. Уровень

удовлеиюренностм обучением и документацией, относящимися к пользовательским и операционным процедурам.
Уменьшение стоимости разработ-■и/поддержда пользовательской доку менгации. операционных процедур и обучающих материалов.
• Уровень посещаемости занятий по обучению пользователей и операторов по каждому приложению,

■ Временная злвержка между измене-ниями и обновлениями в программа)! обучения, процедурах и документации. Доступность, полнота и точность пользовательской и операционной документации
Число приложений, подкрепленных адекватным обучением пользователей и обслуживающего персонала.

Модель зрелости

Управление процессом *«Обеспечение выполнения операций»* удовлетворяет следующим бизнес требованиям к ИТ *обеспечение удовлетворенности конечных пользователей предложением услуг и уровней сервиса, а также гармоничная интеграция приложений и технологическихрешений с бизнес-процессами* и соответствует характеристикам:

0. Несуществующий

Отсутствует процесс, относящийся к подготовке документации для пользователей, руководств по эксплуатации и учебных материалов. Единственные материалы, которые существуют — те, которые поставляются с приобретаемыми продуктами.

1. Начальный/Повторяющийся эпизодически и бессистемно

Существует понимание того, что необходим регламентированный процесс подготовки документации. Документация изредка выпускается, но распространяется непоследовательно и доступна лишь отдельным группам. Большая часть документации и процедур устарели. Учебные материалы обычно представляют собой упрощенные схемы различного качества. Фактически отсутствует интеграция между процедурами по различным системам и бизнес подразделениям. Нет запроса от бизнес подразделений на разработку учебных программ.

2. Повторяющийся, но интуитивный

Используются схожие подходы к разработке документации и процедур, но они не базируются на каком-либо структурированном подходе или концепции. Отсутствует общий подход к разработке пользовательских и эксплуатационных процедур. Учебные материалы выпускаются отдельными сотрудниками или проектными группами, и их качество зависит от сотрудников, принимающих в этом участие. Уровень процедур и качества поддержки пользователей может меняться от плохого до очень хорошего при практическом отсутствии какого-либо их единообразия и интеграции в рамках всей организации. Проводится обучение пользователей, но отсутствует общий план мероприятий по обучению.

3. Определенный

Существует четко определенная, принятая и осознанная концепция подготовки документации для пользователей, инструкций по эксплуатации и учебных материалов. Процедуры хранятся и поддерживаются в библиотеке, и любой сотрудник может иметь к ним доступ. Корректировки документации и процедур делаются при появлении запросов. Доступ к процедурам возможен, в том числе, и в автономном режиме, и их выполнение

может быть обеспечено случае аварийных ситуаций. Существует процесс, который регламентирует, что процедуры обновления и учебные материалы являются неотъемлемой частью реализации проекта изменений. Несмотря на существование определенных подходов, фактическое содержание не отличается постоянством, поскольку отсутствует система контроля, обеспечивающая соблюдение стандартов. Пользователи неформально принимают участие в этом процессе. Автоматизированные инструментальные средства все шире используются при формировании и распространении процедур. Существует план обучения пользователей.

4. Управляемый и измеряемый

Существует определенная методология сопровождения процедур и учебных материалов, которую поддерживает руководство службы ИТ. Подход, выбранный для поддержки процедур и учебных материалов, охватывает все системы и бизнес подразделения, поэтому процессы можно рассматривать с точки зрения бизнеса. Процедуры и учебные материалы интегрированы и включают взаимосвязи. Существуют средства контроля для обеспечения соблюдения стандартов, процедуры разрабатываются и поддерживаются для всех процессов. Отзывы пользователей в отношении документации и обучения собираются и оцениваются в рамках постоянного процесса совершенствования. Документация и учебные материалы обычно поставляются с предсказуемым и достаточным уровнем достоверности и доступности. Возникает формализованный процесс использования автоматизированных методов создания документации и управления процедурами. Процесс автоматизированной разработки процедур все больше интегрируется с разработкой приложений, что способствует большей совместимости и улучшенному доступу пользователей. Обучение отражает потребности бизнеса. Руководство службы ИТ разрабатывает показатели в отношении создания и внедрение документации, учебных материалов и учебных программ.

5. Оптимизированный

Процесс разработки пользовательской и эксплуатационной документации постоянно совершенствует посредством применения новых инструментальных средств или методов. Материалы, относящиеся к процедурам и обучению, рассматриваются как постоянно развивающаяся база знаний, которая ведется в электронном виде с использованием современных технологий управления, организации делопроизводства и распространения, благодаря чему она оказывается доступной и удобной в сопровождении. Обновление документации и учебных материалов проводится с целью отражения организационных, операционных изменений и изменений в программном обеспечении. Разработка и внедрение документации и учебных материалов полностью интегрирована в процесс разработки требований к бизнес-процессам, благодаря чему обеспечивается поддержка требований в масштабе всей организации, а не только процедур, ориентированных на ИТ.

AI 5. Поставки ИТ ресурсов

Описание процесса

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 самого процесса приобретения. Соблюдение этих условий дает гарантии того, что организация обладает всеми необходимыми ИТ ресурсами в нужное время и эффективно с точки зрения затрат.

Управление процессом

Поставки ИТ ресурсов.

удовлетворяет следующим бизнес требованиям к ИТ

повышение эффективности вложений в ИТ и вклада ИТ в прибыльность бизнеса.

сосредоточено на

приобретении и поддержке навыков в области ИТ, которые соответствуют стратегии снабжения, интегрированной и стандартизованной ИТ инфраструктуре, а также на сокращении рисков, связанных с поставками. **достигается с помощью**

- Получения профессиональных консультаций по вопросам законодательства и договорного права.
- Определения процедур и стандартов в области снабжения.
- Поставок требуемого аппаратного и программного обеспечения и услуг в соответствии с определенными процедурами.

результаты оцениваются с помощью следующих показателей

- Число обсуждений, связанных с договорами на поставки.
- Объемы скидок от цены покупки.
- Доля заинтересованных сторон, удовлетворенных поставщиками.

Цели контроля

AI 5.1. Контроль за поставками

Разработать и следовать процедурам и стандартам, соответствующим общекорпоративному процессу осуществления поставок и стратегии в области приобретений при закупках ИТ инфраструктуры, аппаратного и программного обеспечения, а также услуг, необходимых организации.

AI 5.2. Управление контрактами с поставщиками

Установить процедуру по заключению, изменению и прекращению контрактов со всеми поставщиками. Данная процедура должна включать, как минимум, правовые, финансовые, организационные, документальные аспекты, а также вопросы эффективности, безопасности, интеллектуальной собственности, и прекращения ответственности и обязательств (включая вопросы штрафных санкций). Все контракты и изменения в них должны проходить согласование со стороны советников по правовым вопросам.

AI 5.3. Выбор поставщиков

Проводить отбор поставщиков в соответствии с рыночной и формализованной практикой, чтобы получить наиболее конкурентоспособное предложение согласно сформулированным требованиям. Требования должны быть оптимизированы с учетом предложений потенциальных поставщиков.

AI 5.4. Приобретение ИТ ресурсов

Обеспечить защиту и поддержку интересов организации во всех договорных соглашениях, связанных с приобретениями, включая права и обязательства сторон при поставках программного обеспечения, ресурсов для разработки, инфраструктуры и услуг.

Рекомендации по управлению

Из	Входящая информация
PO 1	Стратегия в области ИТ приобретений
PO 8	Стандарты в области приобретений
PO 10	Рекомендации по руководству проектами и детальные планы проектов
AI 1	Обоснование бизнес-требований (ТЭО)
AI 2-3	Решения по поставщикам
DS 2	Каталог поставщиков

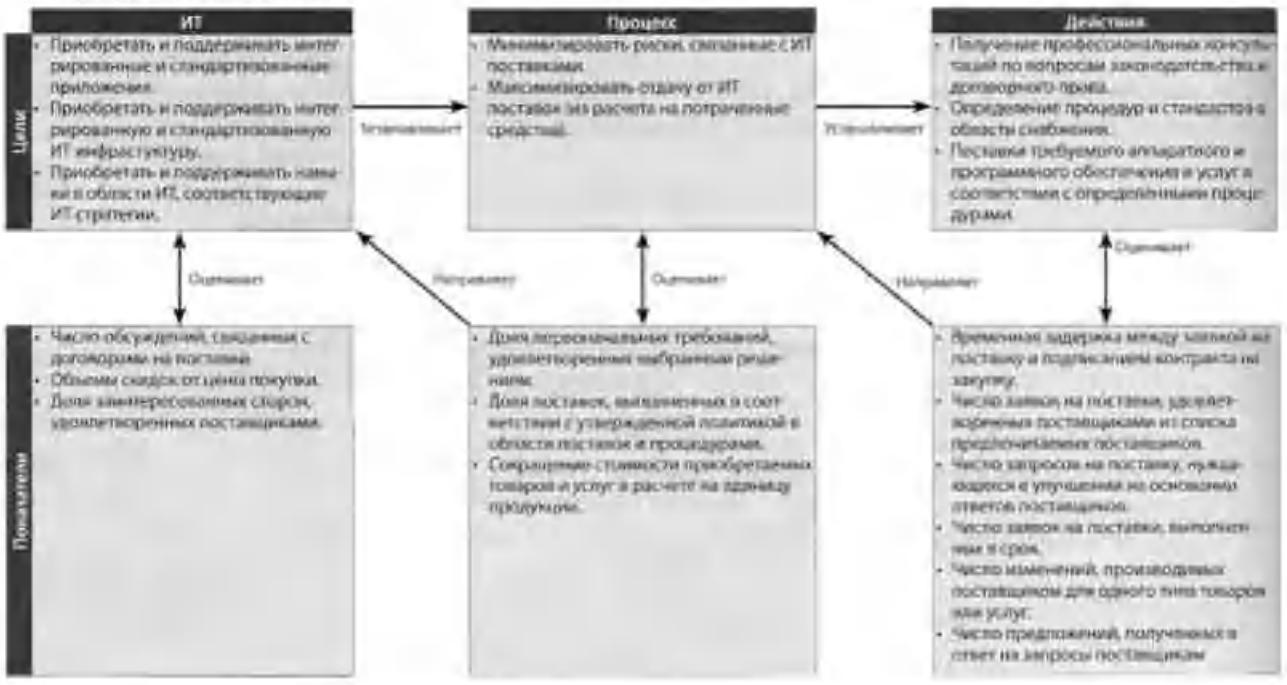
Результаты	В процессы						
Требования по управлению отношениями с третьими сторонами	DS 2						
Перечень закупок	AI 7						
Договорные соглашения	DS 2						

Таблица ОУКИ

Действия ↓ / Функции →	Президент	Финансовый директор	Высшее руководство	Директор по ИТ	Владелец бизнес-процесса	Руководитель эксплуатации систем	Главный архитектор ИТ-систем	Руководитель разработок	Руководитель администрирования ИТ	Руководитель проектного офиса	Аудит, риски, безопасность
Разрабатывать политики ИТ поставок и процедур, соответствующих корпоративной политике поставок	И	К		У		И	И	И	О		К
Создавать и поддерживать перечень аккредитованных поставщиков									К/О		
Оценивать и отбирать поставщиков через процесс запроса предложений	К	К		?		О		О	О	О	К
Разрабатывать контракты, защищающие интересы организации	О	К		У		О		О	О		К
Осуществлять поставки в соответствии с принятыми процедурами				?		О		О	О		К

В таблице ОУКИ показано, кто является Ответственным, Утверждающим, Консультирующим и/или Информированным

Цели и показатели



Модель зрелости

Управление процессом *«Поставки ИТ ресурсов»* удовлетворяет следующим бизнес требованиям к ИТ *повышение эффективности вложений в ИТ и вклада ИТ в прибыльность бизнеса* и соответствует характеристикам:

0. Несуществующий

Отсутствует определенный процесс поставки ИТ ресурсов. В организации не осознается необходимость четких политик и процедур в отношении поставок, обеспечивающих доступность, своевременность и эффективность с точки зрения затрат всех ИТ ресурсов.

1. Начальный/Повторяющийся эпизодически и бессистемно

В организации осознана потребность в документированных политиках и процедурах, которые связывают приобретения в сфере ИТ с общекорпоративным процессом поставок. Контракты на поставку ИТ ресурсов составляются и управляются руководителями проектов и другими сотрудниками, следующими скорее собственным суждениям, нежели формальным процедурам и политикам. Взаимоотношения между корпоративными поставками и управлением контрактами в ИТ возникают только в случае необходимости. Управление контрактами на поставки осуществляется на завершающей стадии проектов, а не на непрерывной основе.

2. Повторяющийся, но интуитивный

В организации присутствует понимание в необходимости наличия базовых политик и процедур в области закупок для ИТ. Политики и процедуры частично интегрированы в общекорпоративный процесс поставок. Процессы поставок в основном применяются для крупных и заметных проектов. Ответственности и отчетность в области ИТ поставок и управления контрактами определяются индивидуальным опытом менеджера, ответственного за контракты. Осознана важность управления взаимоотношениями с поставщиками; однако, этот процесс поддерживается на уровне личной инициативы. Процессы управления контрактами в основном применяются для крупных и заметных проектов.

3. Определенный

Руководство определило политики и процедуры в области ИТ закупок. Политики и процедуры соответствуют общекорпоративному процессу поставок. ИТ закупки в значительной мере интегрированы в общекорпоративную систему поставок. Существуют стандарты приобретения ИТ ресурсов. Поставщики ИТ ресурсов интегрированы в

механизмы корпоративного управления проектами в плане управления контрактами. Руководство службы ИТ сообщает о потребностях в определенных поставках и управлении контрактами в рамках службы ИТ.

4. Управляемый и измеряемый

ИТ приобретения полностью интегрированы в общекорпоративную систему поставок. ИТ стандарты для приобретения ИТ ресурсов применяются для всех поставок. Оценки управления контрактами и поставками адекватны экономическим обоснованиям ИТ закупок. Доступна отчетность по ИТ приобретениям. Руководство, как правило, информировано об отклонениях от политик и процедур ИТ приобретений. Развивается стратегическое управление взаимосвязями. Руководство ИТ распространяет процессы управления поставками и контрактами на все приобретения, отслеживая показатели эффективности.

5. Оптимизированный

Руководство осуществляет закупки ресурсов посредством процессов приобретений в сфере ИТ. Руководство обеспечивает выполнение требований политик и процедур в области ИТ приобретений. Оценки управления контрактами и поставками адекватны экономическим обоснованиям ИТ закупок. В течение продолжительного времени существуют налаженные отношения с большинством поставщиков и партнеров, качество этих отношений измеряется и отслеживается. Осуществляется стратегическое управление взаимоотношениями. Осуществляется стратегическое управление ИТ стандартами, политикой и процедурами в области приобретения ИТ ресурсов в соответствии с оценочным процессом. Руководство службы ИТ информирует о стратегической важности правильного процесса приобретения и управления контрактами в рамках службы ИТ.

AI 6. Управление внесением изменений

Описание процесса

Все изменения, включая обслуживание в аварийных ситуациях и исправления, относящиеся к инфраструктуре и приложениям в среде промышленной эксплуатации, должны управляться и контролироваться формализованным образом. Изменения (включая изменения в процедурах, процессах, системах и параметрах обслуживания) должны протоколироваться, оцениваться и санкционироваться до своего внедрения и анализироваться по плановым показателям после реализации. Это ведет к минимизации рисков негативного воздействия на стабильность и целостность среды промышленной эксплуатации.

Управление процессом

Управление внесением изменений.

удовлетворяет следующим бизнес требованиям к ИТ

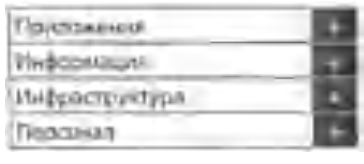
соответствие бизнес требованиям в русле корпоративной стратегии, при сокращении дефектов и переделок в решениях и услугах. **сосредоточено на**

оценке последствий, авторизации и внедрении всех изменений в ИТ инфраструктуру, приложения и технические решения; минимизации ошибок, возникающих по причине неполных спецификаций; предотвращении реализации неавторизованных изменений. **достигается с помощью**

- Определения и информирования о процедурах внесения изменений, включая аварийные изменения.
- Оценки, расстановки приоритетов и авторизации изменений.
- Мониторинга статуса и отчетность об изменениях. **результаты**

оцениваются с помощью следующих показателей

- Число сбоев и ошибок в данных, вызванных неточными спецификациями или неполной оценкой последствий.
- Количество переделок в приложениях или инфраструктуру, вызванных неверными спецификациями изменений.
- Доля изменений, которые производятся согласно формализованным процессам контроля.



Цели контроля

AI 6.1. Стандарты и процедуры изменений

Установить формализованные процедуры в области управления изменениями для стандартизованной обработки всех запросов (включая обслуживание и обновления) на изменения приложений, процедур, процессов, системных и сервисных параметров, а также образующих платформ.

AI 6.2. Оценка последствий, расстановка приоритетов и авторизация

Проводить оценку всех запросов на изменения в соответствии со структурным подходом, позволяющим определить последствия для системы промышленной эксплуатации и ее

функциональности. Следует убедиться, что все изменения категорированы, расставлены по приоритетам и авторизованы.

AI 6.3. Аварийные изменения

Установить процесс определения, заявления, тестирования, документирования, оценки и авторизации аварийных изменений, которые не обрабатываются в соответствии с принятым стандартным процессом изменений.

AI 6.4. Мониторинг и отчетность по статусу изменений

Установить систему мониторинга и отчетности для документирования не принятых изменений, информирования о статусе принятых, находящихся в процессе и завершенных изменений. Следует убедиться, что принятые изменения реализованы в соответствии с планом.

AI 6.5. Завершение изменений и документирование

Когда бы ни были реализованы изменения, следует обновлять связанную с ними системную и пользовательскую документацию, а также процедуры.

Рекомендации по управлению

Из	Входящая информация
PO 1	Портфель ИТ проектов
PO 8	Действия по повышению уровня качества
PO 9	Планы действий по минимизации ИТ рисков
PO 10	Рекомендации по руководству проектами и детальные планы проектов
DS 3	Требуемые изменения
DS 5	Требуемые изменения в области безопасности
DS 8	Запросы на обслуживание/ запросы на изменения
DS 9-10	Запросы на изменения (когда и как реализовать исправление)
DS 10	Журнал проблем

Результаты	В процессы						
Описание процесса изменений	AI 1 _ AI 3						
Отчеты о статусе изменений	ME 1						
Авторизация изменений	AI 7	DS 8	DS 10				

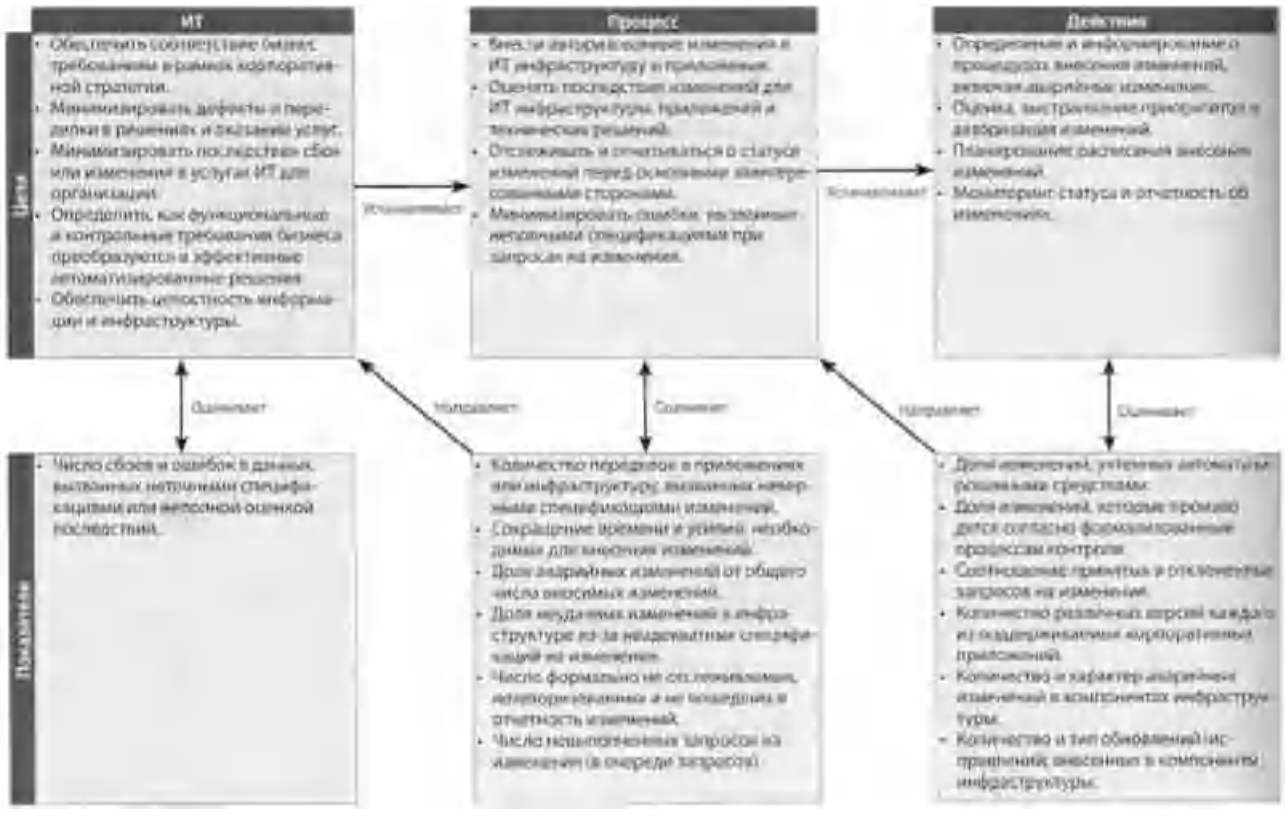
Таблица ОУКИ

Действия ↓ / Функции →	Президент	Финансовый директор	Высшее руководство	Директор по ИТ	Владелец бизнес процесса	Руководитель эксплуатации систем	Главный архитектор ИТ системы	Руководитель разработки	Руководитель администрации ИТ	Руководитель проектного офиса	Другие роли
Разрабатывать и реализовывать процесс постоянного учета, оценки и расстановки приоритетов в запросах на изменения				У	И	О	К	О	К	К	К
Оценивать последствия и расставлять приоритеты в изменениях на основе требований бизнеса				И	О	У/О	К	О	К	О	К
Обеспечивать соответствие аварийным и критическим изменениям утвержденному процессу				И	И	У/О	И	О			+
Утверждать изменения				И	К	У/О		О			
Управлять знаниями информацией об изменениях и распространять ее				У	И	О	К	О	И	О	К

В таблице ОУКИ указаны, кто должен быть Ответственным, Утверждающим, Консультирующим и/или Информированным

Модель зрелости

Цели и показатели



Управление процессом *«Управление внесением изменений»* удовлетворяет следующим бизнес требованиям к ИТ *соответствие бизнес требованиям в русле корпоративной стратегии, при сокращении дефектов и переделок в решениях и услугах* и соответствует характеристикам:

0. Несуществующий

Отсутствует регламентированный процесс управления изменениями, и изменения могут вноситься фактически без всякого контроля. Нет понимания того, что изменение может оказаться разрушительным как для ИТ, так и для бизнес операций, и не осознаются выгоды от применения эффективного управления изменениями.

1. Начальный/Повторяющийся эпизодически и бессистемно

Признается необходимость управления и контроля изменений. Практики внесения изменений заметно различаются, и существует вероятность несанкционированных изменений. Документация по изменениям ведется плохо или отсутствует вообще, а документация по конфигурации является неполной и недостоверной. Существует вероятность ошибок в сочетании с нарушениями работы в среде промышленной эксплуатации, вызванными плохим управлением изменениями.

2. ***Повторяющийся, но интуитивный***

Существует неформальный процесс управления изменениями, который соблюдается для большинства случаев внесения изменений. Однако, он неструктурирован, примитивен и подвержен ошибкам. Точность документации по конфигурации является нестабильной и внесению изменений предшествует лишь ограниченное планирование и оценка возможных последствий.

3. ***Определенный***

Определен формализованный процесс управления изменениями, включая их классификацию, ранжирование, аварийные процедуры, санкционирование изменения, и управление выпуском, однако его соблюдение не обеспечено соответствующими механизмами. Имеют место временные решения, идущие в обход процессов. Могут происходить ошибки и несанкционированные изменения. Анализ последствий изменений в инфраструктуре ИТ на корпоративные операции становится формализованным, обеспечивая поддержку плановым выпускам новых приложений и технологий.

4. ***Управляемый и измеряемый***

Процесс управления изменениями хорошо разработан и соблюдается в отношении всех изменений, и менеджмент уверен, что исключения из этого минимальны. Данный процесс эффективен, но связан с использованием большого количества ручных процедур и средств контроля за обеспечением требуемого качества. Все изменения подвергаются тщательному планированию и всесторонней оценке возможных последствий с целью минимизации вероятности возникновения проблем после внесения изменения в рабочую систему. Внедрен процесс санкционирования внесения изменений. Документация по управлению изменениями актуальна и точна, при этом обеспечивается формальное отслеживание изменений. Документация по конфигурации в целом является точной. Планирование и реализация управления изменениями в инфраструктуре ИТ все более интегрируется с изменениями в бизнес процессах. Это обеспечивает должное рассмотрение вопросов, касающихся обучения персонала, организационных изменений и обеспечения непрерывности бизнеса. Имеет место улучшенная координация вопросов управления изменениями в инфраструктуре ИТ и перестройки бизнес процессов. Происходит постоянный мониторинг уровня качества и эффективности процесса управления изменениями.

5. ***Оптимизированный***

Процесс управления изменениями регулярно рассматривается руководством и корректируется для соответствия лучшим практикам. Данный процесс анализируется по результатам мониторинга. Информация о конфигурации хранится в электронном виде и обеспечивает управление версиями. Отслеживание изменений является сложным процессом и предусматривает использование средств обнаружения несанкционированного и нелицензионного программного обеспечения. Управление изменениями в инфраструктуре ИТ интегрировано с управлением изменениями в корпоративных процессах — это обеспечивает то, что ИТ является фактором, способствующим росту производительности и созданию новых возможностей для организации.

AI 7. Внедрение и приемка решений и изменений

Описание процесса

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.

Управление процессом

Внедрение и приемка решений и изменений.

удовлетворяет следующим бизнес требованиям к ИТ

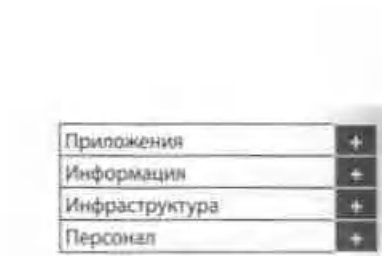
внедрение новых или подвергшихся изменениям систем, которые работают без существенных проблем после инсталляции. **сосредоточено на**

проверке соответствия приложений и инфраструктурных решений поставленным задачам и на отсутствие ошибок, а также на планировании выпуска версий. **достигается с помощью**

- Внедрения методологии тестирования.
- Планировании выпуска версий.
- Оценки и утверждения результатов тестирования бизнес-менеджерами.
- Проведении анализа результатов внедрения. **результаты**

оцениваются с помощью следующих показателей

- Количество простоев в работе приложений или число исправлений в данных, вызванных некачественным тестированием.
- Доля систем, соответствующих ожидаемым результатам (по данным анализа результатов внедрения).
- Доля проектов, имеющих документированный и утвержденный план тестирования.



Цели контроля

AI 7.1. Обучение

Проводить обучение пользователей и операционной группы в составе службы ИТ в соответствии с определенным планом обучения и внедрения, являющимся частью проекта разработки, внедрения или модификации любой информационной системы.

AI 7.2. План тестирования

Разработать план тестирования, основанный на общекорпоративных стандартах, определяющих роли, обязанности, ожидаемые результаты на входе и выходе системы. Следует убедиться, что план утвержден заинтересованными сторонами.

AI 7.3. План внедрения

Разработать план внедрения и отмены изменений. Получить утверждение заинтересованных сторон.

AI 7.4. Среда тестирования

Определить и создать безопасную среду тестирования, содержащую репрезентативную выборку планируемой среды промышленной эксплуатации в таких аспектах как безопасность, меры внутреннего контроля, эксплуатационная практика, качество данных, требования в отношении персональных данных, эксплуатационная нагрузка.

AI 7.5. Перенос системы и данных

Запланировать 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

Тестировать изменения независимо друг от друга в соответствии с определенным ранее планом тестирования до внедрения в эксплуатационную среду. Следует убедиться, что план включает в себя аспекты, связанные с безопасностью и производительностью.

AI 7.7. Тестирование перед окончательной приемкой

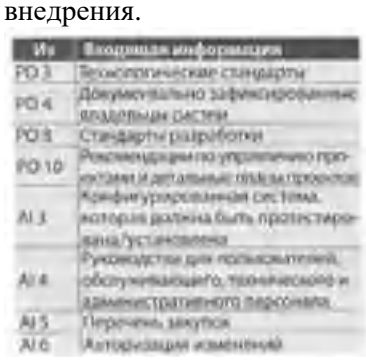
Следует убедиться, что владельцы бизнес процессов и заинтересованные стороны в службе ИТ оценили результаты тестирования, как предусмотрено планом тестирования. Исправить существенные ошибки, выявленные в процессе тестирования, завершить выполнение комплекса испытаний, определенных планом тестирования и, при необходимости, регрессионное тестирование. После завершения анализа, утвердить ввод в эксплуатацию.

AI 7.8. Ввод в эксплуатацию

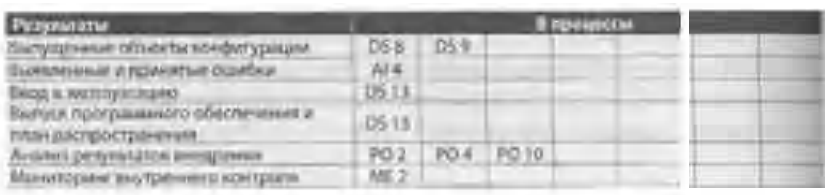
По завершению тестирования, контролировать ввод изменений в среду промышленной эксплуатации в соответствии с планом внедрения. Получить подтверждение от основных заинтересованных сторон, таких как пользователи, владелец системы и операционное руководство. Если это возможно, запустить новую систему параллельно со старой и сравнить их работу и результаты.

AI 7.9. Анализ результатов внедрения

Остановить процедуры, соответствующие стандартам организационного управления изменениями, для получения анализа результатов внедрения как необходимого элемента плана внедрения.



Из	Входящая информация
PO 3	Технологические стандарты
PO 4	Документально зафиксированные владельцем систем
PO 8	Стандарты разработки
PO 10	Рекомендации по управлению проектами и детальные планы проектов
AI 3	Конфигурированная система, которая должна быть протестирована/установлена
AI 4	Руководство для пользователей, обслуживающего, технического и административного персонала
AI 5	Перечень закупок
AI 6	Авторизация изменений



Результаты	В процессах					
Выступление объекты конфигурации	DS 8	DS 9				
Выявленные и принятые ошибки	AI 4					
Ввод в эксплуатацию	DS 13					
Выпуск программного обеспечения и план распространения	DS 13					
Анализ результатов внедрения	PO 2	PO 4	PO 10			
Мониторинг внутреннего контроля	ME 2					

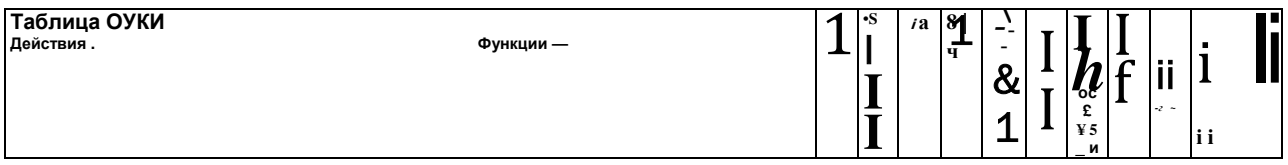


Таблица ОУКИ

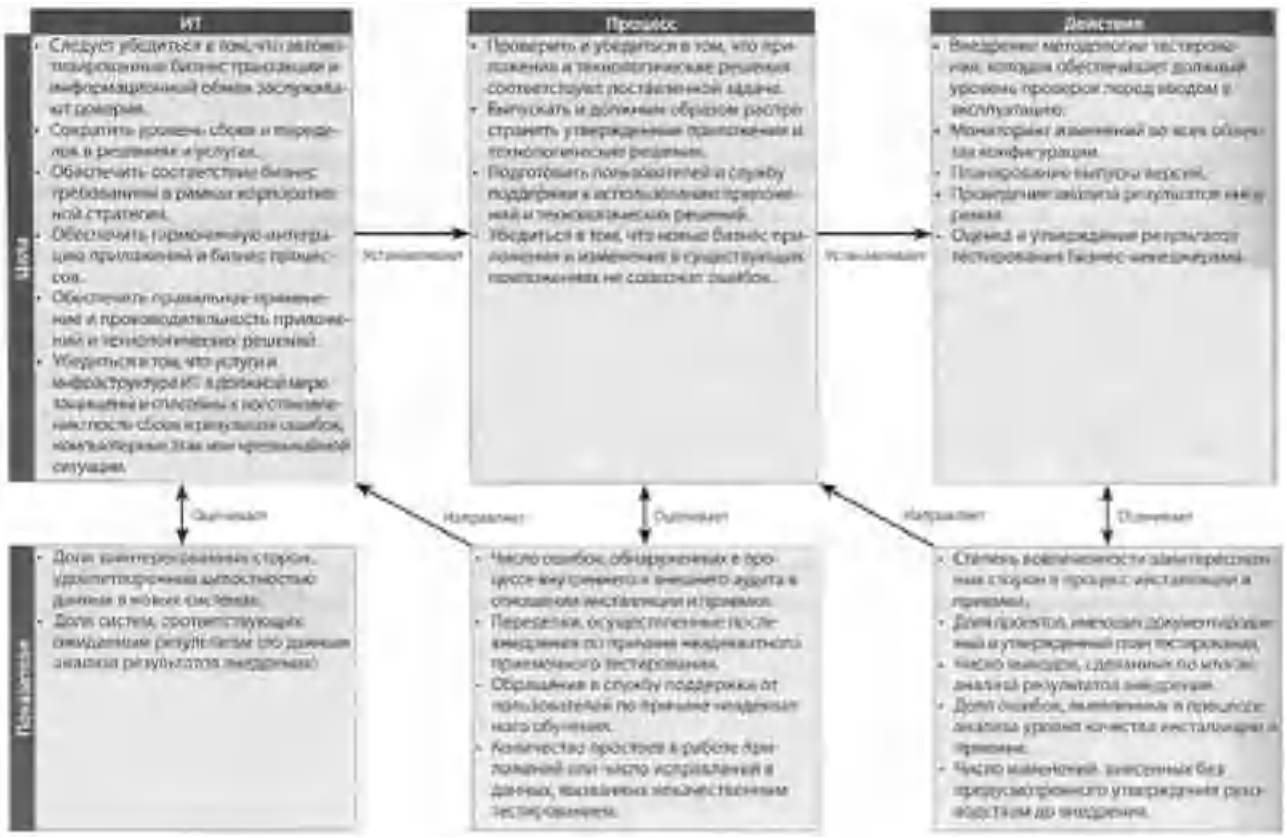
Действия . **Функции —**

Рекомендации по управлению

						rf I	£>- £ s			S	I
Разрабатывать и аналюироаапть план внедрения			**к**	**у**		**К**	**К**	*О*		**к к**	
Определять и анализировать стратегию тестирования (критерии начала и окончании; и vt:aiio.io гикэдлч планирования операционного тестирования			**к**	**V**	**к**	**к**	**К**	*О*		**к**	
Пас троить п поддерживать репозиторий бизнес и технически! требований и сценариев тестиро-вании аккредитованных систем				**V**				*О*			
Осуществлять перенос систем и интеграционное тестирование в тестовой среде			**и**	**и**	**О**	**к**	**К**	**У/О**		**и**	**Г**
Рдтвертызать тестовую среду и проварить окончательные испытания			**и**	**и**	**О**	**У**	**К**	**V70**		**и**	**ш:**
Шаль рекомендации по авову е эксплуэтацяю. осиованние на согласованна оаи« критериях г.рлч",!**			**и**	**0**	**V**	**О**	**К**	**0**		**и ПД**	

В таблице ОУКИ показано, кто является Ответственным, Утверждающим, Консультирующим и/или Информированным

Цели и показатели



Модель зрелости

Управление процессом *«Внедрение и приемка решений и изменений»* удовлетворяет следующим бизнес требованиям к ИТ *внедрение новых или подвергшихся изменениям систем, которые работают без существенных проблем после своей инсталляции* и соответствует характеристикам:

0. Несуществующий

Полностью отсутствуют процессы внедрения или приемки, ни высшее руководство, ни персонал ИТ не осознают необходимости проверки того, что реализованные решения соответствуют предполагаемому назначению.

1. Начальный/Повторяющийся эпизодически и бессистемно

Есть осознание необходимости проверки и подтверждения того, что реализованные решения соответствуют предполагаемому назначению. Тестирование проводится для некоторых проектов, однако инициатива в его проведении оставлена на усмотрение отдельных проектных групп, а применяемые подходы заметно различаются. Формальная приемка систем в эксплуатацию проводится редко или отсутствует вообще.

2. Повторяющийся, но интуитивный

Применяемые подходы к тестированию и приемке отчасти согласованы, однако они не базируются на какой-либо методологии. Обычно метод испытания выбирают сами проектные группы, при этом, как правило, отсутствует комплексное тестирование. Существует неформальный процесс утверждения.

3. Определенный

Внедрена формализованная методология, касающаяся установки, миграции, конвертации данных и приёмки систем. Процессы внедрения и приемки решений ИТ интегрированы в жизненный цикл системы и в определенной степени автоматизированы. Обучение персонала, тестирование, переход в режим промышленной эксплуатации и приемка зачастую отличаются от заданного

процесса. Качество систем, принятых в эксплуатацию, является нестабильным, при этом новые системы часто вызывают появление значительного количества проблем после завершения внедрения.

4. Управляемый и измеряемый

Процедуры формализованы и предусматривают использование на практике тестовой среды и формализованной приемки. На практике данный формализованный подход применяется ко всем крупным изменениям, вносимым в системы. Процесс оценки степени удовлетворения требований пользователей стандартизирован и поддается измерению, а измеряемые показатели могут эффективно рассматриваться и анализироваться руководством. Качество систем, принимаемых в эксплуатацию, является удовлетворительным для руководства, а количество проблем, возникающих после внедрения систем, считается приемлемым. Автоматизация данного процесса проводится от случая к случаю и зависит от реализуемого проекта. Руководство может быть удовлетворено существующим уровнем эффективности, несмотря на недостаток анализа результатов внедрения. Система испытаний адекватно отражает реальные условия эксплуатации. При осуществлении крупных проектов применяется тестирование с возрастающей нагрузкой для новых систем и регрессивное тестирование для существующих систем.

5. Оптимизированный

В результате непрерывного совершенствования и уточнения процессы внедрения и приемки систем доведены до уровня лучших практик. Процессы внедрения и приемки полностью интегрированы в жизненный цикл систем и, при необходимости, автоматизированы, что способствует наиболее оптимальному обучению персонала, тестированию и переходу новых систем в режим промышленной эксплуатации. Тщательно разработанные тестовые среды, процессы регистрации проблем и устранения отказов обеспечивают результативный и эффективный перевод систем в среду промышленной эксплуатации. Обычно приемка не связана с переделками, а проблемы, возникающие после внедрения, сводятся к незначительным корректировкам. Анализ результатов внедрения систем стандартизирован, а полученные при этом уроки учитываются в этом процессе, обеспечивая непрерывное совершенствование качества. Применяется постоянно

тестирование с возрастающей нагрузкой для новых систем и регрессивное тестирование для модернизированных систем.

Эксплуатация и сопровождение

DS 1. Определение и управление уровнем обслуживания

Описание процесса

Эффективная коммуникация между руководством ИТ и корпоративными пользователями соответствующих услуг становится возможной благодаря документально оформленному соглашению об ИТ услугах и уровне обслуживания. Этот процесс также 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.

Управление процессом

Определение и управление уровнем обслуживания.

удовлетворяет следующим бизнес требованиям к ИТ

обеспечение соответствия между основными ИТ услугами и корпоративной стратегией.

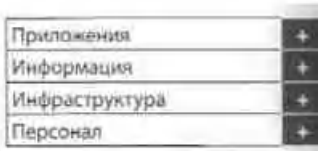
сосредоточено на

определении требований обслуживания, достижении договоренностей и мониторинге достижения уровней обслуживания. **достигается с помощью**

- Формализации внутренних и внешних соглашений в соответствии с требованиями и возможностями оказания услуг.
- Отчетности о достижении уровней обслуживания (отчеты и встречи).
- Определения и включения новых и обновленных требований к обслуживанию в стратегическое планирование.

результаты оцениваются с помощью следующих показателей

- Доля заинтересованных сторон в организации, удовлетворенных тем, что оказание услуг соответствует согласованным ранее уровням обслуживания.
- Число оказываемых услуг, не включенных в каталог.
- Число встреч по обсуждению соглашений об уровне обслуживания с корпоративными потребителями услуг в год.



Цели контроля

DS 1.1. Методология управленияуровнем обслуживания

Сформулировать методологию, которая обеспечит формализованный процесс управления уровнем обслуживания между потребителем и поставщиком услуг. Методология должна поддерживать постоянное соответствие бизнес требованиям и приоритетам, а также способствовать общему пониманию между потребителем и поставщиком услуг. Она должна включать процессы формирования требований к услугам, определения самих услуг, соглашения об уровне обслуживания (SLA) и соглашения операционного уровня (OLA), определение источников финансирования. Данные аспекты должны быть организованы в рамках каталога услуг. Методология должна определять организационную структуру управления уровнем обслуживания, должностные обязанности, цели и ответственность внутренних и внешних поставщиков и потребителей услуг.

DS 1.2. Определение услуг

Определения ИТ услуг должны быть основаны на характеристиках услуг и бизнес требованиях. Обеспечить их оптимизацию и централизованное хранение посредством каталога (портфеля) услуг.

DS 1.3. Соглашения об уровне обслуживания

Сформулировать и заключить соглашения об уровне обслуживания для всех критичных ИТ услуг, основываясь на требованиях потребителей и возможностях службы ИТ. Соглашения должны включать в себя 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. Рассмотреть такие аспекты, как доступность, надежность, производительность, возможности для роста, уровни поддержки, обеспечение непрерывности, безопасность и ограничения требований.

DS 1.4. Соглашения операционногоуровня

Сформулировать соглашения операционного уровня, которые определяют, как технически будут оказываться услуги, для оптимальной поддержки соглашений об уровне обслуживания. Соглашения операционного уровня должны определить технические процессы в терминах, понятных поставщику и могут поддерживать одновременно несколько соглашений об уровне обслуживания.

DS 1.5. Мониторинг и отчетность по выполнению соглашений об уровне обслуживания

Постоянно следить за исполнением соглашений об уровне обслуживания. Отчеты о достижении определенных уровней обслуживания должны предоставляться в формате, удобном для понимания заинтересованных сторон. Отчетные статистические данные должны анализироваться и учитываться при выявлении негативных и позитивных тенденций как в разрезе отдельных услуг, так и в целом по обслуживанию.

Из	Входящая информация
PO 1	Стратегический и тактические планы ИТ, портфель ИТ услуг
PO 2	Принятые классификации данных
PO 5	Обновленный портфель ИТ услуг
AI 2	Первоначальные планы соглашений об уровне обслуживания
AI 3	Первоначальные планы соглашений операционного уровня
DS 4	Требования к аварийному обслуживанию, включая перечень должностных лиц и их обязанностей
ME 1	Аспекты эффективности в ИТ планировании

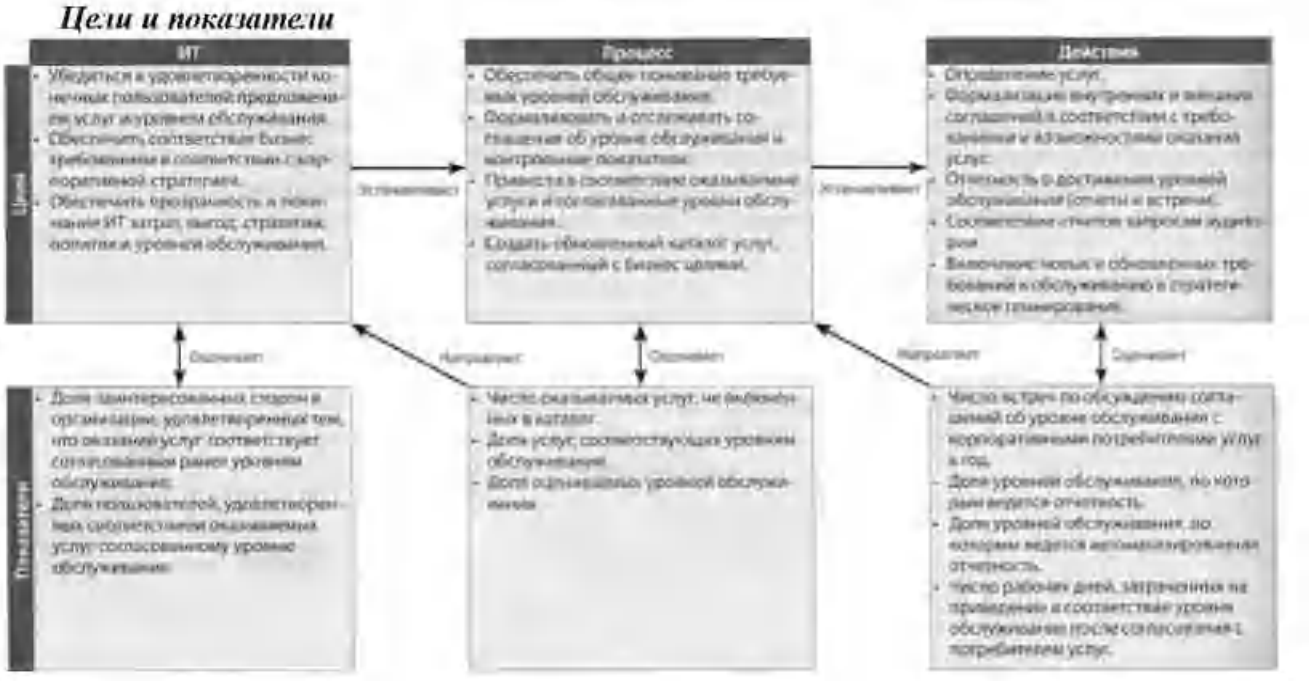
Результаты	В процессы						
Отчет об анализе контракта	DS 2						
Отчеты об эффективности процессов	ME 1						
Новые/обновленные требования к услугам	PO 1						
Соглашения об уровне обслуживания	AI 1	DS 2	DS 3	DS 4	DS 6	DS 8	DS 13
Соглашения операционного уровня	DS 4	DS 5	DS 6	DS 7	DS 8	DS 11	DS 13
Обновленный портфель ИТ услуг	PO 1						

Таблица ОУКИ

Действия ↓ / Функции →	финансовый директор	Высшее руководство	Директор по ИТ	Владелец бизнес-процесса	Руководитель эксплуатации системы	Главный архитектор ИТ-систем	Руководитель разработок	Руководитель администрации ИТ	Руководитель проектного офиса	Аудит, риски, безопасность	Сервис-менеджер
Создать методологию для определения ИТ услуг		К	У	К	К	И	К	К	И	И	О
Создать каталог ИТ услуг		И	У	К	К	И	К	К	И	И	О
Определить соглашения об уровню обслуживания для критичных ИТ услуг	И	И	К	К	О	И	О	О	К	К	У/О
Определить соглашения операционного уровня для соответствия соглашениям об уровне обслуживания			И	К	О	И	О	О	К	К	У/О
Осуществлять мониторинг и вести отчетность об эффективности на всех уровнях обслуживания			И	И	О		И	И		И	У/О
Рассматривать соглашения об уровне обслуживания и контракты	И		И	К	О		О	О		К	У/О
Рассматривать и обновлять каталог ИТ услуг		И	У	К	К	И	И	К	И	И	О
Разработать план совершенствования услуг		И	У	И	О	И	О	К	К	И	О

В таблице ОУКИ показано, кто является Ответственным, Утверждающим, Консультирующим и/или Информированным

Цели и показатели



Модель зрелости

Управление процессом *«Определение и управление уровнем обслуживания»* удовлетворяет следующим бизнес требованиям к ИТ *обеспечение соответствия между основными ИТ услугами и корпоративной стратегией* и соответствует характеристикам:

0. Несуществующий

Руководство еще не осознало необходимость процесса определения уровня обслуживания. Не определен порядок отчетности и не назначены лица, ответственные за осуществление контроля за требуемым уровнем услуг.

1. Начальный/Повторяющийся эпизодически и бессистемно

Есть осознание необходимости управления уровнем услуг, однако, этот процесс пока неформален и, фактически, является лишь реакцией на происходящие события. Ответственность и отчетность по предоставлению услуг определены на неформальном уровне. Если показатели оказания услуг и существуют, то они носят качественный характер при нечетком определении конечных целей. Отчетность является неформальной, нерегулярной и непоследовательной.

2. Повторяющийся, но интуитивный

Имеются соглашения об уровне обслуживания, однако они имеют неформальный характер и не проработаны. Отчетность об уровне обслуживания страдает неполнотой, может быть неадекватной и вводить в заблуждение пользователей. Отчетность об уровне обслуживания зависит от квалификации и инициативности отдельных руководителей. Назначен координатор в отношении уровня услуг, определены его обязанности, однако он не наделен достаточными полномочиями. Если процесс обеспечения соблюдения требований соглашений об уровне обслуживания существует, то он протекает на произвольной основе, а не по указанию руководства.

3. Определенный

Имеется четкое распределение ответственности, однако обязанности в полной мере не подкреплены соответствующими полномочиями. Ведется процесс разработки соглашений об уровне обслуживания, причем предусмотрены контрольные точки для оценки степени удовлетворенности клиентов. Услуги и уровни обслуживания определены, документированы и согласованы в рамках стандартного процесса. Выявлены недостатки в уровнях обслуживания, но процедуры их исправления неформальны. Существует четкая связь между достижением планируемого уровня обслуживания и финансированием. Уровни обслуживания согласованы, но могут не отвечать требованиям бизнеса.

4. Управляемый и измеряемый

Все чаще уровень услуг определяется на этапе формулирования требований к системе и учитывается при разработке дизайна приложений и среды промышленной эксплуатации. Регулярно оценивается степень удовлетворенности потребителей услуг. Контрольные показатели эффективности деятельности все в большей степени отражают нужды конечных пользователей, а не только задачи ИТ. Критерии оценки уровня обслуживания стандартизируются и все полнее отражают нормы, принятые в данной отрасли. Критерии определения уровней обслуживания основаны на их критичности для организации и учитывают доступность, надежность, производительность, возможности для развития, поддержку пользователей, обеспечение целостности и безопасности. В случае не достижения согласованного уровня обслуживания выполняется анализ основных причин ситуации. Все в большей степени автоматизируется система отчетности по результатам мониторинга уровня обслуживания. Определены и полностью осознаны эксплуатационные и финансовые риски, связанные с не достижением согласованного уровня обслуживания. Создана и поддерживается формализованная система мониторинга и оценки.

5. Оптимизированный

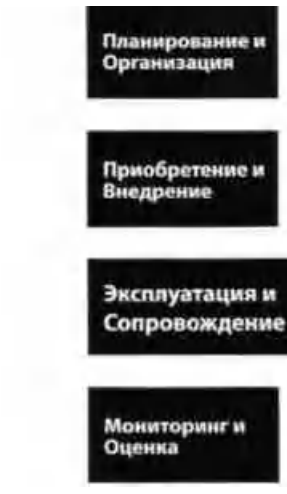
Уровни обслуживания постоянно переоцениваются для обеспечения соответствия бизнес целями и целям ИТ, а также для извлечения преимуществ, которые дает использование передовых технологий и оптимизации соотношения между ценой и качеством ИТ сервисов. Все процессы управления уровнем обслуживания постоянно совершенствуются. Ведется постоянный мониторинг уровня удовлетворенности пользователей. Планируемые показатели уровней обслуживания отражают стратегические цели подразделений организации и оцениваются согласно отраслевым нормам. Руководители

службы ИТ располагают ресурсами и системой отчетности, необходимыми для достижения намеченного уровня обслуживания. Предусмотрено материальное стимулирование инициатив по выполнению задач, стоящих перед организацией. Высшее руководство осуществляет мониторинг эффективности в рамках процесса постоянного совершенствования.

DS 2. Управление услугами сторонних организаций

Описание процесса

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.



Результативность	П
Эффективность	П
Конфиденциальность	В
Целостность	В
Доступность	В
Соответствие требованиям	В
Достоверность	В

Управление процессом

Управление услугами сторонних организаций.

удовлетворяет следующим бизнес требованиям к ИТ

достижение удовлетворительного уровня услуг сторонних организаций при сохранении прозрачности в отношении выгод, затрат и рисков. **сосредоточено на** установлении взаимоотношений и двусторонней ответственности квалифицированных сторонних поставщиков услуг и мониторинге соответствия оказываемых услуг условиям соглашений. **достигается с помощью**

- Выявления и определения категорий услуг, предлагаемых поставщиками.
- Выявления и минимизации рисков, связанных с поставщиками.
- Мониторинга и оценки эффективности работы поставщиков.

результаты оцениваются с помощью следующих показателей

- Число рекламаций пользователей в связи с оказываемыми услугами.
- Доля от числа основных поставщиков, соответствующих четко определенным требованиям и уровням обслуживания.
- Доля от числа основных поставщиков, охваченных мониторингом.

I Приоритетное O Второстепенное

Цели контроля

DS 2.1. Определение взаимоотношений с поставщиками

Выявить все услуги, предлагаемых поставщиками и классифицировать их следующим категориям: тип поставщика, значимость и критичность. Поддерживать формализованную документацию по техническим и организационным взаимоотношениям, в том числе по ролям и обязанностям, целям, ожидаемым результатам, а также полномочиям представителей данных поставщиков.

DS 2.2. Управление взаимоотношениями с поставщиками

Формализовать процесс управления взаимоотношениями с каждым поставщиком. Владельцы взаимоотношений должны согласовывать вопросы между потребителями услуг и поставщиками, а также обеспечивать качество отношений на основе доверия и прозрачности (например, посредством соглашений об уровне обслуживания).

DS 2.3. Управлениерисками, связанными с поставщиками

Выявить и минимизировать риски, связанные с возможностями поставщиков продолжать эффективное оказание услуг безопасным и эффективным образом. Следует убедиться, что контракты ответствуют распространенным корпоративным стандартам, нормативным и регулирующим

требованиям. Управление рисками должно также включать соглашения о неразглашении, договора по условному депонированию (escrow contracts), соответствие требованиям безопасности, альтернативных поставщиков, условия штрафов и бонусов и т.д.

DS 2.4. Мониторинг эффективности поставщиков

Внедрить процесс мониторинга оказания услуг, чтобы быть уверенным в соответствии поставщиков услуг корпоративным требованиям, условиям контрактов и соглашений об уровне обслуживания, а также в конкурентоспособности по отношению к альтернативным поставщикам и рыночным условиям.

Рекомендации по управлению

Из	Входящая информация
PO 1	Стратегия аутсорсинга ИТ
PO 8	Стандарты приобретения
AI 5	Договорные соглашения, требования по управлению взаимоотношениями со сторонними организациями
DS 1	Соглашения об уровне обслуживания, отчеты по договорам
DS 4	Требования к аварийному обслуживанию, включая перечень должностных лиц и их обязанностей

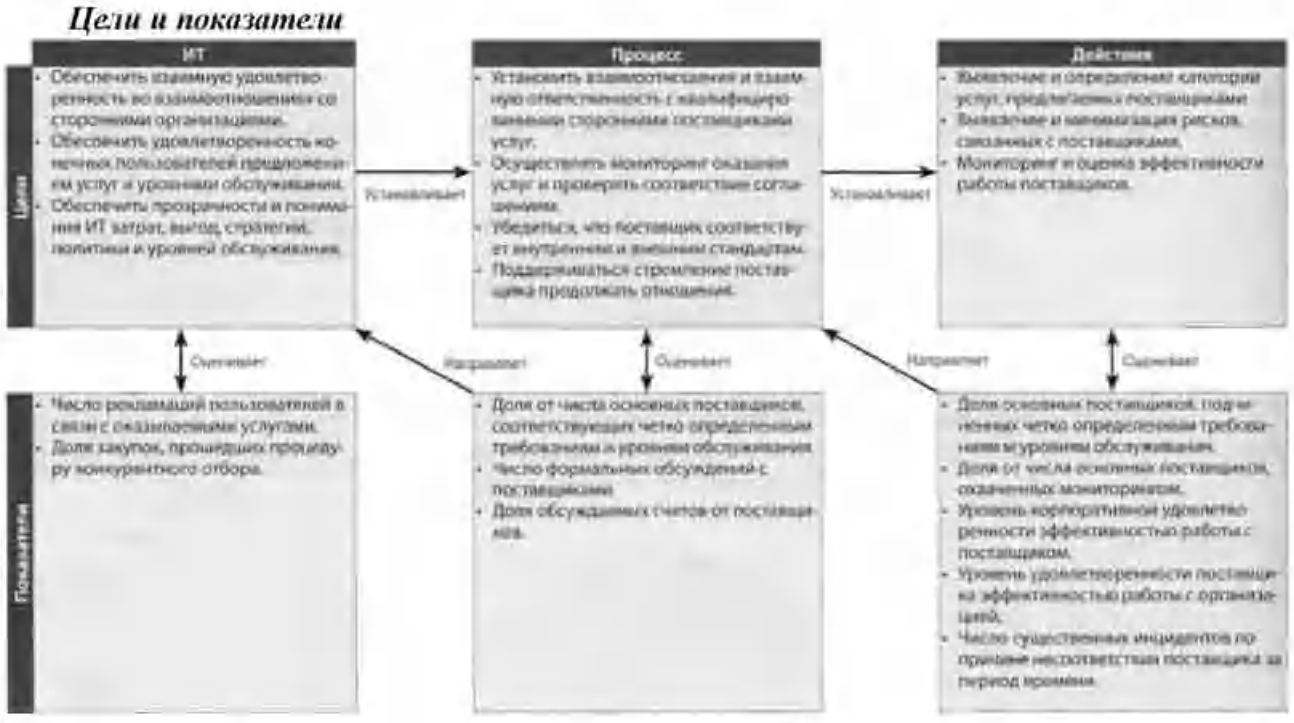
Результаты	В процессы
Отчеты об эффективности процессов	ME 1
Каталог поставщиков	AI 5
Риски, связанные с поставщиками	PO 9

Таблица ОУКИ

Действия ↓ Функции →	Президент	Финансовый директор	Высшее руководство	Директор по ИТ	Владелец бизнес процесса	Руководитель эксплуатации системы	Главный архитектор ИТ системы	Руководитель разработок	Руководитель администрации ИТ	Руководитель проектного офиса	Аудит, риски, compliance
Определить категории взаимоотношений со сторонними поставщиками услуг				И	К	О	К	О	У/О	К	К
Определить и документировать процессы управления поставщиками		К		У	И	О	И	О	О	К	К
Оценить поставщиков, политики и процедуры по отбору		К		У	К	К		К	О	К	К
Выявить, оценить и минимизировать риски, связанные с поставщиками		И		У		О		О	О	К	К
Осуществлять мониторинг оказания услуг поставщиками				О	У	О		О	О	К	К
Оценить долгосрочные цели во взаимоотношениях заинтересованных сторон	К	К	К	У/О	К	К	К	К	О	К	К

В таблице ОУКИ показано, кто является Ответственным, Утверждающим, Консультирующим и/или Информированным

Цели и показатели



Модель зрелости

Управление процессом *«Управление услугами сторонних организаций»* удовлетворяет следующим бизнес требованиям к ИТ *достижение удовлетворительного уровня услуг сторонних организаций при сохранении прозрачности в отношении выгод, затрат и рисков* и соответствует характеристикам:

0. Несуществующий

Не определен порядок отчетности и не назначены ответственные лица. Отсутствуют официальные политика и процедуры в отношении заключения договоров со сторонними организациями. Услуги, предоставляемые сторонними организациями, не утверждены и не проанализированы руководством. Отсутствует какая-либо деятельность в отношении оценки качества услуг и сторонними организациями не предоставляется никакой отчетности. При отсутствии договорных обязательств в части предоставления отчетности руководство организации не может судить о качестве предоставляемых услуг.

1. Начальный/Повторяющийся эпизодически и бессистемно

Руководство осознает необходимость документально оформленных политик и процедур управления поставщиками, в том числе, необходимость наличия подписанных договоров. Отсутствуют стандартные условия договоров в поставщиками услуг. Оценка эффективности процесса предоставления услуг осуществляется неформально и, фактически, является лишь реакцией на происходящие события. Практика зависит от опыта отдельных сотрудников и поставщиков.

2. Повторяющийся, но интуитивный

Процесс надзора за поставщиками услуг, оценка рисков и процесс поставки услуг осуществляются неформально. Используется формализованный согласованный договор со стандартными условиями поставщика (например, описанием услуг, которые должны быть поставлены). Подготавливаются отчеты по предоставленным услугам, однако, они не акцентированы на бизнес целях.

3. Определенный

Имеются документально оформленные процедуры по управлению приобретением услуг у сторонних организаций с четко очерченными процессами, обеспечивающими соответствующее ознакомление с организациями-поставщиками услуг и ведение переговоров с ними. После проработки соглашений, взаимоотношения со сторонними организациями являются исключительно договорными. В договоре подробно рассмотрен

характер поставляемых услуг, в нем также содержатся эксплуатационные и юридические требования и требования по вопросам контроля. Назначены лица, ответственные за надзор в отношении поставки услуг сторонними организациями. Договорные условия базируются на стандартизованных образцах. Оцениваются риски для бизнеса, связанные с договором и подготавливаются соответствующие отчеты.

4. Управляемый и измеряемый

Установлены формальные и стандартизованные критерии для определения условий соглашений, включая объем работ или услуг, обязательства, график выполнения работ, цены, договоренности по выставлению счетов и распределение ответственности. Установлена ответственность в отношении управления выполнением договора и взаимоотношений с поставщиком. Постоянно ведется проверка квалификации поставщика, рисков и возможностей, которыми он располагает. Определены требования, предъявляемые к услугам, эти требования увязаны с бизнес целями. Осуществляется процесс анализа качества поставляемых услуг и их соответствия условиям договора с учетом как текущих, так и будущих поставок услуг сторонними организациями. Применительно к процессу приобретения услуг используются модели трансфертного ценообразования. Все заинтересованные стороны имеют необходимые данные по услугам, их стоимости и основным намеченным этапам их предоставления. Существуют согласованные цели и показатели работы поставщиков услуг.

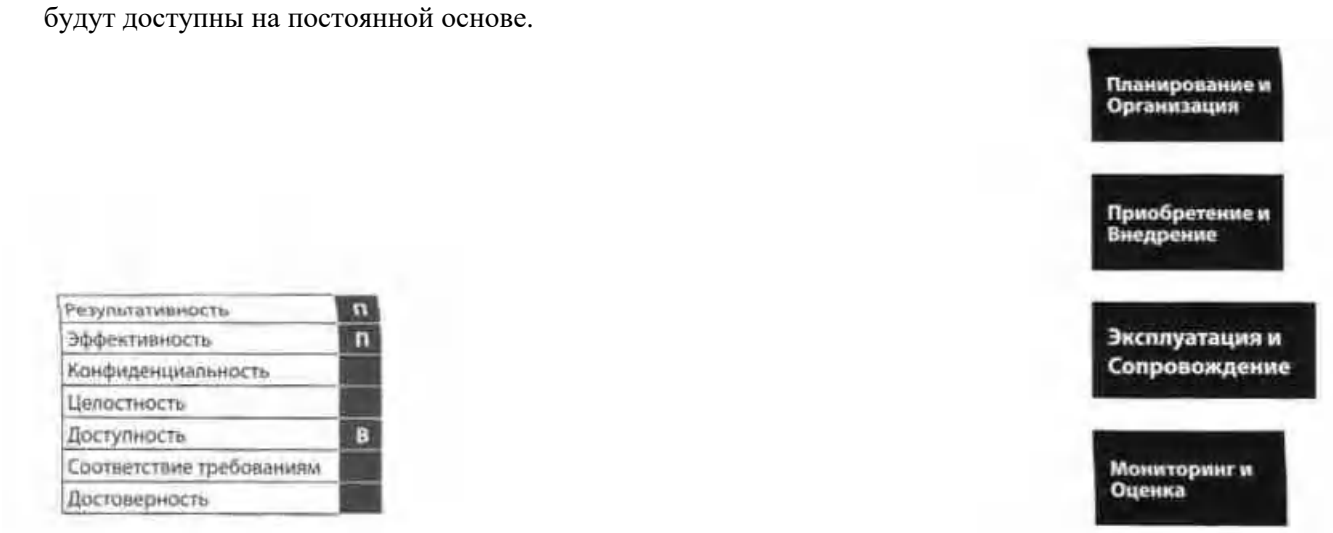
5. Оптимизированный

Заключенные договора с контрагентами периодически пересматривается через определенный интервал времени. Назначены лица, ответственные за управление поставщиками и обеспечение качества поставляемых услуг. Отслеживаются показатели, демонстрирующие соответствие условиям договора в части уровня услуг, мер контроля и нормативных требований; в случае необходимости принимаются корректирующие меры. Сторонние организации периодически подвергаются независимой проверке; ее результаты используются для повышения качества поставляемых услуг. Набор контрольных показателей динамически меняется в зависимости от изменений условий бизнеса. Контрольные показатели способствуют выявлению потенциальных проблем на ранней стадии. Исчерпывающая отчетность о соответствии уровню обслуживания связана с процессом вознаграждения контрагентов. Руководство совершенствует процесс приобретения услуг у сторонних организаций и осуществляет мониторинг контрольных показателей.

DS 3. Управление производительностью и мощностями

Описание процесса

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 емкостям хранения и непрерывности. Данный процесс призван обеспечить уверенность в том, что информационные ресурсы, поддерживающие исполнение бизнес требований, будут доступны на постоянной основе.



Управление процессом

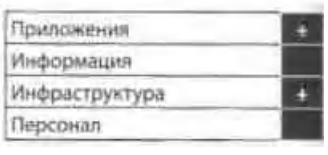
Управление производительностью и мощностями.

удовлетворяет следующим бизнес требованиям к ИТ

оптимизация эффективности ИТ инфраструктуры, ресурсов и возможностей в соответствии с бизнес требованиями. **сосредоточено на**

достижении соответствия требованиям по срокам, указанным в соглашениях об уровне обслуживания, минимизации простоев, а также проведении постоянного совершенствования производительности и мощности ИТ посредством мониторинга и измерений. **достигается с помощью**

- Планирования и обеспечения мощностей и доступности систем.
- Мониторинга и отчетности о производительности систем.
- Моделирования и прогнозирования производительности систем. **результаты оцениваются с помощью следующих показателей**
- Число часов, из расчета на пользователя в месяц, потерянных по причине неэффективного планирования мощностей.
- Доля пиков, при которых превышалась плановая нагрузка.
- Доля показателей времени реакции системы, не соответствующих соглашениям об уровне обслуживания.



Цели контроля

DS 3.1. Планирование производительности и мощностей

Осуществлять планирование для анализа производительности и мощностей ИТ ресурсов, чтобы быть уверенным в том, что производительность и мощности оправданы с точки зрения затрат и соответствуют уровням нагрузки, предусмотренным в соглашениях об уровне обслуживания. Планирование по мощностям и производительности должно с помощью методик моделирования создать модель производительности, мощностей и объема ИТ ресурсов в настоящем и будущем.

DS 3.2. Текущее состояние производительности и мощностей

Оценить текущую производительность и мощности ИТ ресурсов для того, чтобы определить, достаточны ли их текущие показатели для соответствия согласованным уровням обслуживания.

DS 3.3. Прогноз производительности и мощностей

Вести регулярное прогнозирование производительности и мощностей ИТ ресурсов, чтобы минимизировать риск сбоев в предоставлении услуг по причине недостаточных мощностей или снижения производительности и выделить резервные мощности на случай возможного перераспределения ресурсов. Выявить тенденции в распределении эксплуатационной нагрузки и учесть данные прогнозов при составлении планов производительности и мощностей.

DS 3.4. Доступность ИТ ресурсов

Обеспечить требуемые производительность и мощности, принимая во внимание такие аспекты как нормальный уровень эксплуатационной нагрузки, резервы, требования к системам хранения и продолжительность жизненного цикла ИТ ресурсов. Также должны быть учтены приоритетные задачи, механизмы устойчивости к отказам и расположение ресурсов. Руководство должно убедиться в том, что планы по обеспечению непрерывности должным образом учитывают все вопросы, связанные с доступностью, мощностями и производительностью отдельных ИТ ресурсов.

DS 3.5. Мониторинг и отчетность

Осуществлять постоянный мониторинг производительности и мощностей ИТ ресурсов. Полученные в ходе мониторинга данные должны служить двум целям:

- Обеспечению и настройке текущей производительности ИТ и учитывать такие вопросы как устойчивость, вероятность инцидентов, текущая и проектная эксплуатационная нагрузка, планы хранения и приобретение ресурсов.
- Отчетности по вопросу доступности оказываемых услуг для бизнеса, в соответствии с соглашениями об уровне обслуживания.

Сопровождать все отчеты об отклонениях рекомендациями по их устранению.

Рекомендации по управлению

Из	Входящая информация
AI 2	Спецификации по доступности, непрерывности и восстановлению
AI 3	Требования мониторинга систем
DS 1	Соглашения об уровне обслуживания

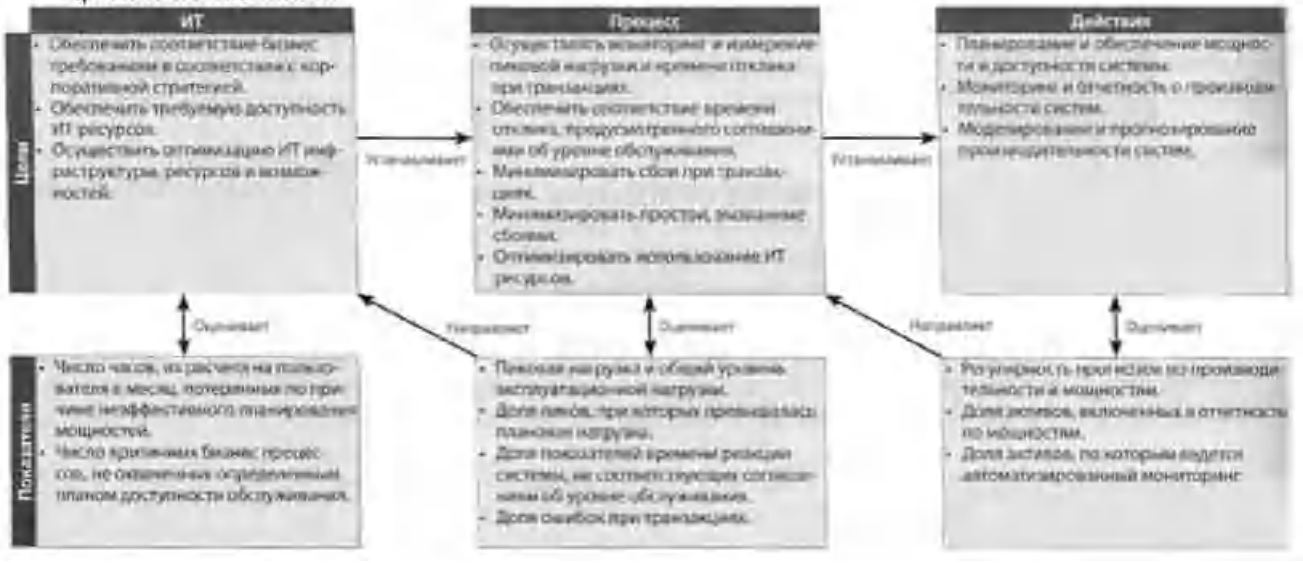
Результаты	В процессах						
Данные по производительности и мощностям	PO 2	PO 3					
Требования к плану по производительности и мощностям	PO 5	AI 1	AI 3	ME 1			
Требуемые изменения	AI 6						
Отчеты об эффективности процесса	ME 1						

Таблица ОУКИ

Действия ↓ / Функции →	Президент	Финансовый директор	Высшее руководство	Директор по ИТ	Владелец бизнес процесса	Руководитель эксплуатации систем	Главный архитектор ИТ систем	Руководитель разработок	Руководитель администрации ИТ	Руководитель проектного офиса	Аудит, риски, безопасность
Вести планирование производительности и мощностей ИТ ресурсов				У		О	К	К	К	К	
Изучать текущую производительность и мощности ИТ ресурсов				К	И	У/О		К	К	К	
Прогнозировать производительность и мощности ИТ ресурсов				К	К	У/О	К	К	К	К	
Проводить анализ проблем для выявления нехватки ИТ ресурсов				К	И	У/О		О	К	К	И
Вести планирование непрерывности для избежания случаев недоступности ИТ ресурсов				К	И	У/О		К	К	И	К
Вести постоянный мониторинг доступности, производительности и мощностей ИТ ресурсов				И	И	У/О		И	И	И	И

В таблице ОУКИ указано, кто является Ответственным, Утверждающим, Консультирующим и кто Информированным.

Цели и показатели



Модель зрелости

Управление процессом *«Управление производительностью и мощностями»* удовлетворяет следующим бизнес требованиям к ИТ *оптимизация эффективности ИТ инфраструктуры, ресурсов и возможностей в соответствии с бизнес требованиями* и соответствует характеристикам:

0. Несуществующий

Руководство не осознает тот факт, что основные бизнес процессы могут потребовать высокого уровня производительности ИТ, или что общая потребность организации в ИТ сервисах может превысить имеющиеся производственные мощности в этой области. Отсутствует процесс планирования загрузки мощностей.

1. Начальный/Повторяющийся эпизодически и бессистемно

Пользователям приходится самостоятельно изобретать способы преодоления препятствий, связанных с низкими производительностью и мощностями. Владельцы бизнес процессов лишь в малой степени осознают потребность в планировании производительности и мощностей. Принятие решений по вопросам производительности и мощностей, как правило, является лишь реакцией на происходящие события. Процесс планирования не формализован. Понимание текущей и будущей производительности и мощностей ограничено.

2. Повторяющийся, но интуитивный

Бизнес менеджмент и ИТ службы осведомлены о возможных отрицательных последствиях отсутствия управления производительностью и мощностями. Потребности в отношении производительности в основном обеспечены на основе оценки отдельных систем и знаний групп поддержки и проектирования. Отдельные технические средства могут быть использованы для диагностики проблем, связанных с производительностью и мощностями, однако адекватность и последовательность получаемых результатов зависит от квалификации отдельных сотрудников. Отсутствует общая оценка технических возможностей ИТ инфраструктуры, а также оценка ситуаций пиковой нагрузки и «наихудших сценариев». Проблемы доступности возникают неожиданно и как бы случайно, требуется значительное время для их обнаружения и устранения. Измерения производительности основаны в основном на нуждах ИТ, а не на потребностях пользователей.

3. Определенный

Требования по производительности и мощностям определены в рамках жизненного цикла систем. Определены требования по уровню обслуживания, а также система показателей, которые могут быть использованы для оценки эффективности. Можно моделировать и прогнозировать будущие требования к производительности в рамках определенного процесса. Готовятся отчеты, обеспечивающие необходимую статистику по производительности. Существует вероятность возникновения проблем, по-прежнему требуется значительное время для их устранения. Несмотря на то, что уровень обслуживания известен, пользователи время от времени могут относиться скептически к возможностям ИТ сервисов.

4. Управляемый и измеряемый

Имеются процессы и технические средства, необходимые для измерения степени загрузки систем, производительности и мощностей, а также сопоставления полученных данных с поставленными целями. Имеется актуальная информация, содержащая статистические данные по стандартизированным характеристикам производительности и предупреждающая о возможных проблемах, связанных с недостаточными производительностью и мощностями. По инцидентам, причиной которых явились несоответствия производительности и мощностей, принимаются меры в соответствии с установленными и стандартизированными процедурами. Для отслеживания конкретных ресурсов, например, емкости дисковых накопителей, сетевых серверов и межсетевых интерфейсов, используются автоматизированные средства. Статистические данные по производительности и мощностям готовятся с точки зрения обеспечения бизнес-процессов, так чтобы конечные пользователи могли понять уровень предлагаемых ИТ сервисов. Пользователи испытывают общую удовлетворенность имеющимися в данный момент возможностями в плане ИТ услуг, однако могут требовать перехода на новые, более высокие уровни. Контрольные показатели ИТ производительности и мощностей согласованы, но могут применяться от случая к случаю и непоследовательно.

5. Оптимизированный

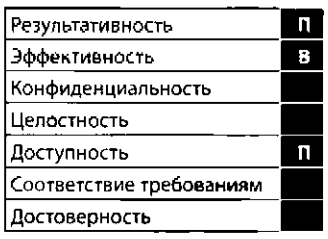
Планы по обеспечению должного уровня производительности и мощностей полностью соответствуют прогнозам развития бизнеса. ИТ инфраструктура и потребности бизнеса регулярно пересматриваются с целью обеспечения оптимальной мощности при минимальных затратах. Инструменты для мониторинга критичных ИТ ресурсов стандартизованы, применяются на всех платформах и увязаны с корпоративной системой управления инцидентами. Инструменты мониторинга выявляют и автоматически исправляют проблемы, связанные с производительностью и мощностями. Проводится анализ тенденций, указывающий на неизбежность возникновения проблем, обусловленных возрастанием объемов бизнеса, что позволяет путем соответствующего планирования избегать неожиданных инцидентов. Контрольные показатели ИТ производительности и мощностей точно настроены посредством индикаторов критичных бизнес процессов и

постоянно замеряются. Руководство совершенствует планирование производительности и мощностей, основываясь на данных анализа контрольных показателей.

DS 4. Обеспечение непрерывности ИТ сервисов

Описание процесса

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.



Управление процессом

Обеспечение непрерывностиИТ сервисов.

удовлетворяет следующим бизнес требованиям к ИТ

минимизация последствий для организации в случае прерываний в оказании ИТ услуг.

сосредоточено на

выработка способности к быстрому восстановлению автоматизированных решений, а также разработка, поддержка и тестирование планов непрерывности обслуживания.

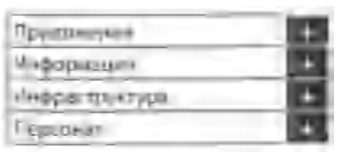
достигается с помощью

- Разработки и поддержки (улучшения) непрерывности обслуживания.
- Подготовки персонала и тестированию планов непрерывности обслуживания ИТ.
- Хранения копий планов непрерывности обслуживания и данных в сторонних хранилищах.

результаты оцениваются с помощью следующих показателей

- Число часов, из расчета на пользователя в месяц, потерянных по причине незапланированных отключений/перебоев в работе.
- Число критичных корпоративных процессов, возложенных на службу ИТ, но не охваченных планом непрерывности обслуживания.

Приоритетное ! ___ Второстепенное



Цели контроля

DS 4.1. Методология непрерывности обслуживания ИТ

Разработать методологию непрерывности обслуживания ИТ, которая будет поддерживать управление непрерывностью бизнеса в масштабах организации на постоянной основе. Цель методологии должна заключаться в определении требуемого уровня надежности (устойчивости) инфраструктуры, направлении разработок по вопросам восстановления после аварийных ситуаций и планов по непрерывности обслуживания. Данная методология должна рассматривать организационную структуру для обеспечения непрерывного управления, включать в себя перечень должностных лиц внутренних и внешних поставщиков услуг и их обязанностей, их руководство и клиентов, процессы планирования, в рамках которых вырабатываются правила и форматы документирования, тестирования и выполнения мер по восстановлению после аварийных ситуаций, а также планы по непрерывности обслуживания ИТ. План также должен включать в себя такие аспекты как определение критических ресурсов, выявление основных взаимозависимостей, мониторинг и отчетность по доступности критических ресурсов, методы альтернативной обработки данных, а также принципы резервного хранения и восстановления.

DS 4.2. Планы непрерывности обслуживания ИТ

Разработать планы непрерывности обслуживания ИТ, на основе методологии и с целью минимизации возможных последствий крупных прерываний для бизнес функций и процессов. Планы должны быть основаны на понимании рисков потенциальных последствий для бизнеса и учитывать требования по надежности, альтернативной обработке данных и возможностям восстановления всех критических ИТ услуг. Они также должны охватывать использование руководств пользователей, перечень должностных лиц и их обязанностей, процессы взаимодействия и подходы к тестированию.

DS 4.3. КритическиеИТресурсы

Обратить внимание на наиболее критические аспекты плана обеспечения непрерывности обслуживания ИТ, от которых зависят надежность и приоритеты в ситуациях восстановления после сбоев. Избегать отвлечения на восстановление менее критичных ресурсов и убедитесь, что время отклика и время на восстановление соответствуют приоритетным потребностям бизнеса, а также, что затраты остаются на приемлемом уровне и соответствуют регулирующим требованиям и условиям контрактов. Изучить аспекты, связанные с устойчивостью к сбоям, различные требования к времени отклика и времени на восстановление (например, от одного до четырех часов, от четырех до двадцати четырех часов, более 24 часов) и критические периоды операционной активности бизнеса.

DS 4.4. Поддержка плана непрерывности обслуживания ИТ

Следует убедить руководство ИТ в необходимости определять и исполнять контрольные процедуры по изменениям, чтобы план непрерывности обслуживания ИТ поддерживался в актуализированном виде и всегда отражал актуальные бизнес требования. Донести информацию об изменениях в процедурах и ответственностях четко и своевременно.

DS 4.5. Тестирование плана непрерывности обслуживания ИТ

Проводить регулярное тестирование плана непрерывности обслуживания ИТ, чтобы удостовериться в возможности эффективного восстановления ИТ систем, выявить недостатки и убедиться в адекватности плана. Это требует тщательного анализа, документирования, отчетности о результатах тестирования и внедрению мер, основанных на этих результатах. Изучить степень способности к восстановлению отдельных приложений, связанную со сценариями комплексного тестирования и интеграционного тестирования со вороны поставщиков.

DS 4.6. Обучение по плану непрерывности обслуживания ИТ

Обеспечить все заинтересованные стороны возможностью регулярного обучения соответствующим процедурам, их ролям и обязанностям в случае инцидента или аварийной

ситуации. Следует проверять и совершенствовать обучение в соответствии с результатами тестирования планов обеспечения непрерывности.

DS 4.7. Распространение плана непрерывности обслуживания ИТ

Следует убедиться в том, что существует определенная и управляемая стратегия по распространению плана, согласно которой уполномоченные заинтересованные стороны могут ознакомиться с планом. Особое внимание следует уделить доступности плана при возникновении аварийных ситуаций.

DS 4.8. Восстановление ИТ услуг после сбоя

Распланировать действия, которые следует предпринять в период восстановления ИТ услуг. К этим действиям относятся активация резервных площадок, переход на альтернативную обработку данных, общение с клиентами и заинтересованными сторонами, процедуры восстановления. Следует убедиться в том, что организация осознает сроки, необходимые для восстановления, а также масштабы требуемых технологических инвестиций для поддержки процессов восстановления.

DS 4.9. Сторонние хранилища резервных данных

Использовать сторонние хранилища для резервного хранения носителей данных, документации и других ИТ ресурсов, требуемых для восстановления ИТ и обеспечения планов непрерывности обслуживания. Определить содержание резервного хранилища совместно с владельцами бизнес процессов и ИТ персоналом. Руководство сторонним хранилищем должно следовать политике классификации данных и корпоративной практике хранения данных. Руководство ИТ должно убедиться в том, что сторонние хранилища проходят проверку не реже раза в год в отношении хранимых ресурсов, защиты от воздействий окружающей среды и безопасности. Следует убедиться в совместимости аппаратного и программного обеспечения для восстановления архивных данных, периодически тестировать и обновлять архивные данные.

DS 4.10. Анализ по результатам восстановления

Определить, предприняло ли руководство ИТ меры по оценке адекватности плана по успешному восстановлению работы ИТ службы после аварийной ситуации, после чего осуществлять

Рекомендации по управлению

Из	Входящая информация
PO 2	Принятые классификации данных
PO 9	Оценка рисков
AI 2	Спецификации по доступности, непрерывности и восстановлению
AI 4	Пользовательские, эксплуатационные, обслуживающие, технические и руководства для администраторов
DS 1	Соглашения об уровне обслуживания и соглашения операционного уровня

Результаты	В процессы						
Результаты тестирования планов отказоустойчивости	PO 9						
Критичность объектов ИТ конфигурации	DS 9						
Планы резервного хранения и защиты	DS 11	DS 13					
Пороговый уровень инцидентов аварийных ситуаций	DS 8						
Требования аварийного обслуживания, включая перечень должностных лиц и их обязанностей	DS 1	DS 2					
Отчеты об эффективности процессов	ME 1						

Таблица ОУКИ

Действия ↓ / Функции →	Президент	Вице-президент, директор	Высшее руководство	Директор по ИТ	Владелец бизнес процесса	Руководитель архитектуры систем	Главный архитектор ИТ-систем	Руководитель разработки	Руководитель администрации ИТ	Руководитель проектного офиса	Аудит, риски, безопасность
Разработать методологию непрерывности обслуживания		К	К	У	К	О	О	О	К	К	О
Оценить риски и проанализировать последствия рисков для бизнеса		К	К	К	К	У/О	К	О	К	К	К
Разработать и поддерживать планы непрерывности ИТ обслуживания	И	К	У	К	И	У/О		О	К	К	К
Определить категории ИТ ресурсов на основе задач восстановления				К		У/О		О	И	К	И
Определить и внедрить процедуры управления изменениями для поддержки плана непрерывности ИТ в обновленном виде				И		У/О		О	О	О	И
Периодически тестировать план непрерывности ИТ обслуживания				И	И	У/О		О	К	И	И
Разработать последовательный план действий на основе результатов тестирования				К	И	У/О	К	О	О	О	И
Планировать и проводить обучение по проблеме непрерывности ИТ обслуживания				И	О	У/О		О	О	И	И
Планировать восстановление ИТ услуг	И	И		К	К	У/О	К	О	О	О	К
Планировать и внедрить систему резервного хранения и защиты				И		У/О		О	К	И	И
Установить процедуры проведения анализа по результатам восстановления				К	И	У/О		О	К		К

В таблице ОУКИ показано, кто является Ответственным, Утверждающим, Консультирующим и/или Информированным

обновление плана.

Модель зрелости

Управление процессом *«Обеспечение непрерывности ИТ сервисов»* удовлетворяет следующим бизнес требованиям к ИТ *минимизация последствий для организации в случае сбоя в оказании ИТ услуг* и соответствует характеристикам:

0. Несуществующий

Нет понимания рисков, уязвимых мест и угроз по отношению к функционированию ИТ, а также негативного воздействия на бизнес, обусловленного потерей ИТ услуг. Обеспечение непрерывности услуг не рассматривается как вопрос, нуждающийся во внимании со стороны руководства.

1. Начальный/Повторяющийся эпизодически и бессистемно

Ответственности по обеспечению непрерывности услуг не формализованы, полномочия ответственных лиц ограничены. Руководство начинает осознавать риски, связанные с потребностью обеспечения непрерывного предоставления услуг. Основное внимание сосредоточено на обслуживании ресурсов инфраструктуры, а не на ИТ услугах. Пользователи применяют свои собственные приемы, чтобы справляться со сбоями в предоставлении ИТ услуг. Реакция службы ИТ на крупные сбои заранее не продумана и не подготовлена. Практикуются плановые отключения системы в целях ИТ обслуживания, без учета выполнения бизнес требований.

2. Повторяющийся, но интуитивный

Назначены сотрудники, ответственные за обеспечение непрерывности услуг. Подходы, применяемые к обеспечению непрерывности услуг, характеризуются фрагментарностью. Поступающая информация относительно доступности системы отличается неполнотой и не учитывает состояние бизнеса. Нет документального плана обеспечения непрерывности обслуживания, хотя имеется такое намерение и определены главные принципы его реализации. Существует перечень критических систем и компонентов, но он может быть не достаточно исчерпывающим. Возникает стандартизация методов обеспечения непрерывного обслуживания, однако успех здесь зависит от усилий отдельных сотрудников.

3. Определенный

Однозначно определена подотчетность и назначены лица, ответственные за планирование и контроль обеспечения непрерывной поставки услуг. План непрерывного обслуживания оформлен документально и основан на критичности систем и учете негативного воздействия на бизнес. Налажена периодическая отчетность по проверкам обеспечения непрерывности предоставления услуг. По инициативе отдельных сотрудников осуществляется дальнейшая стандартизация и обучение по преодолению последствий крупных инцидентов или аварийных ситуаций. Руководство последовательно рассматривает

вопросы, связанные с потребностью обеспечения непрерывного обслуживания. Постепенно начинается использование компонентов, характеризующихся высокой работоспособностью и избыточностью системы. Поддерживается перечень критических систем и компонентов.

4. Управляемый и измеряемый

Распределены ответственности и установлены стандарты для обеспечения непрерывного обслуживания. Назначены лица, ответственные за планирование мероприятий по обеспечению непрерывного обслуживания. Работа службы поддержки основана на результатах сервисного тестирования, внутренних лучших практиках и учитывает изменения ИТ и корпоративной среды. Осуществляется сбор и анализ систематизированных данных по обеспечению непрерывного обслуживания, на основе которых готовится отчетность и принимаются необходимые меры. Осуществляется обучение персонала по вопросам обеспечения непрерывного обслуживания. Последовательно внедряются лучшие практики в области доступности системы. Практика по этому вопросу и планирование предоставления услуг оказывают влияние друг на друга. Классифицированы возможные случаи нарушения непрерывного обслуживания. Соответствующим сотрудникам хорошо известна схема действий по каждому случаю. Цели и контрольные показатели непрерывного обслуживания могут быть внедрены и согласованы, но при этом непоследовательно измеряться.

5. Оптимизированный

Интегрированные процессы обеспечения непрерывного обслуживания основаны на сравнительном анализе и внешних лучших практиках. Планы обеспечения непрерывного обслуживания и планы обеспечения непрерывности бизнеса интегрированы друг с другом, соответствуют друг другу и постоянно поддерживаются. Требования по обеспечению непрерывного обслуживания обеспечены соглашениями с поставщиками. Проводятся масштабное тестирование плана обеспечения непрерывного обслуживания, результаты тестирования используются для обновления плана. Реализация обратной связи по результатам тестирования является частью процесса совершенствования. Практика в отношении доступности связана с планированием оказания услуг. Руководство уверено в том, что крупный инцидент не произойдет в результате сбоя в одном единственном месте. Практики по реализации плана осознаны и используются в полной мере. Проводится систематическое измерение контрольных показателей. Руководство совершенствует планирование непрерывного обслуживания, основываясь на данных анализа контрольных показателей.

DS 5. Обеспечение безопасности систем

Описание процесса

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.

Результативность	
Эффективность	
Конфиденциальность	П
Целостность	П
Доступность	В
Соответствие требованиям	В
Достоверность	В

Управление процессом

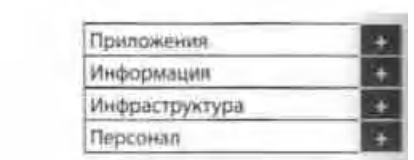
Обеспечение безопасности систем.

удовлетворяет следующим бизнес требованиям к ИТ

обеспечение целостности информации и инфраструктуры обработки данных, а также минимизация последствий для бизнеса от инцидентов и уязвимостей в системе безопасности. **сосредоточено на**

определении политики ИТ безопасности, планов и процедур, мониторинге, выявлении, отчетности и разрешении уязвимостей и инцидентов в области информационной безопасности. **достигается с помощью**

- Понимания требований безопасности, уязвимостей и угроз.
- Стандартизованное управление идентификацией пользователей и авторизациями.
- Регулярное тестирование аспектов, связанных с безопасностью. **результаты оцениваются с помощью следующих показателей**
- Число инцидентов, нанесших урон публичной корпоративной репутации.
- Число систем, в которых не соблюдены требования по безопасности.
- Число нарушений в разделении обязанностей.



Цели контроля

DS 5.1. УправлениеИТ безопасностью

Организовать управление ИТ безопасностью на максимально возможном организационном уровне, чтобы действия по обеспечению безопасности соответствовали требованиям бизнеса.

DS 5.2. План по ИТ безопасности

Преобразовать бизнес требования, а также требования в отношении рисков и соответствия требованиям в общий план по ИТ безопасности, учитывающий ИТ инфраструктуру и корпоративную культуру обеспечения безопасности. Следует убедиться в том, что план внедрен посредством политик безопасности, процедур и подкреплен инвестициям в услуги, персонал, аппаратное и программное обеспечение. Проинформировать заинтересованные стороны и пользователей о политиках и процедурах в области безопасности.

DS 5.3. Управление идентификацией

Следует убедиться в том, что все пользователи (внутренние, внешние и временные) и их деятельность в ИТ системах (приложениях, ИТ среде, системных операциях, разработке и обеспечении) может быть однозначно идентифицирована. Обеспечить идентификацию посредством механизмов авторизации. Подтвердить, что права на доступ пользователей к системам и данным соответствуют определенным и документированным бизнес потребностям и должностным обязанностям, соотнесенными с конкретными пользователями. Следует убедиться, что права на доступ пользователей, запрашиваемые руководством пользователей, подтверждены владельцами систем и предоставляются уполномоченным лицом в области безопасности. Хранить учетные записи пользователей и профили прав доступа в централизованном банке данных. Осуществлять на практике эффективные с точки зрения затрат технические и процедурные мероприятия для установления идентификации пользователей, аутентификации и обеспечения прав доступа.

DS 5.4. Управлениеучетными записями пользователей

Обеспечить управление запросами, созданием, приостановкой, изменением и ликвидацией учетных записей пользователей и связанных с ними полномочий с помощью комплекса процедур. Внедрить процедуру утверждения предоставляемых прав доступа со стороны владельцев данных или систем. Данные процедуры должны применяться по отношению ко всем пользователям, включая администраторов (привилегированных пользователей), а также внутренних и внешних пользователей, в обычных и аварийных условиях. Права и обязанности, относящиеся к доступу к корпоративным системам и информации, должны быть определены для всех типов пользователей в договорном порядке. Осуществлять регулярный управленческий мониторинг всех учетных записей и связанных с ними прав и полномочий.

DS 5.5. Тестирование, надзор и мониторинг в сфере ИТ безопасности Осуществлять тестирование и мониторинг внедрения ИТ безопасности, упреждая события. Вопросы, связанные с ИТ безопасностью должны своевременно пересматриваться с целью соответствия основным корпоративным принципам безопасности. Регистрация событий и мониторинг помогут предотвратить на ранних этапах и/или выявить и своевременно сообщить о необычной и/или ненормальной деятельности, по отношению к которой, возможно, следует принять меры.

DS 5.6. Определение инцидентов в сфере безопасности

Четко определить и сообщить характеристики потенциальных инцидентов в сфере безопасности, чтобы их можно было классифицировать и устранить в процессе управления проблемами и инцидентами.

DS 5.7. Защита технологий безопасности

Обеспечить защиту от взлома для технологий, связанных с безопасностью, и не разглашать соответствующую документацию без необходимости. ***DS 5.8. Управление ключами криптозащиты***

Определить политику и процедуры 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

Принимать превентивные, выявляющие и устраняющие меры (особенно по установке обновлений, связанных с безопасностью и защитой от вирусов) в рамках организации для защиты

информационных систем и технологий от вредоносных программ (вирусов, червей, шпионских программ, спама).

DS 5.10. Сетевая безопасность

Применять технологии обеспечения безопасности и соответствующие процедуры управления (межсетевые экраны, устройства для безопасности, сетевой сегментации и системы обнаружения вторжений) для авторизации доступа и контроля информационных межсетевых потоков.

DS 5.11. Обмен критичными данными

Осуществлять обмен критичными данными (транзакциями) только посредством надежного канала или носителя, которые гарантируют аутентичность содержания, доказательства отправления и

Рекомендации по управлению

Из	Входящая информация
PO 2	Информационная архитектура
PO 3	Технологические стандарты
PO 9	Оценка рисков
AI 2	Спецификации управляемых бизнес-приложений
DS 1	Соглашения об операционном уровне

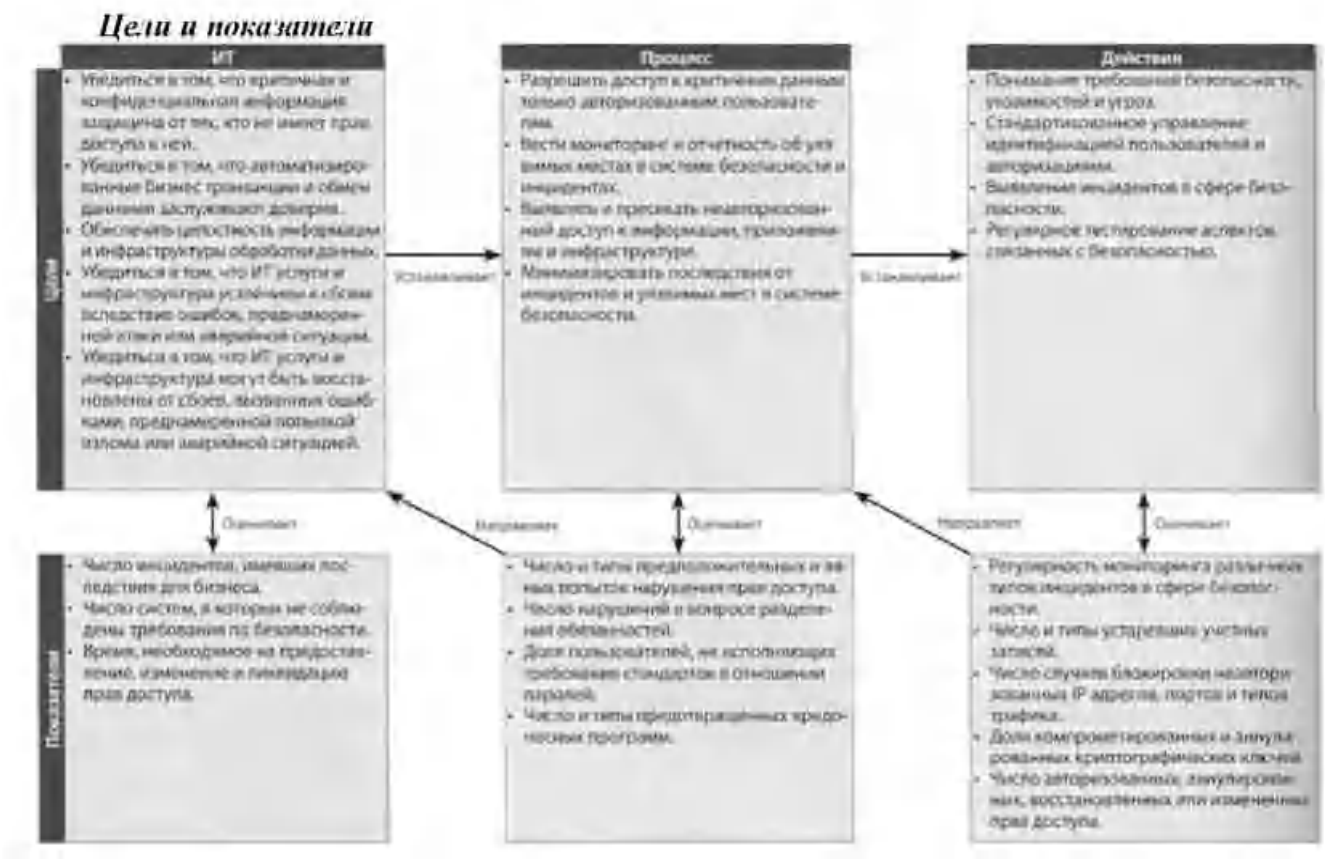
Результаты	В процессы						
Определение инцидентов в сфере безопасности	DS 8						
Специфические требования по планированию осведомленности в области	DS 7						
Отчеты об эффективности процессов	ME 1						
Требуемые изменения по безопасности	AI 6						
Уязвимые места и угрозы для безопасности	PO 9						
План и политики ИТ безопасности	DS 11						

Таблица ОУКИ

Действия ↓ / Функции →	Президент	Финансовый директор	Бизнес руководитель	Директор по ИТ	Владелец бизнес процесса	Руководитель эксплуатации систем	Главный архитектор ИТ систем	Руководитель разработок	Руководитель администрации ИТ	Руководитель проектного офиса	Аудит, риск, безопасность
Определить и поддерживать планы ИТ безопасности	И	К	К	У	К	К	К	К	И	И	О
Определить, принять и применить процесс управления идентификацией пользователей			И	У	К	О	О	И			К
Вести мониторинг потенциальных и существующих инцидентов в сфере безопасности				У	И	О	К	К			О
Вести периодический анализ и проверку прав доступа и полномочий пользователей				И	У	К					О
Установить и поддерживать процедуры поддержки и защиты криптографических ключей				У		О			И		К
Внедрить и поддерживать меры технического и процедурного контроля для защиты межсетевых информационных потоков				У	К	К	О	О			К
Проводить регулярный анализ уязвимых мест		И		У	И	К	К	К			О

В таблице ОУКИ показано, кто является Ответственным, Утверждающим, Консультирующим и/или Информированным

получения, а также невозможность отказа от факта обмена данными.



Модель зрелости

Управление процессом *«Обеспечение безопасности систем»* удовлетворяет следующим бизнес требованиям к ИТ *обеспечение целостности информации и инфраструктуры обработки данных, а также минимизация последствий для бизнеса от инцидентов и уязвимостей в системе безопасности* и соответствует характеристикам:

0. Несуществующий

Организация не осознает необходимость в обеспечении безопасности ИТ. Не определена ответственность и подотчетность по вопросам обеспечения безопасности. Не реализованы меры управления безопасностью ИТ. Не предусмотрены процедуры информирования по состоянию безопасности ИТ и реагирования на случаи нарушения безопасности. Полностью отсутствует какой-либо осязаемый процесс управления процессом обеспечения безопасности.

1. Начальный/Повторяющийся эпизодически и бессистемно

Организация осознает необходимость в обеспечении безопасности ИТ. Однако степень этого осознания зависит от конкретных сотрудников. Меры по обеспечению безопасности ИТ, фактически, являются лишь реакцией на происходящие события и никак не оцениваются. В связи с неопределенной ответственностью при обнаружении случаев нарушения безопасности ИТ происходит реакция по типу «указывания пальцем». Реакции на случаи нарушения безопасности непредсказуемы.

2. Повторяющийся, но интуитивный

Ответственным и подотчетным лицом по вопросам обеспечения безопасности ИТ назначен координатор по вопросам обеспечения безопасности ИТ, не получивший при этом никаких управленческих полномочий. Знания по вопросам обеспечения безопасности имеют фрагментарный и ограниченный характер. Хотя информация, имеющая отношение к вопросам безопасности, генерируется системами, она не анализируется. Услуги сторонних организаций могут не отвечать специфическим потребностям организации. Разработаны политики безопасности, однако, продолжают использоваться неадекватные методы и средства. Отчетность по вопросам обеспечения безопасности страдает неполнотой, может ввести в заблуждение или быть бесполезной. Обучение по вопросам безопасности доступно,

однако проводится в основном по инициативе отдельных сотрудников. Обеспечение ИТ безопасности понимается, в первую очередь, как обязанность службы ИТ и корпоративное руководство не принимает участие в управлении ИТ безопасностью.

3. Определенный

Имеется осведомленность по вопросам обеспечения безопасности, её повышение поощряется руководством. Определены процедуры обеспечения безопасности ИТ, соответствующие политике безопасности. Назначены лица, ответственные за обеспечение безопасности, однако их деятельность не в полной мере внедрена в практику. Существует план по обеспечению безопасности ИТ, обеспечивающий проведение анализа рисков. Отчетность по вопросам безопасности не в полной мере сосредоточена на потребностях бизнеса. Эпизодически выполняется тестирование аспектов обеспечения безопасности (например, возможности взлома системы).

4. Управляемый и измеряемый

Четко определены и внедрены ответственности по управлению ИТ безопасностью. Последовательно выполняется анализ рисков ИТ безопасности, а также возможных последствий. Завершено создание политик и процедур обеспечения безопасности, определены основные направления обеспечения безопасности с учетом особенностей данной организации.

Информирование по вопросам осведомленности о безопасности принимает обязательный характер. Стандартизованы идентификация, аутентификация и авторизация пользователей. Введена аттестация персонала, ответственного за аудит и управление безопасностью. Тестирование системы безопасности является стандартизованным и формализованным процессом, направленным на повышение безопасности. Процессы обеспечения безопасности ИТ координируются со службой общей безопасности всей организации. Отчетность по обеспечению безопасности ИТ увязана с целями бизнеса. Обучение по вопросам обеспечения безопасности проводится как для бизнес подразделений, так и для персонала ИТ. Это обучение планируется и осуществляется в соответствии с бизнес потребностями и выявленными рисками безопасности. Цели и показатели управления безопасностью определены, но пока не подвергаются оценке.

5. Оптимизированный

Руководители основных бизнес подразделений и ИТ службы несут солидарную ответственность по вопросам обеспечения безопасности ИТ, которые интегрированы с корпоративными целями обеспечения безопасности бизнеса. Требования по обеспечению безопасности ИТ четко определены, оптимизированы и включены в утвержденный план мероприятий по обеспечению безопасности. Конечные пользователи и потребители ИТ услуг все в большей степени отвечают за определение требований по безопасности, а функции обеспечения безопасности интегрированы с прикладными задачами на стадии проектирования. В случаях инцидентов немедленно применяются формализованные и автоматизированные процедуры реагирования. В ходе периодически проводимых оценок состояния безопасности проверяется эффективность выполнения плана мероприятий по обеспечению безопасности. Систематически собирается и анализируется информация о новых угрозах и уязвимых местах. Своевременно обсуждаются и принимаются меры по снижению уровня опасности. Тестирование аспектов безопасности, анализ основных причин случаев нарушения безопасности и заблаговременное выявление рисков — все это служит основой непрерывного повышения уровня безопасности. Процессы и технологии обеспечения безопасности интегрированы в рамках организации. Фиксируются, собираются и доводятся до сведения заинтересованных сторон показатели управления безопасностью. Руководство применяет эти данные для постоянного совершенствования плана обеспечения безопасности.

DS 6. Определение и распределение затрат

Описание процесса

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.

Управление процессом

Определение и распределение затрат.

удовлетворяет следующим бизнес требованиям к ИТ

обеспечение прозрачности, понимание ИТ затрат и совершенствование эффективности затрат посредством должного информирования об использовании ИТ услуг. **сосредоточено на**

полном и аккуратном учете затрат на ИТ, справедливом распределении, согласованным с бизнес пользователями и системе оперативной отчетности по использованию ИТ и распределению затрат. **достигается с помощью**

- Приведения в соответствие затрат на оплату услуг с качеством и количеством предлагаемых услуг.
- Создания и согласования полной модели затрат.
- Финансирования затрат в соответствии с принятой согласованной политикой.

результаты оцениваются с помощью следующих показателей

- Доля счетов за ИТ услуги, принятых/оплаченных бизнес-менеджерами.
- Доля расхождений между бюджетами, прогнозами и реальными затратами.
- Доля от общих затрат на ИТ, распределяемая согласно принятым моделям затрат.

Приоритетное |. Второстепенное

Цели контроля

DS 6.1. Определение услуг

Определить все затраты на ИТ и соотнести их с ИТ услугами, чтобы получить прозрачную модель затрат. ИТ услуги должны быть связаны с бизнес процессами, чтобы бизнес мог сравнить связанный с уровнем услуг уровень затрат.

DS 6.2. Бухгалтерский учет в области ИТ

Следует вести учет и распределение текущих затрат в соответствии с корпоративной моделью затрат. Расхождения между прогнозами и реальными затратами должны быть проанализированы, по ним должна вестись отчетность в соответствии с корпоративными системами оценки.

DS 6.3. Моделирование затрат и выставление счетов на оплату

Разработать и применять модель затрат, основанную на определении услуг, которая поддерживает расчет возвратных платежей за каждую услугу. Модель ИТ затрат должна обеспечить поддающееся учету и измерению, предсказуемое выделение средств на услуги для пользователей, что гарантирует рациональное использование ресурсов.

DS 6.4. Поддержка модели затрат

Следует регулярно проводить мониторинг и сравнительный анализ целесообразности модели затрат/выделения средств для поддержания ее соответствия меняющейся бизнес и ИТ деятельности.

Рекомендации по управлению

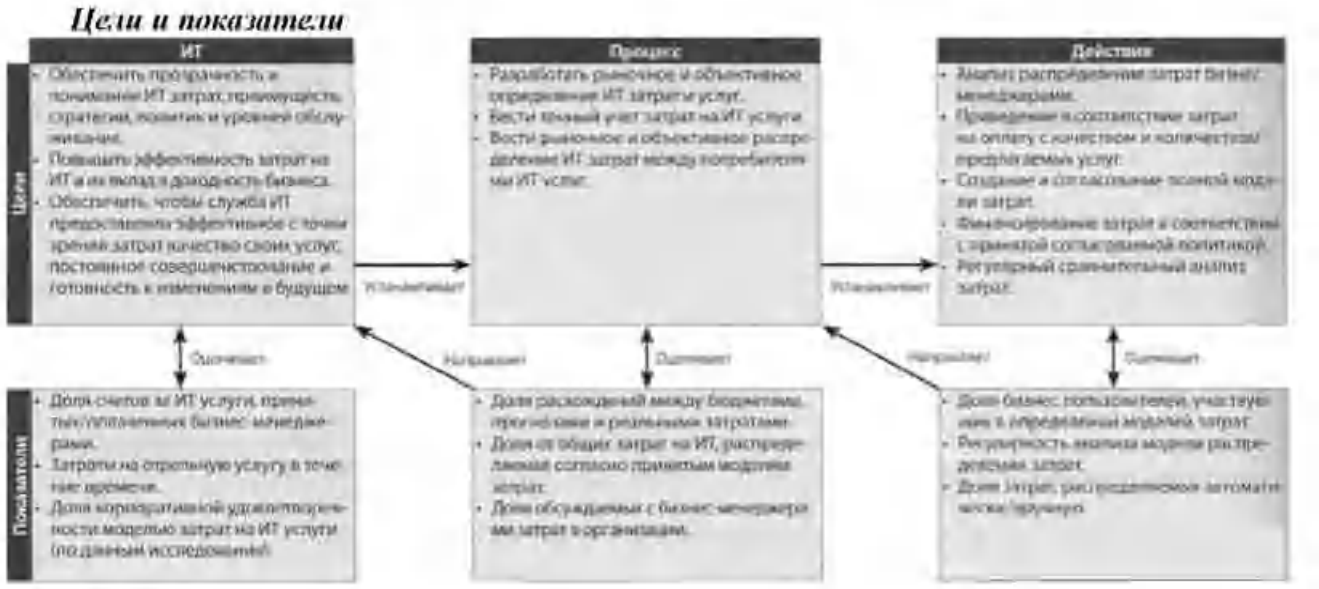
Из	Входящая информация
PO 4	Документально зафиксированные характеристики систем
PO 5	Отчеты о затратах и выгодах, ИТ бюджеты
PO 10	Детализированные планы проектов
DS 1	Соглашения об уровне обслуживания и соглашения операционного уровня

Результаты	В процессы
Финансовая документация ИТ	PO 5
Отчеты об эффективности процессов	ME 1

Таблица ОУКИ

Действия ↓ Функции →	Президент	Финансовый директор	Высшее руководство	Директор по ИТ	Владелец бизнес процесса	Руководитель эксплуатации систем	Главный архитектор ИТ систем	Руководитель разработок	Руководитель администрации ИТ	Руководитель проектного офиса	Аудит совета безопасности
Обеспечить соответствие ИТ инфраструктуры предлагаемым услугам, поддерживающим бизнес процессам		К	В	У	К	К	К	К	О	К	
Определить все ИТ затраты (на персонал, технологии) и соответствие их ИТ услугам из расчета на каждое подразделение		К		У		К	К	К	О	В	
Создать и поддерживать бухгалтерский учет в области ИТ и процесс контроля затрат		К	К	У	К	К	К	К	О	В	
Создать и поддерживать политики и процедуры финансирования		К	К	У	К	В	К	К	О	К	

В таблице ОУКИ показано, кто является Ответственным, Утверждающим, Консультирующим и/или Информированным



Модель зрелости

Управление процессом *«Определение и распределение затрат»* удовлетворяет следующим бизнес требованиям к ИТ *обеспечение прозрачности, понимание ИТ затрат и совершенствование эффективности затрат посредством должного информирования об использовании ИТ услуг* и соответствует характеристикам:

0. Несуществующий

Полное отсутствие процесса идентификации и распределения затрат по информационным услугам. Организация не осознает наличие проблемы, связанной с учетом затрат, поэтому данная проблема даже не обсуждается.

1. Начальный/Повторяющийся эпизодически и бессистемно

Имеется общее понимание о затратах на информационные услуги, но без их разбивки по пользователям, клиентам, подразделениям, группам пользователей, функциям обслуживания, проектам или поставляемым продуктам. Фактически, нет никакого контроля над затратами, руководству сообщают только сумму совокупных затрат. Затраты на ИТ воспринимаются как эксплуатационные накладные расходы. Бизнес не получает информации о затратах или выгодах от предоставления услуг.

2. Повторяющийся, но интуитивный

Имеется общее понимание необходимости определения и распределения затрат. Распределение затрат основано на неформальных или недостаточно развитых исходных предположениях по затратам, например, по затратам на аппаратное обеспечение. Отсутствует какая либо связь с факторами, определяющими пользу для бизнеса. Процессы распределения затрат являются воспроизводимыми и некоторые из них начинают контролироваться. Не проводится никакого формально организованного обучения и обсуждения вопросов стандартизации процедур определения и распределения затрат. Не назначены ответственные лица.

3. Определенный

Определена и документально оформлена модель затрат на ИТ услуги. Определен процесс взаимосвязи между затратами на ИТ и предоставляемыми услугами. Достигнут необходимый уровень понимания затрат на информационные услуги. Бизнес обеспечивается самыми элементарными сведениями о затратах на ИТ.

4. Управляемый и измеряемый

Порядок управления и порядок отчетности по затратам на информационные услуги определены и полностью осознаны на всех уровнях, поставлено формализованное обучение по данному вопросу. Определяются и регистрируются прямые и косвенные затраты, о них делаются соответствующие сообщения руководству, менеджерам бизнес процессов и пользователям. В целом существует мониторинг и оценка затрат, и в случае выявления

отклонений в затратах принимаются соответствующие меры. Отчетность о затратах на информационные услуги увязана с бизнес целями и соглашениями об уровне обслуживания и контролируется владельцами бизнес процессов. Существует система автоматизированного учета затрат, однако она в большей степени фокусируется на ИТ услугах, а не на бизнес процессах. Цели и показатели согласованы, но их измерение проводится непоследовательно. ***5. Оптимизированный***

Затраты на предоставленные услуги определяются, регистрируются, обобщаются и доводятся до сведения руководства, владельцев бизнес процессов и пользователей. Затраты идентифицированы как подлежащие оплате, поддерживается система компенсации затрат, позволяющая выставить счет пользователям за затраты, понесенные при предоставлении ИТ услуг. Подробная разбивка затрат содержится в соглашениях по уровням обслуживания. Мониторинг и оценка затрат на предоставление услуг применяются для оптимизации затрат на ИТ ресурсы. Полученные величины затрат используются при составлении бюджета организации. Сведения о затратах на ИТ услуги содержат заблаговременные предупреждения об изменении бизнес требований с помощью аналитических систем отчетности. Использование модели переменных затрат осуществляется с учетом объема каждой отдельной услуги. Управление затратами доведено до уровня лучших отраслевых практик, основанных на результатах непрерывного совершенствования и сопоставления с другими организациями. Оптимизация затрат является непрерывным процессом. Руководство анализирует цели и показатели в ходе постоянного совершенствования процесса управления затратами.

DS 7. Обучение и подготовка пользователей

Описание процесса

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.

Результативность	П
Эффективность	В
Конфиденциальность	
Целостность	
Доступность	
Соответствие требованиям	
Достоверность	

Управление процессом

Обучение и подготовка пользователей.

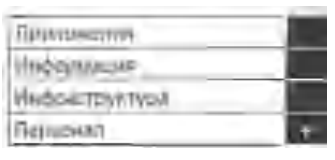
удовлетворяет следующим бизнес требованиям к ИТ

эффективное использование приложений и технологических решений, а также обеспечение выполнения пользователями требований политик и процедур.

сосредоточено на

четком понимании потребностей ИТ пользователей в обучении, реализации стратегии эффективного обучения и оценке его результатов. **достигается с помощью**

- Разработки учебного плана.
- Организации процесса обучения.
- Проведения обучения.
- Мониторинга и отчетности об эффективности обучения. **результаты оцениваются с помощью следующих показателей**
- Число обращений в службу поддержки по причине недостаточного обучения пользователей.
- Доля заинтересованных сторон, удовлетворенных полученным обучением.
- Временная задержка между выявлением потребности в обучении и предоставлением обучения по данному вопросу.



Цели контроля

DS 7.1. Определение потребностей в образовании и тренинге

Создание и регулярное обновление учебного плана для каждой целевой групп сотрудников учитывает следующие обстоятельства:

- Текущие и будущие бизнес потребности и стратегию.
- Ценность информации как актива.
- Корпоративные ценности (этические ценности, управление, культуру в области безопасности и т.д.).
- Внедрение новой ИТ инфраструктуры и 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

Обучение и тренинг основываются на выявленных потребностях, определении целевых групп и их состава, эффективных механизмах организации учебного процесса, преподавателях, тренерах и наставниках. Следует назначить тренеров и заблаговременно организовать занятия. Также необходимо вести учет регистрации на обучение, посещаемости и оценок эффективности учебной сессии.

DS 7.3. Оценкарезультатов обучения

По завершении курса обучения провести оценку актуальности, качества, эффективности, уровня усвоения знаний, затрат и пользы. Результаты данной оценки должны служить отправной точкой при разработке будущих учебных планов и организации учебных сессий.

Рекомендации по управлению

Из	Входящая информация
PO 7	Навыки и компетентность пользователей, включая индивидуальное обучение; специфические требования к обучению
AI 4	Учебные материалы, требования по передаче знаний для внедрения решений
DS 1	Соглашения операционного уровня
DS 5	Специфические требования к обучению по вопросам безопасности
DS 8	Данные об удовлетворенности пользователей

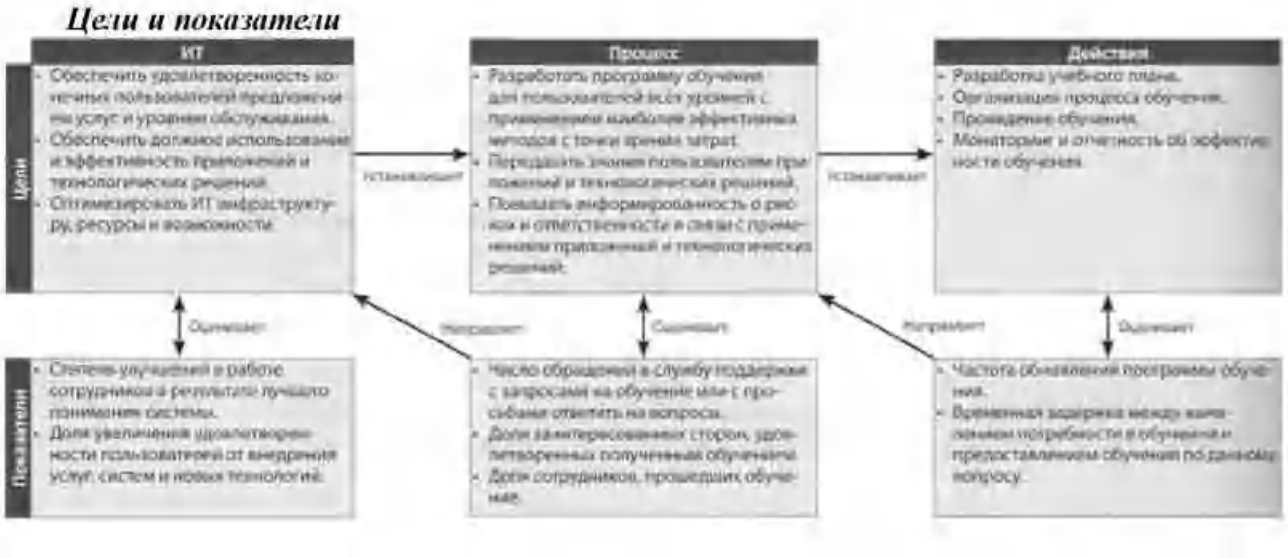
Результаты	В процессы						
Отчеты об эффективности процесса	ME 1						
Требования обновлению документации	AI 4						

Таблица ОУКИ

Действия ↓ / Функции →	Финансовый директор	Высшие руководители	Директор по ИТ	Владелец бизнес процесса	Руководитель эксплуатации систем	Главный архитектор ИТ-систем	Руководитель разработок	Руководитель администрации ИТ	Руководители проектного офиса	Аудит, риски, безопасность	Дальнейшие обучения
Определить и сформулировать потребности пользователей в обучении		К	У	О	К		К	К	К	К	О
Разработать программу учебного курса		К	У	О	К		К	К	К	И	О
Провести работу по информированию, обучению и тренингу		И	У	К	К		К	К	К	И	О
Провести оценку обучения		И	У	О	К		К	К	К	И	О
Определить и оценить лучшие методы и инструменты обучения		И	У/О	О	К		К	В	К	К	О

В таблице ОУКИ показано, кто является Ответственным, Утверждающим, Консультирующим и/или Информированным

Цели и показатели



Модель зрелости

Управление процессом *«Обучение и подготовка пользователей»* удовлетворяет следующим бизнес требованиям к ИТ *эффективное использование приложений и технологических решений, а также обеспечение выполнения пользователями требований политик и процедур* и соответствует характеристикам:

0. Несуществующий

Полное отсутствие каких либо программ подготовки или обучения персонала. Организация не осознает наличие проблемы, связанной с обучением. Этот вопрос даже не обсуждается.

1. Начальный/Повторяющийся эпизодически и бессистемно

Имеются факты, указывающие на то, что в организации осознали необходимость создания программы подготовки и обучения персонала, однако нет отлаженных процессов для решения данного вопроса. В условиях отсутствия организованной программы сотрудники самостоятельно находят нужные им курсы подготовки и посещают их. Некоторые из этих курсов дают подготовку по корпоративной этике, общим вопросам и практическим действиям по обеспечению безопасности

систем. Подходы руководства к вопросам обучения не согласованы. Отсутствует систематическое обсуждение вопросов подготовки и обучения персонала, не выработаны подходы к решению этих вопросов.

2. Повторяющийся, но интуитивный

Организация осознала необходимость создания программы подготовки и обучения персонала и разработки связанных с ней процессов в рамках всей организации. Пункты, связанные с обучением, начинают включать в индивидуальные планы оценки работы сотрудников. Процессы находятся на уровне, когда курсы подготовки и обучения персонала ведутся различными инструкторами на неформальной основе, используются разные подходы к обучению по одним и тем же предметам. Некоторые из этих курсов дают подготовку по корпоративной этике, общим вопросам и практическим действиям по обеспечению безопасности систем. Многое зависит от знаний отдельных сотрудников. Проводится систематическое обсуждение общих вопросов и степени необходимости подготовки и обучения персонала.

3. Определенный

Четко оформлены и доводятся до общего сведения программы подготовки и обучения персонала. Сотрудниками и руководителями определены и документально оформлены потребности в обучении. Стандартизованы и документально оформлены процессы подготовки и обучения персонала. Определены бюджеты, ресурсы, помещения и преподаватели, участвующие в программе обучения. Сотрудники проходят официальные курсы обучения по корпоративной этике, общим вопросам и практическим действиям по обеспечению безопасности систем. Для большей части процессов подготовки и обучения

персонала осуществляется текущий контроль, однако, руководство пока еще не отслеживает все отклонения от программ. Лишь в отдельных случаях выполняется анализ проблем, связанных с подготовкой и обучением персонала.

4. Управляемый и измеряемый

Существует комплексная программа подготовки и обучения персонала, дающая измеряемые результаты. Четко распределены обязанности и назначены лица, ответственные за учебные процессы. Уровень подготовки и обучения является составной частью карьерного роста сотрудника. Руководители оказывают поддержку подготовке и обучению персонала и сами посещают занятия. Все сотрудники проходят обучение по знанию кодекса этики и общим требованиям безопасности. Все сотрудники проходят подготовку по практическим действиям по обеспечению безопасности системы и защите от вреда, причиняемого отказами систем, которые могут оказать отрицательное воздействие на доступность и целостность, а также на конфиденциальность информации. Руководство осуществляет текущий контроль подготовки и обучения персонала, пересмотр и совершенствование учебных программ и процессов. При совершенствовании процессов используются лучшие практики, накопленные в организации.

5. Оптимизированный

Результатом подготовки и обучения персонала является повышение квалификации сотрудников. Уровень подготовки и обучения является основным компонентом карьерного роста сотрудников. Программы подготовки и обучения в достаточной степени обеспечены бюджетными средствами, необходимыми ресурсами, техническими средствами и преподавателями. Процессы уточняются и непрерывно совершенствуются с использованием лучших практик, накопленных в других организациях, разработки моделей развития и сравнительного анализа. Проводится анализ основных причин по всем возникающим проблемам и отклонениям от программ, по результатам которого определяются и принимаются соответствующие меры. Выработано общее положительное отношение к нормам корпоративной этики и знанию принципов обеспечения безгласности систем. Реализация программы подготовки и обучения персонала осуществляется при широком интегрированном и оптимальном использовании ИТ. Для обучения персонала привлекаются сторонние специалисты, в качестве ориентиров используются показатели других организаций.

DS 8. Управление службой технической поддержки и инцидентами Описание процесса

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.

Результативность	П
Эффективность	П
Конфиденциальность	
Целостность	
Доступность	
Соответствие требованиям	
Достоверность	

Управление процессом

Управление службой технической поддержки и инцидентами.

удовлетворяет следующим бизнес требованиям к ИТ

эффективное использование **ИТ** систем путем анализа и решения проблем пользователей, вопросов и инцидентов. **сосредоточено на**

создании профессиональной службы поддержки с быстрой реакцией на запросы пользователей, четкими процедурами информирования и разрешения инцидентов и анализом тенденций. **достигается с помощью**

- Создания и функционирования службы поддержки пользователей.
- Мониторинге и отчетности по выявленным тенденциям.
- Определении четких критериев и процедур разрешения инцидентов. **результаты оцениваются с помощью следующих показателей**
- Доля пользователей, удовлетворенных службой поддержки «первой линии».
- Доля инцидентов, разрешенных в течение согласованного/приемлемого срока.
- Доля запросов, оставшихся без ответа.

Приложения	+
Информация	
Инфраструктура	
Персонал	+

Цели контроля

DS 8.1. Служба технической поддержки

Создать службу технической поддержки, являющуюся зоной взаимодействия пользователей и ИТ, которая призвана регистрировать, распределять и анализировать все обращения, докладывать об инцидентах, требованиях оказания услуг и запросах на информацию. Должен быть налажен мониторинг и процедуры разрешения инцидентов, основанные на принятых уровнях обслуживания в соответствии с соглашением об уровне обслуживания, которые дают возможность классифицировать и расставить приоритеты в отношении всех инцидентов, запросов о поддержке или об информации. Замерять удовлетворенность конечных пользователей качеством работы службы технической поддержки и ИТ услуг.

DS 8.2. Регистрация запросов

Создать функцию и систему, позволяющие учитывать и отслеживать обращения, инциденты, запросы о поддержке или об информации. Регистрация должна быть тесно связана с процессами управления инцидентами, управления проблемами, управления изменениями, управления мощностями и управления доступностью. Инциденты должны классифицироваться в соответствии с

корпоративными и сервисными приоритетами и направляться к соответствующей группе решения проблем. Пользователи должны быть в курсе текущего статуса своих запросов.

DS 8.3. Разрешение инцидентов

Разработать процедуры службы поддержки, предусматривающие управляемое разрешение инцидентов, которые не могут быть ликвидированы незамедлительно. Инцидент может быть разрешен в пределах, установленных соглашением об уровне обслуживания, в случае необходимости, могут предлагаться временные решения или альтернативные варианты. Следует убедиться в том, что «права владения» инцидентами и надзор за ними закреплены за службой технической поддержки для всех инцидентов пользователей, вне зависимости от того, какая ИТ группа работает над их решением.

DS 8.4. Закрытие инцидента

Разработать процедуры оперативного мониторинга по окончательному разрешению запросов пользователей. После разрешения инцидента следует убедиться в том, что служба поддержки зафиксировала механизм решения и подтвердила отсутствие претензий пользователя. Также необходимо вести учет и докладывать о неразрешенных инцидентах (известных ошибках и временных решениях), чтобы обеспечить надлежащей информацией процесс управления проблемами.

DS 8.5. Отчетность и анализ тенденций

Следует вести учет работы службы поддержки, чтобы руководство имело возможность оценить ее эффективность, время ответа службы поддержки на запросы и выявить тенденции или повторяющиеся проблемы. Это необходимо для постоянного совершенствования службы поддержки.

Рекомендации по управлению

Из	Входящая информация
AI 4	Пользовательские, эксплуатационные, поддерживающие, технические и руководства администраторов
AI 6	Авторизация изменений
AI 7	Перечень конфигураций
DS 1	Соглашения об уровне обслуживания и соглашения операционного уровня
DS 4	Предельные значения для инцидентов/аварийных ситуаций
DS 5	Определение инцидентов в сфере безопасности
DS 9	ИТ конфигурация/подробности по затратам
DS 10	Известные проблемы, ошибки и временные решения
DS 13	Билеты инцидентов

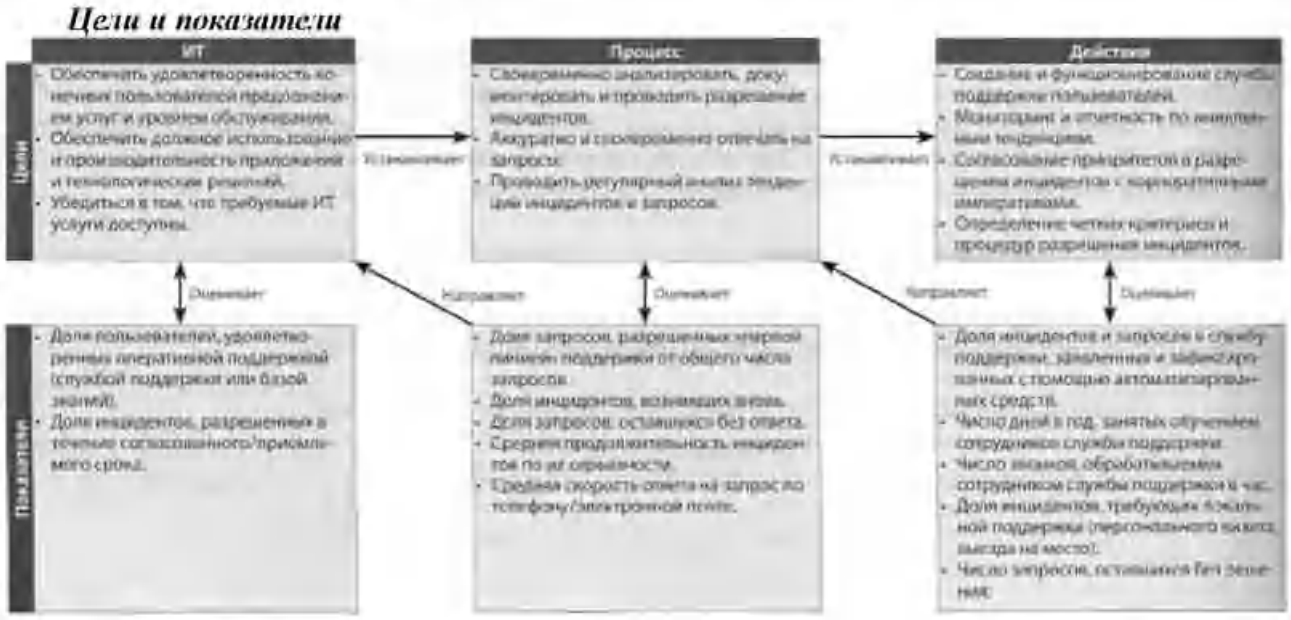
Результаты	В процессы						
Запросы о поддержке/запросы на изменения	AI 6						
Отчеты об инцидентах	DS 10						
Отчеты об эффективности процессов	ME 1						
Отчеты об удовлетворенности пользователя	DS 7	ME 1					

Таблица ОУКИ

Действия ↓ / Функция →	Президент	Высшее руководство	Директор по ИТ	Владелец бизнес процесса	Руководитель эксплуатации системы	Главный архитектор ИТ систем	Руководитель разработок	Руководитель администрации ИТ	Руководитель проектного офиса	Аудит, риски, безопасность	Менеджмент ИТ-инцидентами
Создать классификацию (РСО серьезности и последствиям) и мобилизационные процедуры (функциональные и иерархические)			К	К	К	К	К	К		К	У/О
Выявить и вести учет инцидентов/ запросов о поддержке/ запросов об информации											У/О
Вести классификацию, расследование и диагностику запросов			И		К	К	К			И	У/О
Осуществлять ликвидацию, восстановление и полное разрешение инцидентов				И	О	О	О			К	У/О
Информировать пользователей (например о статусе обновлений)			И	И							У/О
Вести отчетность	И		И	И	И			И		И	У/О

В таблице ОУКИ показано, кто является Ответственным, Утверждающим, Консультирующим и/или Информированным

Цели и показатели



Модель зрелости

Управление процессом *«Управление службой технической поддержки и инцидентами»* удовлетворяет следующим бизнес требованиям к ИТ эффективное *использование ИТ систем путем анализа и решения проблем пользователей, вопросов и инцидентов* и соответствует характеристикам:

0. Несуществующий

Отсутствуют средства поддержки, обеспечивающие ответы на вопросы и проблемы, с которыми сталкиваются пользователи. Управление инцидентами полностью отсутствует. В организации еще не осознана необходимость поддержки пользователей.

1. Начальный/Повторяющийся эпизодически и бессистемно

Организация осознала, что для ответа на вопросы пользователей и решения возникающих у них проблем требуется процесс, поддерживаемый инструментальными средствами и персоналом. Однако, стандартизованный процесс, отсутствует. Поддержка оказывается в порядке реагирования на возникающие проблемы. Руководство не осуществляет текущий контроль за проблемами пользователей и связанными с ними тенденциями. Не разработан процесс, предусматривающий разрешение инцидентов и эскалации на следующий уровень поддержки для обеспечения решения возникающих проблем.

2. Повторяющийся, но интуитивный

В организации осознана необходимость создания службы поддержки пользователей и процесса управления инцидентами. Помощь пользователям предоставляется на неформализованной основе сотрудниками, обладающими специальными знаниями. Они располагают некоторыми инструментальными средствами, которые могут быть использованы для оказания помощи пользователям в решении возникающих у них проблем. Отсутствуют формальное обучение и взаимодействие как стандартные процедуры, ответственность лежит на отдельных сотрудниках.

3. Определенный

Осознана и признана необходимость создания службы поддержки пользователей и процесса управления инцидентами. Стандартизованы и документально оформлены процедуры. Обучение осуществляется на неформальном уровне. Однако решение вопросов обучения и соблюдения стандартов предоставлено отдельным сотрудникам. Разработана база данных на основе часто задаваемых вопросов, содержащая ответы на эти вопросы, подготовлены рекомендации для пользователей. Однако отдельные сотрудники должны искать ответы на вопросы и могут не всегда следовать им. Отслеживание вопросов и проблем осуществляется вручную, текущий контроль ведется в отдельных случаях, отсутствует формализованная система отчетности. Не фиксируется время реагирования на возникшие вопросы и инциденты. Возможны ситуации, когда возникшие запросы и инциденты не решаются. Пользователи имеют четкие инструкции когда и как сообщать о проблемах и инцидентах.

4. Управляемый и измеряемый

На всех уровнях организации имеется полное понимание всех выгод создания службы поддержки пользователей и процесса управления инцидентами. Эта функция уже действует в соответствующих подразделениях организации. Инструментальные средства и методы автоматизированы, осуществлена централизация базовых знаний по возникающим инцидентам и их решениям. Персонал службы поддержки пользователей тесно взаимодействует с сотрудниками, ответственными за управление проблемами. Четко распределены обязанности, осуществляется текущий контроль эффективности. Установлены и доведены до сведения сотрудников процедуры обсуждения и комплексного решения проблем. Подготовлен и обучен персонал службы поддержки пользователей, процессы усовершенствованы за счет использования программного обеспечения, ориентированного на конкретную задачу. Руководство разрабатывает показатели для оценки эффективности работы службы поддержки пользователей.

5. Оптимизированный

Внедрено и хорошо организовано функционирование службы поддержки пользователей и процесса управления инцидентами. Показатели работы службы систематически измеряются, по ним налажена отчетность. База ответов на часто задаваемые вопросы представляет собой обширную, всестороннюю базу знаний. Имеются инструментальные средства, дающие пользователю возможность самостоятельной диагностики и решения проблем. Советы, получаемые пользователями, непротиворечивы, проблемы решаются быстро, в рамках структурированного процесса развития инцидента. Для получения статистики эффективности работы службы поддержки руководство применяет интегрированные инструменты. В результате анализа показателей эффективности,

постоянного совершенствования и сопоставления с другими организациями процессы доведены до уровня лучших отраслевых практик.

DS 9. Управление конфигурацией

Описание процесса

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.

Результативность	П
Эффективность	В
Конфиденциальность	
Целостность	
Доступность	В
Соответствие требованиям	
Достоверность	В

Управление процессом

Управление конфигурацией.

удовлетворяет следующим бизнес требованиям к ИТ

оптимизация ИТ инфраструктуры, ресурсов и возможностей, учет ИТ активов.

сосредоточено на

создании и поддержке точного и полного хранилища конфигурационных атрибутов ИТ активов и прототипов, а также на сравнении их с текущей конфигурацией. **достигается с помощью**

- Создания централизованного хранилища всех объектов конфигурации.
- Выявления объектов конфигурации и их поддержке.
- Проверки целостности данных о конфигурации. **результаты**

оцениваются с помощью следующих показателей

- Число проблем, связанных с соответствием требованиям бизнеса, вызванных неправильной конфигурацией активов.
- Число отклонений, выявленных между конфигурационными данными в хранилище и текущей конфигурацией активов.
- [1] Доля приобретенных, но не учтенных в хранилище лицензий.

Приоритетное	Второстепенное

Приложения	+
Информация	+
Инфраструктура	+
Персонал	

Цели контроля

DS 9.1. Хранилище конфигурационных данных и прототип

Создать средства поддержки и централизованное хранилище, в которое должна помещаться все информация, имеющая отношение к объектам конфигурации. Следует вести мониторинг и учет всех активов и изменений в них. Поддерживать прототипы для объектов конфигурации всех систем и услуг в качестве контрольной точки, к которой можно вернуться после совершения изменений.

DS 9.2. Идентификация и обслуживание объектов конфигурации

Разработать процедуры конфигурации для поддержки управления и документирования всех изменений в хранилище конфигурационных данных. Интегрировать данные процедуры с процессами управления конфигурацией, управления инцидентами и управления проблемами.

DS 9.3. Проверка целостности конфигурации

Периодически проверять конфигурационные данные и подтверждать целостность конфигурации в настоящем и прошлом. Периодически проверять установленное программное обеспечение на предмет соответствия политике использования ПО, либо использования нелицензионного ПО либо иных случаев

использования ПО не в соответствии с условиями контрактов. Следует вести отчетность и предпринимать действия по исправлению ошибок и отклонений.

Рекомендации по управлению

Из	Входящая информация
AC 4	Пользовательские, операционные, поддерживающие, технические и руководства администраторов
AC 7	Распространенные объекты конфигурации
DS 4	Критичность объектов ИТ конфигурации

Результаты	В процессы						
ИТ конфигурации/детализации по ИТ активам	DS 8	DS 10	DS 13				
Запросы на изменения (где и как производить исправления)	AI 6						
Отчеты об эффективности процессов	ME 1						

Таблица ОУКИ

Действия ↓ / Функции →	Президент	Финансовый директор	Директор по ИТ	Владелец бизнес процесса	Руководитель эксплуатации системы	Главный архитектор ИТ-систем	Руководитель разработок	Руководитель администрации ИТ	Руководитель проектного офиса	Аудит, риски, безопасность	Менеджер по конфигурации
Разработать процедуры планирования управления конфигурацией				К	У	У	И	К		К	О
Вести сбор первичных данных о конфигурации и разрабатывать прототипов					К	У	К			И	У/О
Осуществлять проверку и аудит данных о конфигурации (включая выявление нелегитимного программного обеспечения)		И			У			И		И	У/О
Обновлять хранилище конфигурационных данных					О	О	О			И	У/О

В таблице ОУКИ показано, кто является Ответственным, Утверждающим, Консультирующим и/или Информированным

Цели и показатели

Модель зрелости

Управление процессом *«Управление конфигурацией»* удовлетворяет следующим бизнес требованиям к ИТ *оптимизация ИТ инфраструктуры, ресурсов и возможностей, учет ИТ активов* и соответствует характеристикам:

0. Несуществующий

Руководство не осознает преимуществ наличия процесса учета и управления ИТ инфраструктурой применительно к конфигурациям как аппаратного, так и программного обеспечения.

1. Начальный/Повторяющийся эпизодически и бессистемно

Осознана необходимость управления конфигурацией. Базовые задачи по управлению конфигурацией, такие как ведение реестров аппаратного и программного обеспечения, решаются лишь в отдельных случаях. Стандартные методы не применяются.

2. Повторяющийся, но интуитивный

Руководство осознает выгоды управления ИТ конфигурацией и понимает преимущества точной и полной конфигурационной информации, однако, полностью полагается на знания и опыт технического персонала. В некоторой степени применяются инструментальные средства управления конфигурацией, однако, они различны для разных платформ. Более того, не определены стандартные методы работы. Состав данных по конфигурации ограничен и не используется взаимосвязанными процессами, например управлением изменениями и управлением проблемами.

3. Определенный

Документально оформлены, стандартизованы и доведены до общего сведения процедуры и методы работы, однако, вопросы обучения и применения стандартов решаются самостоятельно отдельными сотрудниками. Кроме того, для разных платформ используются одинаковые инструментальные средства управления конфигураций. Вероятность обнаружения отклонений от процедур мала, проверки физического наличия компонентов осуществляются нерегулярно. Отслеживание изменений в оборудовании и программном обеспечении кое-где автоматизировано. Данные по конфигурации используются взаимосвязанными процессами.

4. Управляемый и измеряемый

Необходимость управления конфигурацией полностью осознана на всех уровнях организации. Продолжается накопление лучших практик. Процедуры и стандарты доведены до сведения исполнителей и включены в курс обучения. Отклонения от них контролируются, отслеживаются и отражаются в отчетности. Для внедрения стандартов и повышения устойчивости применяются автоматизированные инструментальные средства, например, такие как технология принудительного обновления. Системы управления конфигурацией охватывают наибольшую часть ИТ инфраструктуры и обеспечивают возможность надлежащего управления выпусками новых версий программных продуктов и контроля за их распределением. Регулярно выполняется анализ исключений, а также проверки физического наличия компонентов, проводится анализ первопричин.

5. Оптимизированный

В рамках системы управления конфигурацией, которая содержит всю необходимую информацию о компонентах, их взаимосвязи и событиях, осуществляется управление всеми ИТ активами. Каталоги поставщиков и данные по конфигурации соответствуют друг другу. Связанные процессы полностью интегрированы, они используют и обновляют данные по конфигурации в автоматическом режиме. В отчетах о проверках приводятся данные по ремонту, исправлению, обслуживанию, гарантийных сроках, обновлению и технической оценке по наиболее важным аппаратным и программным средствам каждого отдельного подразделения. Внедрены меры, ограничивающие установку неавторизованных программ. Руководство предвидит необходимость ремонта или модификации на основе анализа сообщений о предусмотренных графиком сроках модификации технологии и технических возможностях ее обновления. Мониторинг ресурсов и текущий контроль отдельных рабочих

станций позволяют обеспечить защиту ресурсов и предотвратить возможность их хищения, неправильного использования или эксплуатации с нарушением установленных режимов.

DS 10. Управление проблемами

Описание процесса

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.

Результативность	П
Эффективность	П
Конфиденциальность	
Целостность	
Доступность	В
Соответствие требованиям	
Достоверность	

Управление процессом

Управление проблемами.

удовлетворяет следующим бизнес требованиям к ИТ

обеспечение удовлетворенности конечных пользователей предложением услуг и уровнями обслуживания, сокращение дефектов и переделок в предлагаемых услугах.

сосредоточено на

Учёте, отслеживании и разрешении проблем в среде промышленной эксплуатации; анализе первопричин всех существенных проблем и определении путей решения выявленных эксплуатационных проблем. **достигается с помощью**

- Проведения анализа первопричин выявленных проблем.
- Анализа тенденций.
- Назначения владельцев проблем и интенсификации их решения. **результаты оцениваются с помощью следующих показателей**
- Число повторяющихся проблем, имеющих последствия для бизнеса.
- Доля проблем, решенных в течение определенного периода времени.
- Регулярность отчетов или обновлений, касающихся текущих проблем, ранжированных по их серьезности.

Приоритетное Второстепенное

Приложения	+
Информация	+
Инфраструктура	+
Персонал	+

Цели контроля

DS 10.1. Выявление и классификация проблем

Реализовать на практике отчетность и классификацию проблем, которые были выявлены в ходе процесса управления инцидентами. Этапы этой работы аналогичны классификации инцидентов; то есть проблемам нужно присвоить категории, определить последствия, срочность и приоритетность. Категорировать проблемы по группам или разделам (например, проблемы в аппаратном обеспечении, программах, поддержке программ). Эти группы должны соответствовать организационным обязанностям пользователей и являться основой для постановки задач перед персоналом службы поддержки.

DS 10.2. Отслеживание иразрешение проблем

Следует убедиться в том, что система управления проблемами обеспечена необходимыми средствами по отслеживанию, анализу и определению первопричин всех выявленных проблем, включая:

- Все связанные объекты конфигурации.
- Неразрешенные проблемы и инциденты.
- Известные и предполагаемые ошибки.

- Отслеживание тенденций в проблемах.

Выявить и предложить поддерживающие решения в отношении первопричин проблем, вызывающие запросы на изменения в процессе управления изменениями. Через процесс решения, управление проблемами должно получать регулярные отчеты от управления изменениями по разрешению проблем и ошибок. Управление проблемами предполагает ведение мониторинга постоянного воздействия проблем и выявленных ошибок на сервисы для пользователей. В случае достижения неприемлемого уровня данного воздействия, управление проблемами должно осуществить эскалацию проблемы, возможно повысив ее приоритет или предпринять экстренные изменения. Отслеживать продвижение в решении проблем в рамках соглашений об уровне обслуживания.

DS 10.3. Закрытие проблем

Предусмотреть процедуру окончательного решения проблемы либо после 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 и проблемами

Осуществить интеграцию процессов управления конфигурацией, управления инцидентами и проблемами для обеспечения эффективного управления проблемами и совершенствования.

Рекомендации по управлению

Из	Входящая информация
AI 6	Авторизация изменений
DS 8	Отчеты об инцидентах
DS 9	Детальная ИТ конфигурация/ИТ активы
DS 13	Протоколы ошибок

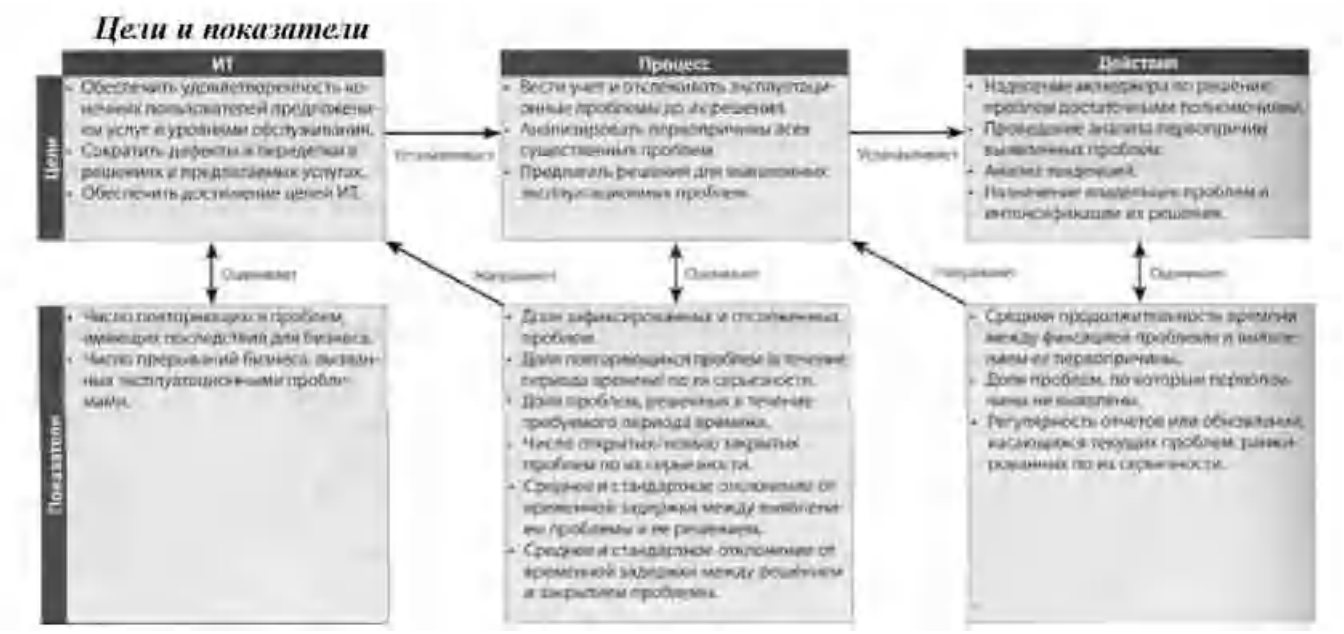
Результаты	В процессы						
Запросы на изменение (где и как осуществить исправления)	AI 6						
Протоколы проблем	AI 6						
Отчеты об эффективности процесса	ME 1						
Выявленные проблемы, ошибки и временные способы их решения	DS 8						

Таблица ОУКИ

Действия ↓ / Функции →	Президент	Высшее руководство	Директор по ИТ	Владелец бизнес-процесса	Руководитель эксплуатации систем	Главный архитектор ИТ систем	Руководитель разработок	Руководитель администрации ИТ	Руководитель проектного офиса	Аудит, риски, безопасность	Менеджер по проблемам
Выявлять и классифицировать проблемы		И	И	К	У	К	К			И	О
Провести анализ первопричин					К		К				И,О
Разрешить проблемы				К	У	О	О		О	К	К
Отслеживать статус проблем		И	И	К	У,О	Б	И		К	К	О
Предложить рекомендации по улучшению и создать запросы на изменения				И	У	И	И		И		О
Поддерживать протоколы проблем				И	И		И			И	У,О

В таблице ОУКИ показано, кто является Ответственным, Утверждающим, Консультирующим и/или Информированным

Цели и показатели



Модель зрелости

Управление процессом *«Управление проблемами»* удовлетворяет следующим бизнес требованиям к ИТ *обеспечение удовлетворенности конечных пользователей предложением услуг и уровнями обслуживания, сокращение дефектов и переделок в предлагаемых услугах* и соответствует характеристикам:

0. Несуществующий

Нет понимания необходимости в управлении проблемами, так же как и в классификации проблем и инцидентов. Поэтому нет и попыток выявить первопричины инцидентов.

1. Начальный/Повторяющийся эпизодически и бессистемно

Персонал осознает необходимость управления проблемами и устранения их первопричин. Ведущие сотрудники, обладающие наибольшим багажом знаний, оказывают помощь по решению проблем, связанных с областью их знаний, но обязанности в этой сфере не определены. Нет обмена информацией с другими сотрудниками, что приводит к созданию дополнительных проблем и к непродуктивным затратам времени на поиск ответов.

2. ***Повторяющийся, но интуитивный***

Имеется повсеместное понимание необходимости и преимуществ управления ИТ проблемами, как в бизнес подразделениях, так и в службе ИТ. Процесс решения проблем развит до уровня, когда несколько ведущих сотрудников несут ответственность за выявление и решение возникших проблем. Налажен неформальный и являющийся реакцией на случившиеся события обмен информацией среди персонала. Уровень обслуживания пользователей непостоянен и ограничен недостаточно систематизированными знаниями, имеющимися у менеджера по решению проблем.

3. ***Определенный***

Потребность в эффективной системе управления проблемами признана и подкреплена поддержкой руководства, бюджетными ассигнованиями на оплату труда персонала и обучением. Процессы решения проблем и мобилизации ресурсов для их решения стандартизованы. Отчетность, отслеживание проблем и их решение группой реагирования носят фрагментарный характер с использованием имеющихся инструментальных средств, без централизации. Вероятность обнаружения отклонений от принятых норм или стандартов незначительна. Распространение информации среди персонала формализовано и ведется с

упреждением событий. Анализ, проводимый руководством в отношении инцидентов, выявления проблем и их решения ограничен и не формализован.

4. Управляемый и измеряемый

Процесс управления проблемами осознан на всех уровнях организации. Четко определены ответственные лица и владельцы процессов. Документально оформлены и доведены до сведения сотрудников необходимые методы и процедуры, проводится оценка их эффективности. Выявлено и зарегистрировано большинство возникающих проблем, по которым подготовлены соответствующие отчеты и приняты корректирующие меры. Приобретаются и накапливаются необходимые знания и опыт, которые переходят на более высокий уровень и рассматриваются как актив и главный фактор, способствующий достижению целей, стоящих перед ИТ. Управление проблемами сильно взаимосвязано с такими родственными процессами, как управление инцидентами, изменениями, доступностью и конфигурацией, а, кроме того, оказывает помощь потребителям ИТ услуг в управлении данными, оборудованием и операциями. Цели и показатели согласованы с руководством процесса управления проблемами.

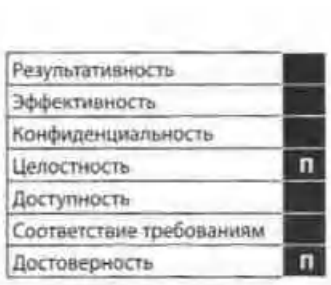
5. Оптимизированный

Процесс управления проблемами приобрел упреждающий и профилактический характер. Он вносит свой вклад в достижение целей, стоящих перед ИТ. Сотрудники готовы к возникновению проблем и могут их предотвращать. Уровень знаний характерных особенностей прошлых и будущих проблем поддерживается благодаря регулярным контактам с поставщиками и экспертами. Регистрация проблем и инцидентов, отчетность о них, а также их анализ автоматизированы и полностью интегрированы с управлением данными по конфигурации. Достижение целей постоянно оценивается. Большинство систем оснащены механизмом обнаружения и предупреждения, который постоянно контролируется и подвергается оценке. Процесс управления проблемами изучается для постоянного совершенствования на основе анализа контрольных показателей, результаты анализа докладываются заинтересованным сторонам.

DS 11. Управление данными

Описание процесса

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.



Управление процессом

Управление данными.

удовлетворяет следующим бизнес требованиям к ИТ

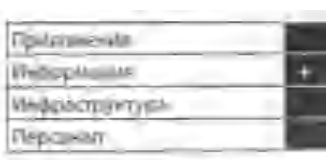
оптимизация использования информации и обеспечение доступности информации по требованию. **сосредоточено на**

обеспечении полноты, точности, доступности и защищенности данных. **достигается с помощью**

- Резервного копирования данных и тестирования их способности к во станов лению.
- Управления внутренними и удаленными хранилищами данных.
- Безопасным уничтожением данных и оборудования. **результаты**

оцениваются с помощью следующих показателей

- Доля пользователей, удовлетворенных доступностью данных.
- Доля случаев успешного восстановления данных.
- Число инцидентов, при которых важные данные были доступны после списания носителей данных.



| Приоритетное ! ___! Второстепенное

Цели контроля

DS 11.1. Бизнес требования куправлению данными

Следует проверить, чтобы все данные, предназначенные для обработки, были получены и обработаны в полном объеме, точно и своевременно, а результаты обработки соответствовали бизнес требованиям. Обеспечить поддержку перезапуска и повторной обработки.

DS 11.2. Запись и хранение

Определить и реализовать на практике процедуры эффективного и производительного хранения, записи и архивирования данных в соответствии с бизнес целями, корпоративной политикой безопасности и регулятивными требованиями.

DS 11.3. Управление библиотекой носителей данных

Определить и реализовать на практике инвентаризацию архива носителей данных, чтобы удостовериться в их исправности и целостности. ***DS 11.4. Вывод из эксплуатации (списание)***

Определить и реализовать на практике процедуры, отвечающие бизнес требованиям по защите важных данных и программ при списании или передаче оборудования и данных. ***DS 11.5. Резервноехранение и восстановление***

Определить и реализовать на практике процедуры резервного хранения и восстановления систем, приложений, данных и документации, соответствующие бизнес требованиям и плану обеспечения непрерывности обслуживания.

DS 11.6. Требования по безопасности куправлению данными

Сформулировать и реализовать на практике политики и процедуры определения и применения требований по безопасности в отношении приема, обработки, хранения и вывода данных, соответствующие бизнес целям, корпоративной политике безопасности и регулятивным требованиям.

Из	Входящая информация
PO 2	Справочник данных; утвержденные классификации данных
AI 4	Пользовательские, операционные, поддерживающие, коммерческие и руководства администраторов
DS 1	Соглашения операционного уровня
DS 4	План резервного хранения и защиты
DS 5	План и политика ИТ безопасности

Результаты	В процессы					
Отчеты об эффективности процесса	ME 1					
Инструкции операторов по управлению данными	DS 13					

Таблица ОУКИ

Действия ↓ / Функции →	Президент	Финансовый директор	Высшее руководство	Директор по ИТ	Владелец бизнес процесса	Руководитель эксплуатации систем	Главный архитектор ИТ систем	Руководитель разработок	Руководитель администрации ИТ	Руководитель проектного офиса	Аудит/риски безопасности
Преобразовать требования по хранению данных и восстановлению в процедуры				У	И	К	У				К
Определить, поддерживать и реализовывать процедуры по управлению библиотекой носителей данных				У		У	К	К	И		К
Определить, поддерживать и реализовывать процедуры по безопасному уничтожению носителей данных и оборудования				У	К	У			И		К
Осуществлять плановое резервное копирование				У		У					
Определить, поддерживать и реализовывать процедуры по восстановлению данных				У	К	У	К	К			И

В таблице ОУКИ показано, кто является Ответственным, Утверждающим, Консультирующим и/или Информированным

Рекомендации по управлению

Модель зрелости

Управление процессом *«Управление данными»* удовлетворяет следующим бизнес требованиям к ИТ *оптимизация использования информации и обеспечение доступности информации по требованию* и соответствует характеристикам:

0. Несуществующий

Нет осознания того факта, что данные являются корпоративным ресурсом и активом. Не назначены владельцы данных и лица, ответственные за управление данными. Качество и безопасность данных находятся на низком уровне или вообще отсутствуют.

1. Начальный/Повторяющийся эпизодически и бессистемно

Организация осознает необходимость в наличии эффективного управления данными. От случая к случаю происходит определение требований по безопасности к управлению данными, но не существует формализованных процедур информирования. Не проводится специального обучения по управлению данными. Ответственность за управление данными не определена. Существуют процедуры резервного копирования, восстановления данных и списания носителей данных.

2. Повторяющийся, но интуитивный

В организации осознается необходимость эффективного управления данными. Появляются владельцы данных. Требования по безопасности в сфере управления данными документально оформлены ведущими специалистами. В службе ИТ проводится определенный мониторинг по основным действиям с данными (например, резервное копирование, восстановление, уничтожение). Обязанности в сфере управления данными неформально переданы ведущим сотрудникам ИТ службы.

3. Определенный

Необходимость управления данными осознана и принята данных всей организацией. Назначены обязанности в сфере управления данными. Определены владельцы данных, а также стороны,

ответственные за обеспечение целостности и безопасности данных. Процедуры по управлению данными формализованы в рамках службы ИТ, применяются некоторые автоматизированные средства для резервирования/восстановления и вывода из эксплуатации оборудования. Ведется определенный мониторинг в сфере управления данными. Определены основные показатели эффективности. Начинает проводиться обучение персонала по вопросам управления данными.

4. Управляемый и измеряемый

Потребность в управлении данными осознана, в организации предприняты необходимые меры в этой области. Четко определены, назначены и доведены до сведения сотрудников организации лица, ответственные за владение данными. Процедуры формализованы и широко известны, ведется распространение знаний. Начинается применение современных автоматизированных средств. Показатели цели и эффективности

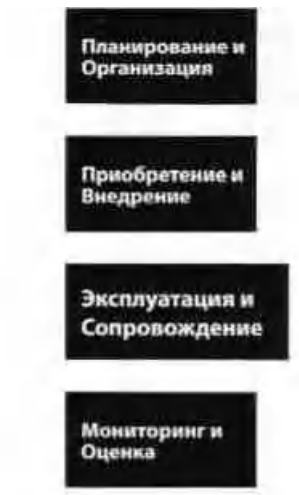
согласованы с потребителями и отслеживаются в рамках четко определенного процесса. Существует формализованное обучение персонала по вопросам управления данными. ***5. Оптимизированный***

Потребность в управлении данными и понимании всех необходимых действий осознана и принята в рамках организации. Будущие потребности выявляются и учитываются заранее. Четко определены, назначены и доведены до сведения сотрудников организации лица, ответственные за владение данными, сведения об этом своевременно обновляются. Процедуры формализованы и широко известны, распространение знаний стало обычной практикой. Применяются комплексные средства управления данными с максимальным уровнем автоматизации. Показатели цели и эффективности согласованы с потребителями, связаны с целями бизнеса и постоянно отслеживаются в рамках четко определенного процесса. Постоянно изыскиваются возможности для совершенствования. Внедрено обязательное формализованное обучение персонала по вопросам управления данными.

DS 12. Управление Физической безопасностью и зашитой от воздействия окружающей среды

Описание процесса

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.



Результативность	
Эффективность	
Конфиденциальность	
Целостность	П
Доступность	П
Соответствие требованиям	
Достоверность	

Управление процессом

Управление физической безопасностью и защитой от воздействия окружающей среды.

удовлетворяет следующим бизнес требованиям к ИТ

защита компьютерных активов и корпоративных данных и минимизация риска сбоев в работе организации. **сосредоточено на**

обеспечении и поддержке подходящих физических условий для защиты ИТ активов от несанкционированного доступа, ущерба или кражи. **достигается с помощью**

- Внедрения показателей физической безопасности.
- Выбора и управления объектами (зданиями и сооружениями).

результаты оцениваются с помощью следующих показателей

- Количество простоев, вызванных инцидентами в физической среде.
- Число инцидентов, вызванных нарушениями требований физической безопасности или ошибками.
- Регулярность анализа и оценки физических рисков.

Приложения	
Информация	
Инфраструктура	
Персонал	

Цели контроля

DS 12.1. Выбор места и проектирование

Определить и выбрать помещения для размещения ИТ оборудования, которое должно осуществлять поддержку технологической стратегии, связанной с корпоративной стратегией. Выбор и проектирование помещений должно учитывать риски, связанные с природными и антропогенными чрезвычайными ситуациями, при соблюдении соответствующего законодательства и регулирующих требований, в частности, по технике безопасности и охране здоровья.

DS 12.2. Показатели физической безопасности

Определить и внедрить показатели физической безопасности, соответствующие бизнес требованиям к безопасности места и физическим активам. Показатели физической безопасности должны быть применимы для оценки эффективного предотвращения, выявления и минимизации рисков, связанных с кражей, тепловым воздействием, пожаром, задымлением, затоплением, вибрацией, актами терроризма, вандализма, перебоями в подаче напряжения, воздействием химических или взрывчатых веществ.

DS 12.3. Физический доступ

Определить и реализовать на практике процедуры предоставления, ограничения и прекращение доступа в помещения, здания и территории в соответствии с бизнес потребностями, включая действия при чрезвычайных ситуациях. Доступ в помещения, здания и территории должен быть обоснован, разрешен, учтен и подвергнут проверке. Это относится ко всем лицам, входящим в помещения, включая персонал, временный персонал, клиентов, поставщиков, посетителей или любых других представителей третьей стороны.

DS 12.4. Защита от факторов окружающей среды

Спланировать и реализовать на практике меры по защите от факторов окружающей среды. Установить специализированное оборудование и устройства по мониторингу и контролю среды.

DS 12.5. Управление физическими объектами

Управлять объектами, включая энергетическое и коммуникационное оборудование, в соответствии с законодательством и регулирующими нормами, техническими и бизнес требованиями, спецификациями поставщиков, руководящими указаниями по технике безопасности и охране здоровья.

Рекомендации по управлению

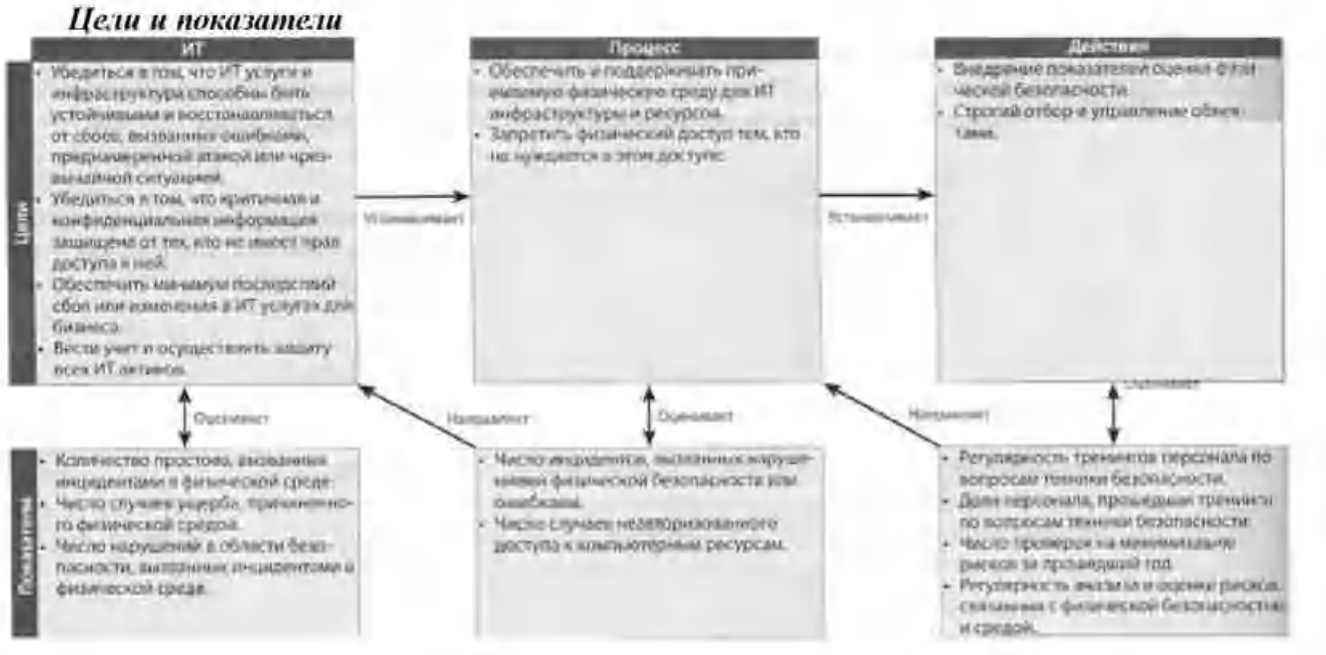
Из	Входящая информация	Результаты	В процессы
PO 2	Утвержденные классификации данных	Отчеты об эффективности процессов	ME 1
PO 9	Оценки рисков		
AI 3	Требования по физическим условиям		

Таблица ОУКИ

Действия ↓ / Функции →	Директор	Финансовый директор	Вице-президент (руководство)	Директор по ИТ	Владелец бизнес-процесса	Руководитель эксплуатации систем	Главный архитектор ИТ систем	Руководитель разработки	Руководитель администрации ИТ	Руководитель департамента офиса	Аудит, риски, комплаенс
Определить требуемый уровень физической защиты					К	У/О	К				К
Выбрать и утвердить помещение (центра обработки данных, офис и т.д.)	И	К	К	К	К	У/О	К		К	К	К
Внедрить показатели оценки физической среды					И	У/О	И	И			К
Управлять физической средой (включая обслуживание, мониторинг и отчетность)						У/О	К				
Спланировать и внедрить процедуры авторизации и подтверждения физического доступа				К	И	У/О	И	И	И		К

В таблице ОУКИ показано, кто является Ответственным, Утверждающим, Консультирующим и/или Информированным

Цели и показатели



Модель зрелости

Управление процессом *«Управление физической безопасностью и защитой от воздействия окружающей среды»* удовлетворяет следующим бизнес требованиям к ИТ *защита компьютерных активов и корпоративных данных и минимизация риска сбоев в работе организации* и соответствует характеристикам:

0. Несуществующий

Нет понимания необходимости обеспечения защиты объектов или капитала, вложенного в электронно-вычислительные ресурсы. Не отслеживаются и не контролируются факторы окружающей среды, включая противопожарную защиту, запыленность, энергоснабжение, а также температурный режим и влажность.

1. Начальный/Повторяющийся эпизодически и бессистемно

В организации осознано требование бизнеса обеспечить пригодное физическое окружение, защищающее оборудование и людей от антропогенных и природных опасностей. Не существует никаких стандартных процедур. Управление объектами и оборудованием зависит от квалификации и способностей отдельных ведущих сотрудников. Сотрудники могут передвигаться по объектам без каких бы то ни было ограничений. Руководство не следит ни за факторами окружающей среды на объектах, ни за перемещением персонала.

2. ***Повторяющийся, но интуитивный***

Внедрены средства контроля факторов окружающей среды, за их работой следит операционный персонал. Процесс обеспечения физической безопасности осуществляется неформально, по инициативе небольшой группы сотрудников, проявляющих высокий уровень озабоченности вопросами обеспечения физической безопасности объектов. Процедуры технического обслуживания объектов плохо оформлены документально и основываются на опыте нескольких отдельных сотрудников. Задачи обеспечения физической безопасности не базируются на официально оформленных стандартах, и руководство не уверено в достижении целей обеспечения безопасности.

3. ***Определенный***

В организации осознана и принята необходимость обеспечения контроля среды, где располагается компьютерное оборудование. Контроль факторов окружающей среды, профилактическое обслуживание и обеспечение физической безопасности являются бюджетными статьями, утвержденными и отслеживаемыми руководством. Применяются меры ограничения доступа к вычислительным ресурсам, который предоставляется только сотрудникам, имеющим специальное разрешение. Как правило, ведется регистрация посетителей в журнале и их сопровождение на объектах. Помещения, где располагается оборудование, не носят указаний на свое предназначение. Гражданские власти следят за соблюдением правил техники безопасности и охраны труда. Риски застрахованы, проводятся незначительные усилия по оптимизации затрат на страхование.

4. ***Управляемый и измеряемый***

Полностью осознана необходимость обеспечения контроля вычислительной среды, что отражено в организационной структуре и распределении бюджетных средств. Документально оформлены требования по обеспечению экологической и физической безопасности. Осуществляется строгий контроль и мониторинг доступа к объектам. Установлены и доведены до сведения сотрудников ответственности и обязанности в части обеспечения физической безопасности. Персонал, работающий на объектах, прошел полную подготовку по действиям в чрезвычайных ситуациях, а также обучение практическим методам техники безопасности и охраны труда. Имеются стандартизованные механизмы контроля над ограничением доступа к объектам, которые имеют дело с факторами окружающей среды и с факторами безопасности. Руководство следит за эффективностью применяемых средств контроля и их соответствием установленным стандартам. Руководство приняло цели и показатели для оценки эффективности управления вычислительной средой. Способность к восстановлению вычислительных ресурсов включена в бизнес процесс управления рисками. Интегрированная информация используется для оптимизации страхового покрытия и связанных с ним затрат.

5. ***Оптимизированный***

Имеется согласованный, долгосрочный план по объектам, необходимый для поддержки вычислительной среды организации. Для всех объектов определены стандарты, охватывающие вопросы выбора объектов, строительства, охраны, обеспечения безопасности персонала, механических и электрических систем, а также защиты от рисков со стороны окружающей среды (пожар, молния и затопление). Все объекты инвентаризованы и классифицированы в соответствии с осуществляемым в организации процессом управления рисками. Осуществляется строгий контроль доступа к объектам, который предоставляется только лицам, имеющим соответствующую производственную необходимость. Осуществляется постоянный мониторинг доступа. Посетители допускаются на объект только с сопровождающими лицами. Ведется мониторинг и контроль факторов окружающей среды с использованием специализированного оборудования. Объекты организуются по «безлюдному» принципу, то есть, в помещениях, где размещается оборудование, отсутствуют рабочие места персонала. Достижение целей подлежит постоянной оценке. Программы предупредительного технического обслуживания обеспечивают строгое соблюдение графиков и проведение регулярных проверок наиболее значимого оборудования. Стратегия и стандарты работы с объектами соответствуют целям обеспечения доступности ИТ услуг, взаимосвязаны с планированием непрерывности деятельности организации и управлением кризисными ситуациями. Руководство постоянно осуществляет анализ и оптимизацию объектов, стремясь использовать любую возможность для привнесения пользы бизнесу.

DS 13. Управление операциями по эксплуатации систем

Описание процесса

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.

Управление процессом

Управление операциями по эксплуатации систем.

удовлетворяет следующим бизнес требованиям к ИТ

поддержка целостности данных, обеспечение устойчивости инфраструктуры ИТ и её способности к восстановлению от ошибок и сбоев. **сосредоточено на**

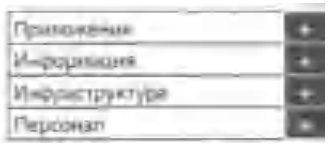
соответствии операционным уровням обслуживания для плановой обработки данных, защиты вывода важной информации, мониторинга и обслуживания инфраструктуры.

достигается с помощью

- Эксплуатации ИТ среды в соответствии с принятыми уровнями обслуживания и определенными инструкциями.
- Обслуживания ИТ инфраструктуры.

результаты оцениваются с помощью следующих показателей

- Число уровней обслуживания, затрагиваемых при операционных инцидентах.
- Часы незапланированных простоев, вызванных операционными инцидентами.
- Доля оборудования, включенного в программы превентивного обслуживания.



Цели контроля

DS 13.1. Операционные процедуры и инструкции

Определить, реализовать на практике и поддерживать процедуры для ИТ операций, убедиться в том, что операционный персонал ознакомлен со всеми необходимыми операционными задачами. Операционные процедуры должны учитывать сменную работу (передачу выполняемых действий, обновления статуса, операционные проблемы, процедуры эскалации и отчетность по текущим обязанностям) для поддержки соответствия согласованным уровням обслуживания и обеспечения непрерывности операций.

DS 13.2. Определение графикаработ

Организовать составление графика работ, процессов и задач в наиболее эффективной последовательности, увеличивая результативность и использование в соответствии с бизнес требованиями.

DS 13.3. Мониторинг ИТ инфраструктуры

Определить и реализовать на практике процедуры мониторинга ИТ инфраструктуры и относящихся к ней событий. Следует убедиться в том, что достаточная хронологическая информация хранится в составе протоколов операций, для обеспечения возможности восстановления, изучения и проверки временных последовательностей операций и другой деятельности, связанной с поддержкой операций.

DS 13.4. Важные документы иустройства вывода данных

Создать адекватную физическую защиту, практику учета и инвентаризации наиболее важных ИТ активов, таких как специальные формы, платежные документы, принтеры для специальных задач или жетоны идентификации.

DS 13.5. Превентивное обслуживание оборудования

Определить и реализовать на практике процедуры, обеспечивающие оперативную поддержку инфраструктуры для сокращения частоты и масштабов сбоев или падения производительности.

Рекомендации по управлению

Из	Входящая информация
AI 4	Пользовательские, эксплуатационные, обслуживающие, технические и руководства для администраторов
AI 7	Ввод в среду промышленной эксплуатации, планы выпуска версий программ и планы распространения
DS 1	Соглашения об уровне обслуживания и соглашения операционного уровня
DS 4	Планы резервного хранения и защиты
DS 9	ИТ конфигурация/подробности по активам
DS 11	Инструкции операторов управления данными

Результаты	В процессы
Карточки инцидентов	DS 8
Протоколы ошибок	DS 10
Отчеты об эффективности процессов	ME 1

Таблица ОУКИ

Действия ↓ Функции →	Президент	Финансовый директор	Высшее руководство	Директор по ИТ	Владелец бизнес-процесса	Руководитель эксплуатации систем	Главный архитектор ИТ-систем	Руководитель разработок	Руководитель администрирования ИТ	Руководитель проектного офиса	Аудит, риски, безопасность
Создать/изменить операционные процедуры (включая руководства, проверочные листы, планирование отклонений, передаваемую документацию, процедуры развития и т.д.)						У/О					И
Разработать график рабочей нагрузки и системные задания на пакетную обработку					К	У/О	К	К			
Осуществлять мониторинг инфраструктуры и обработки, разрешение проблем						У/О					И
Управлять и обеспечивать безопасность физического вывода (например, на бумагу или иной носитель)						У/О					И
Вносить исправления в графики и инфраструктуру					К	У/О	К	К			К
Внедрять проекты защиты устройств от стороннего вмешательства, потери или кражи				У		О			И		К
Создать график и реализовать превентивное обслуживание						У/О					

В таблице ОУКИ показано, кто является Ответственным, Утверждающим, Консультирующим и/или Информированным

Цели и показатели

Модель зрелости

Управление процессом *«Управление операциями по эксплуатации систем»* удовлетворяет следующим бизнес требованиям к ИТ *поддержка целостности данных, обеспечение устойчивости инфраструктуры ИТ и её способности к восстановлению от ошибок и сбоев* и соответствует характеристикам:

0. Несуществующий

Организация не выделяет время и ресурсы для организации поддержки основных информационных технологий и выполнения операций.

1. Начальный/Повторяющийся эпизодически и бессистемно

Организация осознает необходимость структуризации функций поддержки ИТ. Приняты некоторые стандартные процедуры, но операции выполняются, по сути дела, как реакция на происшедшие события. Для большинства операций нет формально утвержденного графика. Заявки на обработку данных принимаются без предварительного подтверждения их правильности. У компьютеров, систем и приложений, поддерживающих бизнес процессы, часто имеют место сбои, задержки и неготовность к работе. Сотрудники теряют время в ожидании ресурсов. Носители выводимых данных часто оказываются в неожиданных местах или вовсе отсутствуют.

2. Повторяющийся, но интуитивный

Организация осознает ключевую роль, которую ИТ операции играют в обеспечении функций поддержки ИТ. Лишь от случая к случаю имеет место выделение бюджета на инструментальные средства. Операции поддержки ИТ выполняются на неформальном и интуитивном уровне. Многое зависит от квалификации и способностей отдельных сотрудников. Инструкции о том, что нужно делать, когда и в каком порядке, не оформлены

документально. Существует определенное обучение операторов и ряд формализованных операционных стандартов.

3. Определенный

В организации понята и принята необходимость управления компьютерными операциями. Выделяются ресурсы, в некоторых случаях проводится обучение без отрыва от работы. Повторяющиеся функции формально определены, стандартизованы, документально оформлены и доведены до сведения. Осуществляется регистрация событий и результатов выполнения задач, однако, отчетность перед руководством ограничена. Имеют место применение автоматизированных средств для управления графиком пакетных заданий и другие инструменты в целях ограничения возможности вмешательства со стороны операторов. Внедряется контроль за внедрением новых видов работ. Разработана формализованная политика по сокращению незапланированных событий. Соглашения с поставщиками о техническом обслуживании и предоставлении услуг все еще носят неформальный характер.

4. Управляемый и измеряемый

Четко определены обязанности по выполнению компьютерных операций и их поддержки. Назначены владельцы процессов. Операции поддерживаются бюджетными средствами, выделяемыми на соответствующие капиталовложения, и людскими ресурсами. Обучение проводится формально и систематически и является фактором продвижения сотрудников по службе. Графики и

задачи документально оформлены и доведены до сведения как службы ИТ, так и до корпоративных подразделений. Существует возможность измерения и отслеживания ежедневно выполняемой работы по типовым договорам на выполнение работ, а также установленных уровней предоставления услуг. Быстро принимаются меры по устранению любых отклонений от установленных норм. Руководство следит за использованием компьютерных ресурсов и выполнением работ или поставленных задач. Непрерывно прилагаются усилия по повышению уровня автоматизации процессов, которые считаются средством обеспечения непрерывного совершенствования. С поставщиками заключаются формальные договора о техническом обслуживании и предоставлении услуг. Налажено полное соответствие с процессами управления проблемами, мощностями и обеспечением готовности систем к работе, которое поддерживается анализом причин ошибок и сбоев.

5. Оптимизированный

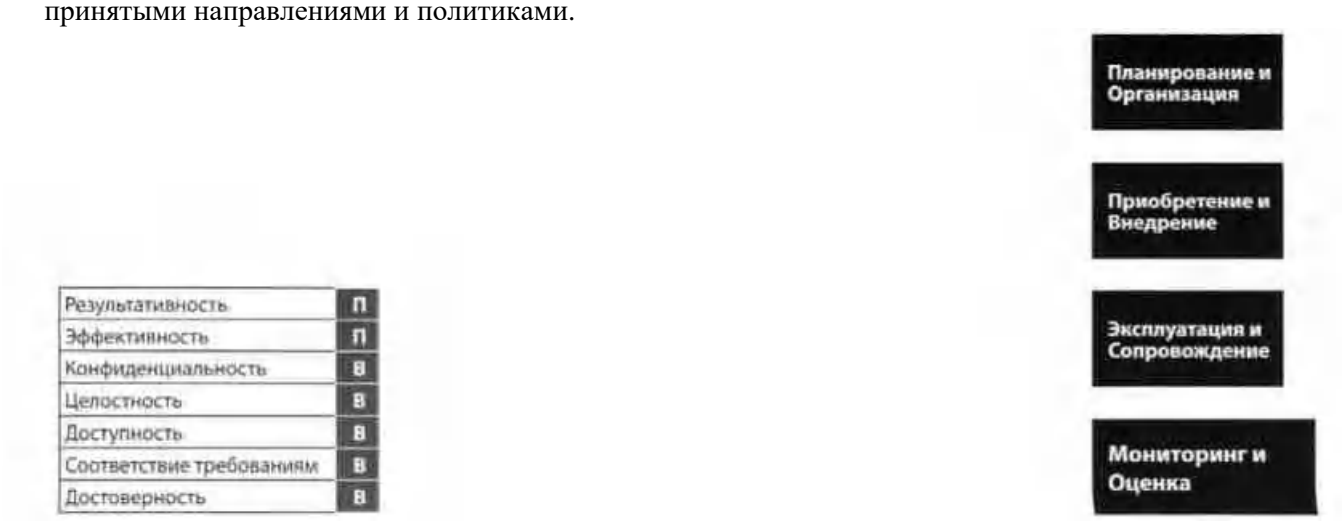
Операции по поддержке ИТ выполняются эффективно, результативно и с достаточной гибкостью, что позволяет быстро и с минимальными потерями в производительности реагировать на требования, соответствующие уровню обслуживания. Процессы управления операциями по поддержке ИТ стандартизованы и документально оформлены в базе знаний. Ведется постоянное совершенствование этих процессов. Автоматизированные процессы и системы поддержки работают незаметно для пользователей и вносят свой вклад в создание стабильной среды. Все проблемы и сбои анализируются с определением первопричин. Регулярно проводимые совещания с сотрудниками, ответственными за управление изменениями, позволяют своевременно учитывать введенные изменения в графиках работы. При сотрудничестве с поставщиками проводится анализ возраста оборудования и признаков, указывающих на его неправильную работу. Проводимое техническое обслуживание носит, в основном, профилактический характер.

Мониторинг и оценка

ме1. мОНИТОРИНГ И оценка эффективности ИТ

Описание процесса

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 делается правильно, в соответствии с принятыми направлениями и политиками.



Управление процессом

Мониторинг и оценка эффективности **ИТ.**

удовлетворяет следующим бизнес требованиям к ИТ

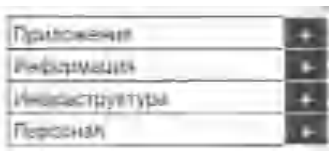
прозрачность и понимание затрат на **ИТ,** преимуществ, стратегии, политик и уровней услуг в соответствии с требованиями корпоративного управления. **сосредоточено на** мониторинге и отчетности по показателям процессов, а также на выявлении и реализации действий по повышению эффективности. **достигается с помощью**

- Составления и преобразования отчетов об эффективности процессов в управленческую отчетность.
- Анализа эффективности согласно поставленным целям и инициировании корректирующих действий.

результаты оцениваются с помощью следующих показателей

- Удовлетворенность руководства отчетностью об эффективности.
- Число действий по совершенствованию по результатам мониторинга.
    - Доля критических процессов, охваченных мониторингом.

Приоритетное Второстепенное



Цели контроля

ME 1.1. Подход к организации мониторинга

Разработать общую методологию мониторинга и подход к определению масштаба, методологии и процесса оценки ИТ решений и оказания услуг, а также мониторинга вклада ИТ в бизнес. Интегрировать эту методологию в корпоративную систему оценки эффективности.

ME 1.2. Определение и сбор данных мониторинга

Совместно с бизнес подразделениями разработать сбалансированную систему целей эффективности, утвердить ее на корпоративном уровне и обеспечить поддержку всех заинтересованных сторон. Определить виды сравнительного анализа для сопоставления целей и выявить данные, приемлемые для сбора в качестве показателей оценки достижения данных целей. Разработать процессы своевременного сбора достоверных данных для отчетности по достижению целей.

ME 1.3. Методика мониторинга

Внедрить методику мониторинга эффективности (например, сбалансированную систему показателей) для учета целей и показателей, получения емкой, всесторонней характеристики ИТ эффективности и обеспечения совместимости с корпоративной системой мониторинга.

ME 1.4. Оценка эффективности

Периодически проводить проверку текущей эффективности в сравнении с поставленными целями, анализировать случаи отклонения, предпринимать корректирующие действия в отношении выявленных причин. В необходимое время проводить анализ первопричин в отношении отклонений.

ME 1.5. Отчетность перед высшимруководством и Советом директоров

Разработать отчетность перед высшим руководством по вкладу ИТ в развитие бизнеса, с учетом характеристики эффективности связанных с ИТ инвестиционных программ в корпоративном портфеле, а также в части эффективности автоматизированных решений и предоставляемых ИТ сервисов в разрезе инвестиционных программ. Обозначить в отчетности тот уровень, до которого продвинулось достижение запланированных целей, объем использованных бюджетных ресурсов, перечень достигнутых целей по эффективности и минимизацию выявленных рисков. Предварять отчетность перед высшим руководством предложением корректирующих действий в отношении наиболее существенных отклонений. Предоставить отчетность высшему руководству и запрашивать замечания по итогам анализа со стороны руководства.

ME 1.6. Корректирующие действия

Определить и реализовать на практике корректирующие действия, основанные на данных мониторинга эффективности, оценках и отчетности. Эти действия включают в себя следование рекомендациям по результатам мониторинга, отчетности и оценкам посредством:

- Анализа, обсуждения и принятия ответных действий со стороны руководства.
- Назначения ответственных лиц за выполнение корректирующих действий.
- Отслеживания результатов выполненных корректирующих действий.

Рекомендации по управлению

Из	Входящая информация
PO 5	Отчеты о затратах и выгодах
PO 10	Отчеты об эффективности проектов
AI 6	Отчеты о статусе изменений
DS 1–DS 13	Отчеты об эффективности процессов
DS 3	Требования плана по производительности и мощностям
DS 8	Отчеты об удовлетворенности пользователей
ME 2	Отчет об эффективности мер ИТ контроля
ME 3	Отчет о соответствии ИТ деятельности внешним требованиям законодательства и регулирующих норм
ME 4	Отчет о статусе корпоративного ИТ управления

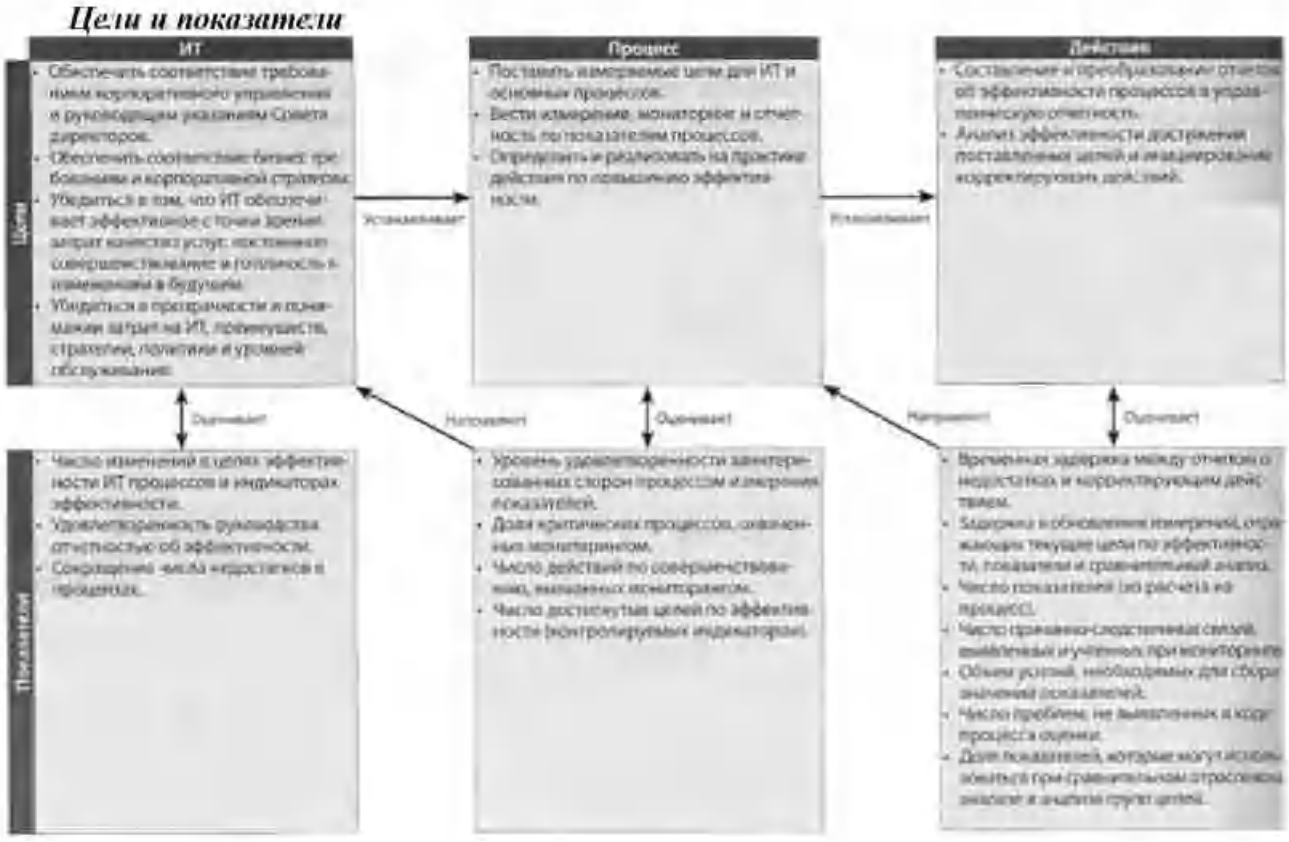
Результаты	В процессы						
Требования по эффективности в ИТ планировании	PO 1	PO 2	DS 1				
Планы корректирующих действий	PO 4	PO 8					
Ретроспективный анализ рисков и инцидентов	PO 9						
Отчет об эффективности процессов	ME 2						

Таблица ОУКИ

Действия ↓ Функции →	Совет директоров	Президент	Финансовый директор	Бизнес-руководство	Директор по ИТ	Владелец бизнес-процесса	Руководитель эксплуатации систем	Главный архитектор ИТ-систем	Руководитель разработок	Руководитель администрации ИТ	Аудит, риски, безопасность
Разработать подход к организации мониторинга		У	О	К	О	И	К	И	К	И	К
Определить и собрать измеримые цели и поддерживать бизнес-цели		К	К	К	У	О	О		О		
Создать систему сравнительных показателей					У		О	К	О	К	
Провести оценку эффективности деятельности ИТ			И	И	У	О	О	К	О	К	
Вести отчетность по эффективности деятельности ИТ	И	И	И	О	У	О	О	И	О	К	И

В таблице ОУКИ показано, кто является Ответственным, Утверждающим, Консультирующим и/или Информированным

Цели и показатели



Модель зрелости

Управление процессом *«Мониторинг и оценка эффективности ИТ»* удовлетворяет следующим бизнес требованиям к ИТ *прозрачность и понимание затрат на ИТ, преимуществ, стратегии, политик и уровней услуг в соответствии с требованиями корпоративногоуправления* и соответствует характеристикам:

0. Несуществующий

В организации отсутствует процесс мониторинга эффективности деятельности. Служба ИТ не проводит независимый контроль хода проектов или процессов. Не подготавливаются содержательные, актуальные и точные отчеты. Не осознана потребность в ясном понимании целей процесса.

1. Начальный/Повторяющийся эпизодически и бессистемно

Руководство осознает необходимость процесса мониторинга. Стандартные процессы сбора и оценки информации еще не установлены. Мониторинг и система показателей используются от случая к случаю, применительно к нуждам конкретных ИТ проектов или процессов. Мониторинг внедряется, в основном, как реакция на инцидент, который привел к потерям или создал проблему для организации. Бухгалтерская служба отслеживает основные финансовые показатели, относящиеся к ИТ.

2. Повторяющийся, но интуитивный

Определены основные показатели, подлежащие мониторингу. Существуют методы и способы сбора и оценки информации, однако, они не внедрены в целом по всей организации. Интерпретация результатов мониторинга основана на личном опыте ключевых сотрудников. Выбраны и применяются отдельные, ограниченные по своим возможностям, инструментальные средства для сбора информации, однако эта работа ведется без планового подхода.

3. Определенный

Руководством утверждены документально оформленные стандартные процессы мониторинга, которые доведены до сведения сотрудников. Реализуются программы обучения и подготовки персонала по вопросам проведения мониторинга. Создана формализованная база знаний по показателям работы за прошедшие периоды. Оценка все еще выполняется на уровне отдельных ИТ процессов и проектов и не интегрирована со всеми процессами. Определены инструментальные средства для проведения мониторинга ИТ процессов и уровней обслуживания. Установлены показатели для определения вклада службы ИТ в общую работу организации с использованием традиционных финансовых и операционных критериев. Определены показатели эффективности, характерные для ИТ, а также нефинансовые, стратегические и показатели удовлетворенности пользователей и уровни обслуживания. Определена методология оценки эффективности.

4. Управляемый и измеряемый

Руководством определены допустимые отклонения для всех процессов. Установлены стандарты и нормы для отчетности по результатам мониторинга. Существует единая система показателей для всех ИТ проектов и процессов. Формализованы системы управленческой отчетности службы ИТ. Автоматизированные инструментальные средства интегрированы и используются в масштабах всей организации для сбора и мониторинга информации по приложениям, системам и процессам. Руководство может оценивать эффективность ИТ, основываясь на критериях, утвержденных заинтересованными сторонами. Показатели работы службы ИТ согласованы с общекорпоративными целями.

5. Оптимизированный

Разработан процесс непрерывного повышения качества для обновления методик и стандартов мониторинга в масштабе всей организации с учетом лучших отраслевых практик. Все процессы мониторинга оптимизированы и поддерживают цели всей организации. Соответствующие целям бизнеса показатели постоянно используются для оценки эффективности и взаимосвязаны с системой стратегических оценок, например, с системой сбалансированных показателей. Мониторинг процессов и их пересмотр согласуются с планами совершенствования бизнес процессов в масштабах всей организации. Формализован сравнительный анализ показателей организации с показателями отрасли и основных конкурентов на основе четких критериев.

ME 2. Мониторинг и оценка системы внутреннего контроля

Описание процесса

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.

Управление процессом

Мониторинг и оценка системы внутреннего контроля.

удовлетворяет следующим бизнес требованиям к ИТ

подтверждение достигнутых целей ИТ и соответствие ИТ законодательству, регулирующим нормам и контрактам. **сосредоточено на**

мониторинге процессов внутреннего контроля видов ИТ деятельности и выявлении действий по совершенствованию. **достигается с помощью**

- Определения системы внутреннего контроля, включенной в методологию ИТ процессов.
- Мониторинга и отчетности об эффективности внутреннего контроля в сфере ИТ.
- Отчетности об исключительных случаях и принятии корректирующих мер.

результаты оцениваются с помощью следующих показателей

- Число крупных нарушений в сфере внутреннего контроля.
- Число инициатив по совершенствованию мер контроля.
- Число и охват самооценок системы контроля.

Цели контроля

ME 2.1. Мониторинг методологии внутреннего контроля

Постоянно осуществлять мониторинг, сравнительный анализ и совершенствование среды ИТ контроля и соответствующей методологии согласно корпоративным целям. ***ME 2.2. Надзор***

Осуществлять мониторинг и оценку эффективности и результативности внутреннего управленческого контроля ИТ.

ME 2.3. Исключения из мер контроля

Выявить случаи исключения из требований контроля, проанализировать их и выявить их первопричины. По этим исключениям подготовить отчетность для заинтересованных сторон. Выработать необходимые корректирующие действия.

ME 2.4. Контрольные самооценки

Провести оценку полноты и эффективности управленческого контроля над ИТ процессами, политики и контрактов в рамках постоянной программы самооценки. ***ME 2.5. Аудит системы внутреннего контроля***

Получить, в случае необходимости, гарантии полноты и эффективности системы внутреннего контроля, с помощью проверок третьей стороны. ***ME 2.6. Система внутреннего контроля третьих сторон***

Оценить уровень системы внутреннего контроля у внешних поставщиков услуг. Следует убедиться в том, что внешние поставщики услуг соответствуют требованиям законодательства и регулирующих норм, а также контрактных обязательств.

ME2.7. Корректирующие действия

Определить, инициировать, отслеживать и реализовать на практике корректирующие действия, вытекающие из оценок системы контроля и отчетности.

Рекомендации по управлению

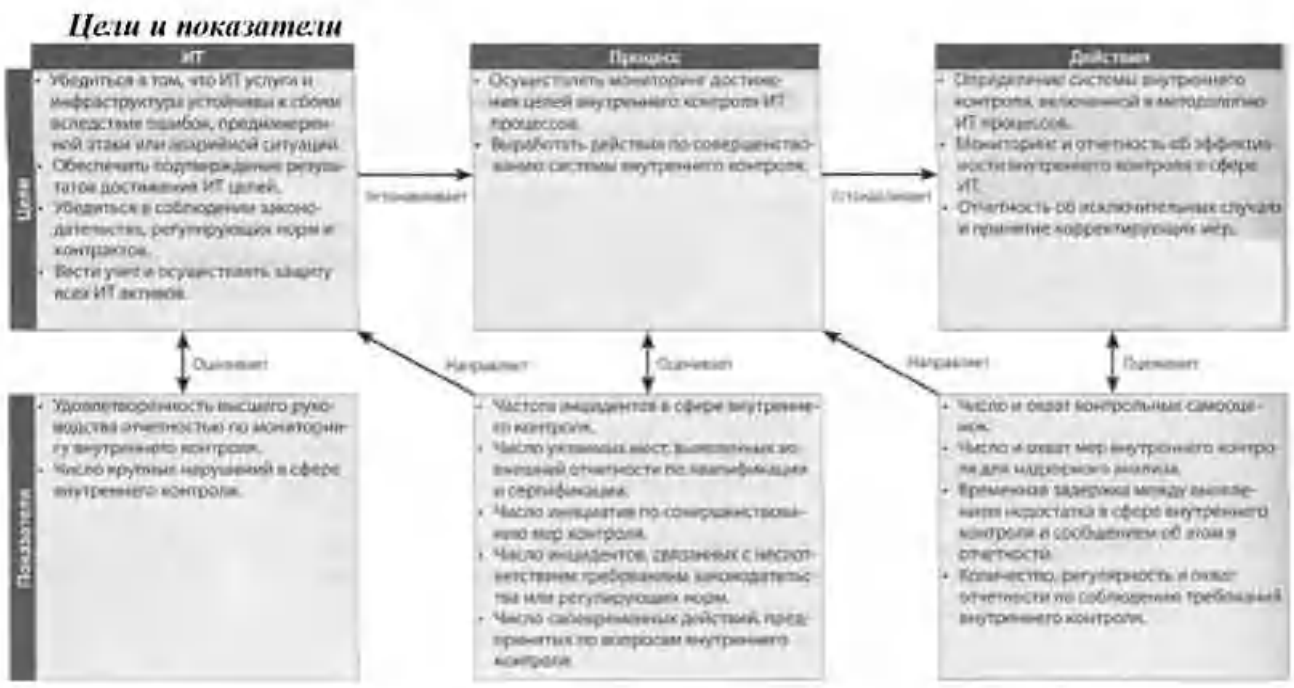
Из	Входящая информация
AI 7	Мониторинг внутреннего контроля
ME 1	Отчеты об эффективности процессов

Результаты	В процессы						
Отчет об эффективности мер контроля ИТ	PO 4	PO 6	ME 1	ME 4			

Таблица ОУКИ

Действия / Функции	Совет директоров	Президент	Генеральный директор	Высшее руководство	Директор по ИТ	Владелец бизнес процесса	Руководитель архитектуры системы	Главный архитектор ИТ системы	Руководитель разработки	Руководитель администрирования ИТ	Аудит, риски, безопасность
Осуществлять мониторинг и надзор за системой внутреннего ИТ контроля					У		О		О	О	О
Осуществлять мониторинг процесса самооценки				И	У		О		О	О	К
Осуществлять мониторинг эффективности на независимой отчетности, аудита и проверок				И	У		О		О	О	К
Осуществлять мониторинг процесса получения сертификата в отношении системы контроля третьих сторон		И	И	И	У		О		О	О	К
Осуществлять мониторинг процесса определения и оценки исключений из контроля		И	И	И	У	И	О		О	О	К
Осуществлять мониторинг процесса определения и коррекции исключений из контроля		И	И	И	У	И	О		О	О	К
Вести отчетность перед основными заинтересованными сторонами	И	И	И		У/О						К

В таблице ОУКИ показано, кто является Ответственным, Утверждающим, Консультирующим и/или Информированным



Модель зрелости

Управление процессом *«Мониторинг и оценка системы внутреннего контроля»* удовлетворяет следующим бизнес требованиям к ИТ *подтверждение достигнутых целей ИТ и соответствие ИТ законодательству, регулирующим нормам и контрактам* и соответствует характеристикам:

0. Несуществующий

В организации отсутствуют процедуры отслеживания действенности мер внутреннего контроля. Отсутствуют методы информирования руководства по вопросам внутреннего контроля. Имеет место общая неосведомленность по мерам контроля ИТ безопасности и внутреннего контроля. Как руководители, так и сотрудники проявляют общую неосведомленность в вопросах внутреннего контроля.

1. Начальный/Повторяющийся эпизодически и бессистемно

Руководство осознает необходимость в регулярных проверках в области управления средой контроля ИТ. Опыт отдельных сотрудников по оценке адекватности мер внутреннего контроля применяется от случая к случаю. Руководители службы ИТ официально не назначили лиц, ответственных за осуществление мониторинга эффективности системы внутреннего контроля. Оценка системы внутреннего контроля ИТ является частью обычного финансового аудита, при этом используемые технологии и квалификация персонала не отражают потребностей службы ИТ.

2. Повторяющийся, но интуитивный

Организация использует неформальную отчетность по вопросам контроля для инициирования корректирующих мер. Оценка внутреннего контроля зависит от уровня квалификации ведущих сотрудников. Организация повысила уровень своего понимания важности мониторинга внутреннего контроля. Руководство службы ИТ выполняет регулярный мониторинг эффективности того, что им понимается как наиболее важные меры внутреннего контроля. Начинается применение, хотя и бессистемное, методологий и инструментов мониторинга системы внутреннего контроля. На основе опыта ведущих сотрудников выявляются факторы риска, характерные для ИТ среды.

3. Определенный

Руководство поддерживает и официально внедряет в практику организации мониторинг системы внутреннего контроля. Разработаны политика и процедуры оценки и отчетности по результатам мониторинга адекватности системы внутреннего контроля. Создана программа обучения мониторингу внутреннего контроля. Предусмотрены процедуры самооценки и

независимого анализа состояния внутреннего контроля, которые определяют обязанности бизнес и ИТ менеджеров. Используются инструментальные средства, которые, однако, не всегда интегрированы во всех процессах. Методики оценки рисков ИТ процессов, используемые в рамках системы контроля, разработаны специально для службы ИТ. Определены риски, характерные для конкретных процессов и политика их минимизации.

4. Управляемый и измеряемый

Руководство внедряет методологию мониторинга внутреннего контроля. В организации принимаются допустимые отклонения для процесса мониторинга внутреннего контроля. Для стандартизации оценок и автоматического выявления исключительных случаев внедрены инструментальные средства. Официально создано подразделение внутреннего контроля информационных технологий, обеспечиваемое работой сертифицированных профессионалов, которые применяют методологию, утвержденную высшим руководством. Опытные сотрудники персонала ИТ постоянно участвуют в процессе оценки внутреннего контроля. Создана база знаний, включающая в себя архив полученных в прошлом показателей внутреннего контроля. Введен обмен опытом по вопросам мониторинга внутреннего контроля.

5. Оптимизированный

Руководство вводит программу постоянного совершенствования в масштабах всей организации с использованием как собственных, так и отраслевых лучших практик для мониторинга внутреннего контроля. Организация использует современные интегрированные инструментальные средства, которые позволяют эффективно оценивать важнейшие меры ИТ контроля и быстро выявлять инциденты при мониторинге. Официально организован процесс обмена опытом. Формализован сравнительный анализ отраслевых стандартов и лучших практик.

ME 3. Обеспечение соответствия внешним требованиям

Описание процесса

Эффективный надзор за соответствием внешним требованиям требует установления процесса анализе 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.

Результативность	
Эффективность	
Конфиденциальность	
Целостность	
Доступность	
Соответствие требованиям	П
Достоверность	В

Управление процессом

Обеспечение соответствия внешним требованиям.

удовлетворяет следующим бизнес требованиям к ИТ

обеспечение соблюдения законодательства, регулирующих норм и условий контрактов. **сосредоточено на**

выявлении всех применимых требований законодательных актов, регулирующих норм и условий контрактов, а также необходимого уровня ИТ соответствия и оптимизации ИТ процессов на сокращение риска несоответствия. **достигается с помощью**

- Выявления требований законодательства, регулирующих норм и условий контрактов, имеющих отношение к ИТ.
- Оценки последствий требований по соответствию внешним требованиям.
- Мониторинга и отчетности по соответствию данным требованиям. **результаты оцениваются с помощью следующих показателей**
- Затраты, связанные с несоответствиями, включая выплаты и штрафы.
- Средняя временная задержка между выявлением проблем с соответствием внешним требованиям и их решением.
- Частота анализа соответствия внешним требованиям.

Приоритетное Второстепенное

Приложения	
Информация	
Инфраструктура	
Персонал	

Цели контроля

ME 3.1. Выявление внешних требований законодательства, регулирующих норм и условий контрактов

Необходимо вести постоянную работу по выявлению требований национального и международного законодательства, регулирующих норм и других внешних требований, которым должны соответствовать корпоративные ИТ политики, стандарты, процедуры и методики.

ME 3.2. Оптимизация результатов приведения в соответствие с внешними требованиями

Анализировать и корректировать ИТ политики, стандарты, процедуры и методики на предмет соответствия требованиям законодательства, регулирующих норм и условий контрактов.

ME 3.3. Оценка соответствия внешним требованиям

Подтвердить соответствие ИТ политики, стандартов, процедур и методик требованиям законодательства и регулирующих норм.

ME 3.4. Положительное заключение о соответствии

Получить заключение о соответствии и строгом соблюдении положений внутренней политики, вытекающих из внутренних директив и внешних требований законодательства, регулирующих норм и условий контрактов. Заключение должно подтверждать, что все корректирующие действия, направленные на обеспечение соответствия данным требованиям были своевременно предприняты ответственным владельцем процесса.

ME 3.5. Интеграция отчетности

Проводить интеграцию отчетности по соблюдению требований законодательства, регулирующих норм и условий контрактов с аналогичной отчетностью других корпоративных подразделений.

Рекомендации по управлению

Из	Входящая информация
?	Требования законодательства и регулирующих норм
PO 6	ИТ политики

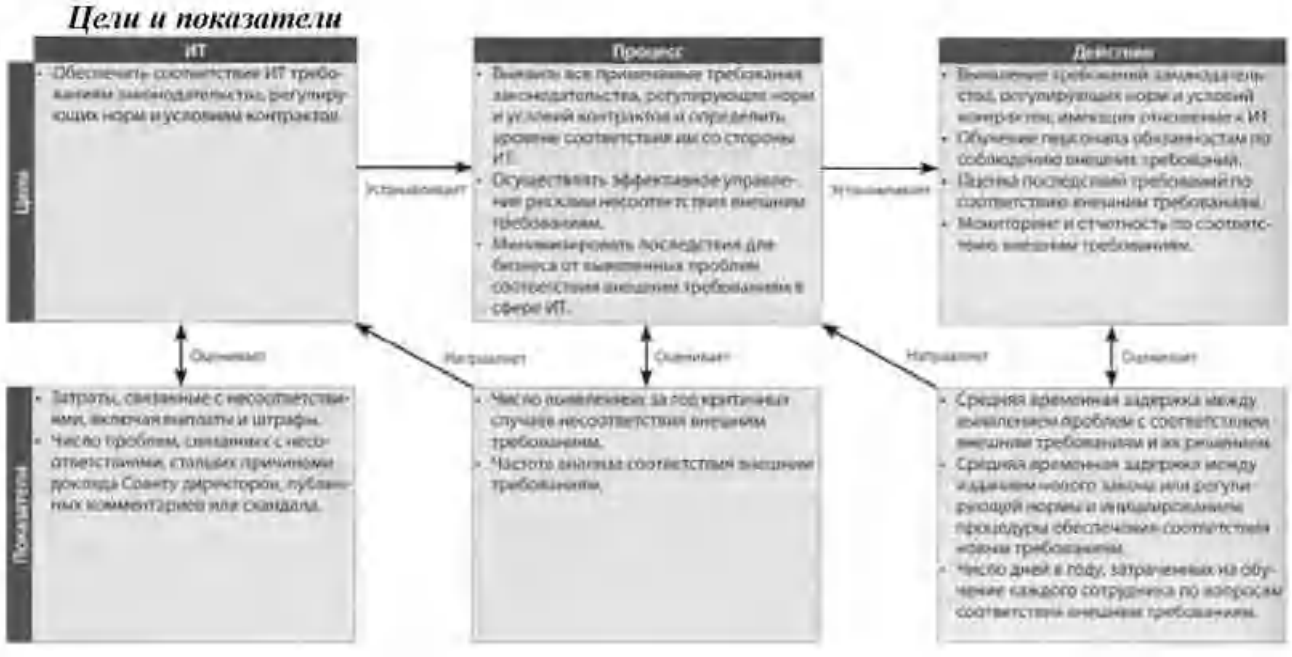
* Источники вне COBIT

Результаты	В процессе						
Каталог требований законодательства и регулирующих норм, имеющих отношение к оказанию ИТ услуг	PO 4	ME 4					
Отчет о соответствии деятельности в сфере ИТ внешним требованиям законодательства и регулирующих норм	ME 1						

Таблица ОУКИ

Действия ↓ / Функции →	Президент	Финансовый директор	Внешние консультанты	Директор по ИТ	Владелец бизнес-процесса	Руководитель эксплуатации системы	Главный архитектор ИТ-систем	Руководитель разработок	Руководитель администрации ИТ	Руководитель проектного офиса	Аудит, риски, безопасность	Совет директоров
Определить и инициировать процесс по выполнению внешних требований законодательства, регулирующих норм и условий контрактов				У/О	К	И	И	И	К	И	О	
Оценить соответствие деятельности в сфере ИТ политикам, планам и процедурам ИТ	И	И	И	У/О	И	О	О	О	О	О	О	И
Получить положительное заключение о соответствии деятельности в сфере ИТ политикам, планам и процедурам ИТ				У/О	К	К	К	К	К	К	О	
Вести мероприятия по приведению ИТ политик, планов и процедур в соответствие с внешними требованиями				У/О	К	И	К	К	К		О	
Осуществить интеграцию ИТ отчетности по соблюдению внешних требований с аналогичной отчетностью других корпоративных подразделений				У/О		И	И	И	О		О	

В таблице ОУКИ показано, кто является Ответственным, Утверждающим, Консультирующим и/или Информированным



Модель зрелости

Управление процессом *«Обеспечение соответствия внешним требованиям»* удовлетворяет следующим бизнес требованиям к ИТ *обеспечение соблюдения законодательства, регулирующих норм и условий контрактов* и соответствует характеристикам:

0. Несуществующий

Имеется незначительное осознание того, что внешние требования влияют на ИТ, при этом отсутствует процесс, касающийся соблюдения требований законодательства, регулирующих норм и контрактных обязательств.

1. Начальный/Повторяющийся эпизодически и бессистемно

Осознается необходимость соблюдения требований законодательства, регулирующих норм и контрактных обязательств, влияющих на организацию. Неформальные процессы обеспечения их соблюдения осуществляются только когда возникает необходимость в новых проектах, либо в результате аудиторских проверок или рассмотрений этих вопросов руководством.

2. Повторяющийся, но интуитивный

Есть понимание необходимости соблюдения внешних требований и это доведено до сведения персонала. В тех случаях, где подтверждение соблюдения требований носит регулярный характер, например, в области регулирования финансовой деятельности или конфиденциальности персональных данных, разработаны и ежегодно соблюдаются отдельные процедуры обеспечения соответствия. Тем не менее, отсутствует общий подход. Организация во многом полагается на знания и ответственность сотрудников, вследствие чего возможны ошибки. Осуществляется неформальное обучение вопросам, касающимся внешних требований и вопросам их соблюдения.

3. Определенный

Разработаны, документально оформлены и доведены до сведения персонала политика, процедуры и процессы обеспечения соблюдения требований законодательства, регулирующих норм и контрактных обязательств. Требования, однако, не всегда соблюдаются, и в ряде случаях могут оказаться устаревшими или невыполнимыми. Мало используется мониторинг и есть не исполненные требования. Осуществляется обучение вопросам, касающимся внешних законодательных и нормативных требований, влияющих на организацию, а также определенным процессам обеспечения соответствия. Имеются стандартные типовые договора и юридические процессы для минимизации рисков, связанных с договорными обязательствами.

4. Управляемый и измеряемый

Существует полное понимание вопросов и рисков, связанных с внешними требованиями, и необходимости обеспечения соответствия на всех уровнях. Имеется официально утвержденная система обучения, которая гарантирует информирование всех сотрудников об их обязанностях соблюдать эти требования. Определена ответственность должностных лиц и владельцы процесса. Данный процесс предусматривает анализ среды с целью выявления внешних требований и продолжающихся изменений. Реализован механизм мониторинга несоблюдения внешних требований, внедрения внутренних практик и реализации корректирующих мер. Вопросы несоответствия внешним требованиям анализируются с помощью стандартной процедуры для выявления первопричин с тем, чтобы найти эффективные решения. В конкретных случаях, таких как устоявшиеся регулятивные требования и повторяющиеся договора на обслуживание, используются стандартизованные лучшие отраслевые практики.

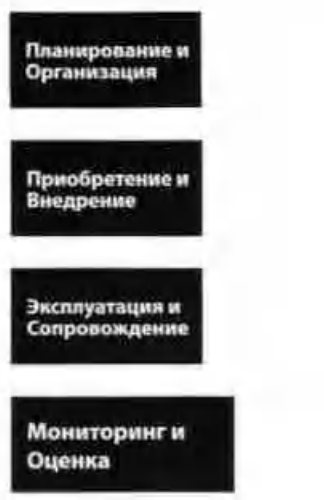
5. Оптимизированный

Имеется хорошо организованный, эффективный и регламентированный процесс обеспечения соответствия внешним требованиям, предусматривающий создание единого централизованного органа, который обеспечивает руководство и координацию в рамках всей организации. Имеется глубокая осведомленность о потенциальных внешних требованиях, включая тенденции их развития и ожидаемые изменения, и существует потребность в новых решениях. Организация принимает участие в работе нормативных и отраслевых ассоциаций и групп с целью понимания и влияния на соответствующие внешние требования, в результате чего несоответствия сведены к минимуму. Существует централизованная система контроля в масштабе организации, позволяющая руководству документально оформлять процедуры рабочего процесса, измерять и повышать качество и эффективность мониторинга соответствия. Реализован процесс внутренней оценки соответствия внешним требованиям, который доведен до уровня лучших практик. Стиль руководства и корпоративная культура в отношении вопросов соответствия являются достаточно требовательными, процессы обучения достаточно хорошо разработаны и применяются только к новым сотрудникам и в случаях, когда происходят значительные перемены.

ME 4. Обеспечение корпоративного управления ИТ

Описание процесса

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.



Результативность	П
Эффективность	П
Конфиденциальность	В
Целостность	В
Доступность	В
Соответствие требованиям	В
Достоверность	В

Управление процессом

Обеспечение корпоративного управления ИТ.

удовлетворяет следующим бизнес требованиям к ИТ

интеграция целей управления ИТ и корпоративного управления, обеспечение соответствия с требованиями законодательства, регулирующих норм и условий контрактов. **сосредоточено на**

подготовке отчетности для Совета директоров по вопросам ИТ стратегии, эффективности и рисков, а также о соответствии требований по управлению указаниям Совета директоров. **достигается с помощью**

- Создания системы управления ИТ, интегрированной с корпоративным управлением.
- Получения независимой оценки статуса управления ИТ. **результаты оцениваются с помощью следующих показателей**
- Регулярность отчетности Совета директоров перед акционерами по вопросам ИТ (включая оценку зрелости).
- Регулярность ИТ отчетности перед Советом директоров (включая оценку зрелости).
- Регулярность независимых оценок по вопросам совместимости ИТ.

Приложения	+
Информация	+
Инфраструктура	+
Персонал	+

Цели контроля

ME 4.1. Создание системы корпоративногоуправления ИТ

Обеспечить соответствие системы управления ИТ общекорпоративному управлению и среде контроля. В основе системы должен быть соответствующий ИТ процесс и модель контроля, а также, должна быть налажена точная отчетность и практика, гарантирующая избежание нарушений в сфере внутреннего контроля и надзора. Подтвердить, что система управления ИТ соответствует требованиям законодательства, регулирующих норм, корпоративной стратегии и целям. Следует вести отчетность о статусе управления ИТ и проблемам в данной сфере.

ME 4.2. Соответствие стратегии

Обеспечить Совет директоров и высшее руководство со своим пониманием стратегических вопросов ИТ, таких как роль ИТ, технологии и возможности. У корпоративного руководства и службы ИТ должно существовать общее понимание потенциального вклада ИТ в достижение целей корпоративной стратегии. Провести работу с Советом директоров и существующими органами

управления, такими как комитет по ИТ стратегии, для выработки стратегического направления руководства ИТ. Данная работа должна привести к созданию последовательному внедрению стратегии и целей в деятельность бизнес подразделений и ИТ службы, а также установлению доверия между ними. Обеспечить соответствие ИТ и бизнеса на уровне стратегии и бизнес операций, поддерживать взаимную ответственность при принятии стратегических решений и извлечении выгод от применения ИТ инструментов.

ME 4.3. Вклад ИТ в бизнес

Следует так управлять связанными с ИТ инвестиционными программами и другими ИТ активами и услугами, чтобы убедится в том, что они дают максимальную отдачу, поддерживая корпоративную стратегию и цели. Необходимо убедиться в четком понимании как ожидаемых результатов от связанных с ИТ инвестиций, так и масштабов усилий, требуемых для их достижения, коме того, в полном и последовательном экономическом обосновании, утвержденном заинтересованными сторонами, управлении активами и инвестициями в течение всего срока их существования, а также в активном управлении получаемыми результатами, такими как новые услуги, лучшая эффективность и восприимчивость к запросам пользователей. Поддерживать ответственный подход к управлению портфелем, программами и проектами, настаивая на том, что бизнес владеет всеми ИТ инвестициями, а служба ИТ обеспечивает оптимизацию затрат на получаемые ИТ услуги и возможности.

ME 4.4. Управление ресурсами

Осуществлять надзор за инвестициями, использованием и распределением ИТ ресурсов посредством регулярных оценок инициатив и операций в сфере ИТ. Обеспечить уверенность в должном выделении ресурсов и их соответствии текущим и будущим бизнес целям и указаниям.

ME 4.5. Управлениерисками

Провести работу с Советом директоров для определения приемлемого уровня ИТ рисков для организации и получить разумные гарантии того, текущие ИТ риски при существующей практике управления ими не превышают установленный Советом директоров уровень. Внедрить обязанности по управлению рисками на уровне организации, чтобы бизнес подразделения и служба ИТ регулярно оценивали и отчитывались об ИТ рисках и их воздействии, а также Обеспечить прозрачность статуса организации в области ИТ рисков и их последствий для всех заинтересованных сторон.

ME 4.6. Управление эффективностью

Подтвердить достижение (или перевыполнение) поставленных ИТ целей, или соответствие процесса достижения ИТ целей ожиданиям. В случаях, когда намеченные цели не были достигнуты или их достижение не соответствует ожиданиям, провести анализ необходимых управленческих корректирующих действий. Необходимо вести отчетность

перед Советом директоров по актуальным портфелям, эффективности программ и ИТ. Эти сведения дополнят отчетность перед высшим руководством по оценке продвижения к намеченным целям.

ME 4.7. Независимая оценка

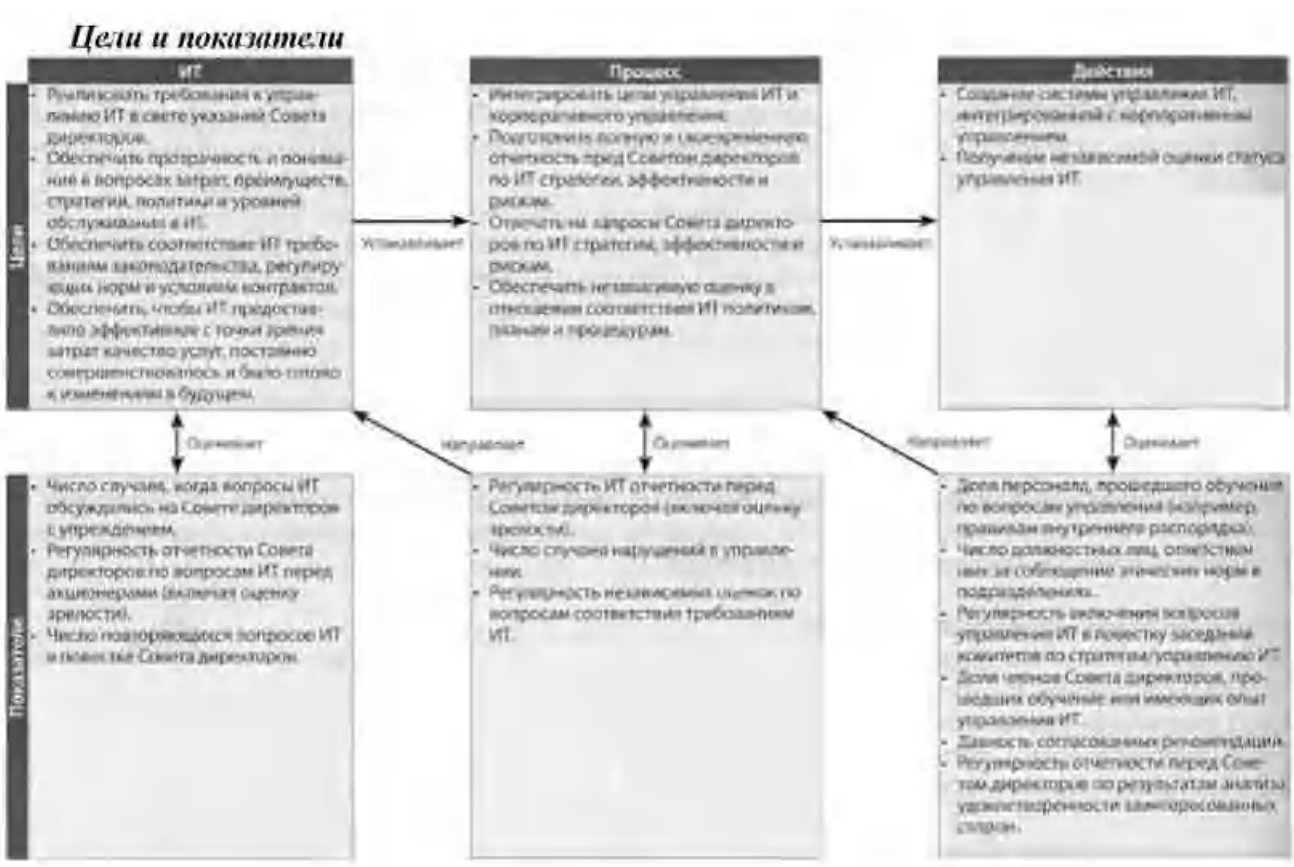
Получить независимую оценку (внутреннюю или внешнюю) соответствия ИТ требованиям законодательства и регулирующих норм, корпоративной политики, стандартов и процедур, общепринятых практик, а также эффективности и результативности ИТ.

Рекомендации по управлению

Таблица ОУКИ

Действия / Функции	Совет директоров	Президент	Финансовый директор	Высшее руководство	Директор по ИТ	Владелец бизнес-процесса	Руководитель эксплуатации систем	Главный архитектор ИТ-систем	Руководитель разработок	Руководитель администрации ИТ	Руководитель проектных работ	Аудит, риски, безопасность
Обеспечить содействие и надзор за деятельностью ИТ со стороны высшего руководства и Совета директоров	У	О	К	К	К							К
Анализировать, утверждать, приводить в соответствие с корпоративной стратегией и информировать об ИТ эффективности, ИТ стратегии, управлении рисками и ресурсами	У	О	И	И	О							К
Регулярно получать независимые оценки эффективности и соответствия политикам, планам и процедурам	У	О	К	И	К		И	И	И	И	И	О
Реализовать на практике рекомендации, полученные в ходе независимых оценок	У	О	К	И	К		И	И	И	И	И	О
Создать отчет по управлению ИТ	У	К	К	К	О	К	И	И	И	И	И	С

В таблице ОУКИ показано, кто является Ответственным, Утверждающим, Консультирующим и/или Информированным



Модель зрелости

Управление процессом *«Обеспечениеуправления ИТ»* удовлетворяет следующим бизнес требованиям к ИТ *интеграция целей управления ИТ и корпоративного управления, обеспечение соответствия с требованиями законодательства, регулирующих норм и условий контрактов* и соответствует характеристикам:

0. Несуществующий

Полное отсутствие какого-либо процесса корпоративного управления ИТ. Организация не осознает существование такой проблемы, данный вопрос не обсуждается.

1. Начальный/Повторяющийся эпизодически и бессистемно

Есть признаки того, что организация признает существование проблем в корпоративном управлении ИТ и необходимость их решения. Возникающие проблемы решаются на индивидуальной основе от случая к случаю. Управление осуществляется в виде реакции на произошедшие события, способы информирования о наличии и подходы к решению проблем случайны и непоследовательны. Руководство имеет самые общие представления о вкладе ИТ в эффективность организации.

Управление осуществляется только как реакция на инциденты, повлекшие за собой определенные убытки либо проблемы для организации.

2. Повторяющийся, но интуитивный

Существует общее понимание проблем корпоративного управления ИТ. Виды деятельности в области корпоративного управления ИТ, которые включают в себя процессы планирования, эксплуатации и контроля, а также система показателей эффективности деятельности находятся в стадии развития. Ведется совершенствование некоторых ИТ процессов по инициативе отдельных сотрудников. Руководство выбрало основные показатели и методы оценки корпоративного управления ИТ, хотя сам процесс не внедрен во всей организации. Ответственность за процессы обучения и информирования персонала о стандартах в области корпоративного управления ИТ возложена на отдельных сотрудников. Указанные сотрудники осуществляют процесс управления ИТ в рамках различных проектов и ИТ процессов. Процессы, инструменты и показатели оценки управления ИТ ограничены и могут используются не в полной мере в силу отсутствия знаний об их функциональных возможностях.

3. Определенный

Важность и необходимость корпоративного управления ИТ осознана и принята руководством и доведена до сведения персонала организации. Разработан базовый набор показателей корпоративного управления ИТ, с определенными и документально зафиксированными взаимосвязями между показателями эффективности. Процедуры стандартизированы, документально оформлены и внедрены. Определены инструментальные средства, применяемые при надзоре за управлением ИТ. В качестве компонента системы сбалансированных показателей образованы инструментальные панели. Тем не менее, ответственность за обучение, соблюдение и применение стандартов возложена на сотрудников. Процессов могут подвергаться мониторингу, однако отклонения от стандартов часто остаются незамеченными руководством, поскольку многие действия выполняются по личной инициативе.

4. Управляемый и измеряемый

Существует полное понимание проблем корпоративного управления ИТ на всех уровнях. Есть четкое представление о том, кто является потребителем ИТ услуг, обязанности определены и их исполнение контролируется, исходя из соглашений об уровне обслуживания. Установлены владельцы процессов и определены их обязанности. ИТ процессы увязаны с бизнесом и ИТ стратегией. Совершенствование ИТ процессов базируется на количественном анализе, что позволяет контролировать и оценивать соответствие показателям процессов и процедур. Все заинтересованные стороны процессов осознают риски, важность и возможности ИТ. Руководством определены допустимые отклонения от стандартов, в рамках которых должно происходить исполнение процессов. Существует ограниченное, преимущественно тактическое, применение технологии

управления, основанной на развитых методиках и стандартизованных инструментальных средствах. Управление ИТ интегрировано с процессами стратегического и операционного планирования и мониторинга. Показатели эффективности всех видов ИТ деятельности фиксируются и отслеживаются в целях общекорпоративных усовершенствований. Налажена отчетность по основным процессам, менеджмент поощряется по результатам основных показателей эффективности. ***5. Оптимизированный***

Существует продвинутое понимание корпоративного управления ИТ, проблем ИТ и соответствующих решений, а также их перспектив. Обучение и информирование персонала обеспечивается самыми передовыми методами и концепциями. Благодаря постоянному совершенствованию, процессы соответствуют моделям зрелости, построенным на основе лучших практик. Внедрение ИТ политик привело к появлению сотрудников и процессов, которые способны быстро адаптироваться к изменяющимся условиям при полной поддержке требований корпоративного управления ИТ. Первопричины всех возникающих проблем и отклонений тщательно анализируются, затем определяются и принимаются соответствующие эффективные меры. Информационные технологии широко распространены, интегрированы, оптимизированы и применяются для автоматизации рабочего процесса и повышения качества и эффективности. Риски и отдача от ИТ определены и донесены до всех заинтересованных сотрудников организации. Внешние эксперты проводят сравнительный анализ. Контроль, внутренняя оценка, информирование об ожиданиях корпоративного управления ИТ являются нормальной практикой в организации и обеспечивают оптимальное использование технологий для поддержки проведения оценки, анализа, информирования и обучения. Корпоративное управление ИТ и корпоративное управление организацией стратегически взаимосвязаны и служат средством усиления эффективности технологических, человеческих и финансовых ресурсов с целью повышения конкурентоспособности организации. Деятельность по управлению ИТ интегрирована с общекорпоративным процессом управления.

Модель зрелости для среды внутреннего контроля

В данном приложении содержится общая модель зрелости, характеризующая состояние среды внутреннего контроля и постановку мер внутреннего контроля в организации. Она показывает, как управление средой (системой) внутреннего контроля и осознание в необходимости в более совершенных мерах внутреннего контроля развивается от начального до оптимизированного уровня. Модель предлагает общее руководство, чтобы помочь пользователям COBIT оценить, что именно необходимо им для построения эффективной среды внутреннего контроля в сфере ИТ и определить уровень ее зрелости в организации.

Уровень зрелости	Состояние среды внутреннего контроля	Установление мер внутреннего контроля
0. Несуществующий	Отсутствует понимание необходимости в системе внутреннего контроля. Контроль не является частью корпоративной культуры или миссии. Существует высокий риск недостатков и инцидентов.	Отсутствует потребность в оценке системы внутреннего контроля. Последствия инцидентов ликвидируются по мере их возникновения.
1. Начальный / Повторяющийся эпизодически и бессистемно	Существует определенное осознание потребностей в системе внутреннего контроля. Подходы в отношении рисков и требований контроля непоследовательны и неорганизованны, отсутствуют информирование заинтересованных сторон и процесс мониторинга. Недостатки не выявлены. Сотрудники не в полной мере осознают требования к своим должностным обязанностям.	Отсутствует осознание потребности в оценке того, что требуется в свете требований мер контроля в области ИТ. Даже когда элементы этого осознания существуют, оно непоследовательно, лишь в общих чертах, и является следствием существенных инцидентов. Процесс оценки применяется только в отношении реально произошедших инцидентов.
2. Повторяющийся, но интуитивный	Меры контроля существуют, но они не документированы. Их применение зависит от знаний и мотивации отдельных сотрудников. Эффективность деятельности не подвергается адекватной оценке. Существуют существенные недостатки в функционировании системы контроля, последствия которых могут быть серьезными. Усилия руководства по разрешению проблем в области контроля непоследовательны и не являются приоритетными. Сотрудники могут не в полной мере осознавать требования к своим должностным обязанностям.	Оценка потребностей в области контроля производится только в случае необходимости определить уровень зрелости определенных процессов, требуемый уровень, который должен быть достигнут, а также существующие недостатки. Для определения адекватного подхода в области контроля над процессами и обоснования согласованного плана действий проводятся неформальные рабочие совещания с участием руководства службы ИТ и сотрудников, участвующих в определенном процессе.
3. Определенный	Существуют и применяются документированные меры контроля. Эффективность деятельности оценивается на регулярной основе, выявлен ряд ограничений. Тем не менее, процесс оценки не документирован. В то время как руководство способно разрешать и предупреждать проблемы в сфере контроля, остаются определенные недостатки в функционировании системы контроля, последствия которых могут быть серьезными. Сотрудники осознают требования в соответсвии со своими должностными обязанностями в области контроля.	Выявлены наиболее важные ИТ процессы на основе их значимости и уровнем риска. Проведен детальный анализ для определения требований контроля, определения первопричин недостатков и выявления возможностей по усовершенствованиям. В дополнение к рабочим совещаниям, в рамках анализа применяются различные методики и проводятся интервью с целью убедиться в том, что владельцы ИТ процессов выполняют свою роль и стимулируют процессы оценки и усовершенствования.
4. Управляемый и измеряемый	Существует эффективная система внутреннего контроля и управления рисками. Регулярно проводится формализованная, документированная процедура оценки действенности мер контроля. Многие меры контроля автоматизированы и подвергаются регулярному анализу. Руководство выявило большинство проблем в области управления, однако не все проблемы выявляются в плановом порядке. Существует последовательность действий, предпринимаемых при выявлении проблемы. Для автоматизации мер контроля в тактических целях и в ограниченной форме применяются технологии.	Регулярно определяется степень важности ИТ процессов при полной поддержке со стороны владельцев бизнес процессов. Оценка требований в области мер контроля основана на политике и текущем состоянии зрелости процессов и следует тщательному и измеряемому анализу при участии заинтересованных сторон. Отчетность по результатам процедур оценки четкая и обязательная. Стратегии усовершенствования основаны на примерах из практики бизнеса. Эффективности в достижении желаемых выгод является предметом постоянного мониторинга. Эпизодически проводятся внешние независимые оценки эффективности контроля.
5. Оптимизированный	Программа контроля и управления рисками в масштабе всей организации обеспечивает эффективное и непрерывное разрешение проблем, связанных с рисками и мерами контроля. Система внутреннего контроля и управления рисками интегрирована с корпоративными практиками, которые поддерживаются с помощью автоматизированного мониторинга в режиме реального времени с полной отчетностью по вопросам контроля, управления рисками и соответствия требованиям. Оценка системы контроля производится на постоянной основе, основана на самооценках и анализе недостатков и первопричин. Сотрудники вовлечены в усовершенствование системы контроля в упреждающем стиле.	При изменениях бизнеса учитывается важность ИТ процессов а также необходимость в переоценке уровня мер контроля в процессах. Владельцы ИТ процессов регулярно проводят процедуры самооценки для того, чтобы убедиться в том, что меры контроля находятся на должном уровне зрелости и соответствуют требованиям бизнеса, а также учитывают атрибуты зрелости для того, чтобы сделать меры контроля более эффективными и результативными. В организации применяется сравнительный анализ внешних лучших практик и используются внешние консультации по совершенствованию эффективности системы внутреннего контроля. В отношении наиболее важных процессов проводится независимый анализ, чтобы удостовериться в том, что меры контроля находятся на должном уровне зрелости и соответствуют ожиданиям.

Глоссарий терминов

ISO 17799 — Международный стандарт, определяющий понятия конфиденциальности, целостности и доступности информации, а также меры контроля в этой области.

ISO 277001 — «Управление информационной безопасностью — Спецификация с указаниями по применению», международный стандарт, заменивший BS7799 2. Используется как основа независимого аудита и гармонизирован с другими стандартами в области управления, такими как ISO/IEC 9001 и 14001.

ISO 9001:2000 — Свод практик в области управления качеством, подготовленный Международной Организацией Стандартизации. ISO 9001:2000, определяет требования к системе управления качеством в любой организации, которая нуждается в том, чтобы демонстрировать возможность постоянно производить продукцию или услуги, соответствующие определенным качественным показателям.

Автоматизированный контроль приложений (Automated application control) — Комплекс контрольных мер, включенный в автоматизированные решения (приложения).

Анализ первопричин (Root cause analysis) — Процесс диагностики происхождения событий, который может применяться для изучения последовательностей, обычно состоящих из ошибок и проблем.

Библиотека ИТ инфраструктуры при Управлении правительственной коммерции Великобритании (IT Infrastructure Library, ITIL) — Комплекс наставлений по управлению и оказанию ИТ сервисов.

Бизнес процесс (Business process) — См. Процесс.

Владельцы данных (Data owners) — Лица, как правило, менеджеры или директора, которые несут ответственность за целостность, точную отчетность и использование компьютерных данных.

Внутренний контроль (Internal control) — Меры, планы, процедуры и организационные структуры предназначенные для обеспечения уверенности в том, что цели бизнеса будут достигнуты, нежелательные события предотвращены, либо обнаружены и исправлены.

Возможность, Способность (Capability) — Наличие необходимых характеристик для исполнения или завершения.

Генеральный директор, президент (Chief executive officer, CEO) — Высшее должностное лицо в организации.

Действие (Activity) — Основные виды деятельности, предпринимаемые в рамках процесса COBIT.

Директор службы по информационным технологиям (Chief information officer, CIO) — Должностное лицо организации, ответственное за работу ИТ. В некоторых случаях функции директора по ИТ расширяются до уровня Директора по знаниям (chief knowledge officer, CKO), который имеет дело с совокупностью знаний, а не только информацией. См. также Технический Директор.

Жизненный цикл разработки систем (System development life cycle, SDLC) — Фазы развертывания разработки или приобретения системы программного обеспечения. Как правило, фазы включают в себя обоснование, анализ необходимых требований, анализ определений, подробный проект, программирование, тестирование, установку и обзор системы после реализации, но не включает оказание услуг или отдачи от реализации.

Зрелость (Maturity) — Понятие, характеризующее степень, в которой бизнес может положиться на определенный процесс, ведущий к достижению желаемых целей.

Идентификация (Authentication) — Процедура проверки подлинности субъекта компьютерной системы (пользователя, системы, узла сети) и прав субъекта на доступ к компьютерной информации. Хотя идентификация предполагает собой защиту от несанкционированного доступа, под этим термином также понимается проверка целостности фрагмента данных.

Инструментальная панель (Dashboard) — Инструмент для отображения ожиданий организации на каждом из уровней ответственности и продолжительного мониторинга процессов на пути достижения поставленной цели.

Инструментальная панель ИТ инвестиций (IT investment dashboard) — Инструмент для определения ожиданий на каждом из уровней организации и для продолжительного мониторинга эффективности, согласно определенным затратам и прибылям от ИТ инвестиционных проектов.

Информационная архитектура (Information architecture) — Один из компонентов ИТ архитектуры (вместе с приложениями и технологией). См. ИТ архитектура.

Информационные технологии (IT) — Аппаратное и программное обеспечение, средства связи и другие активы, используемые для ввода, хранения, обработки, передачи и вывода данных в какой либо форме.

Информированный (Informed) — В таблице ОУКИ, лица, поставленные в известность о развитии какого либо действия (односторонний обмен информацией).

ИТ архитектура (IT architecture) — Описание фундаментального устройства ИТ компонентов организации, взаимосвязей между ними и способа, посредством которого компоненты системы обеспечивают достижение корпоративных целей.

ИТ архитектура организации (Enterprise architecture for IT) — Описание фундаментального устройства ИТ компонентов бизнеса, взаимосвязей между компонентами и способа, посредством которого компоненты системы обеспечивают достижение целей организации.

ИТ инцидент (IT incident) — Любое событие, не являющееся штатным элементом ИТ сервиса, которое причиняет, или может причинить сбой или снижение качества (в соответствии с ITIL).

Ключевой показатель достижения цели (Key goal indicator, KGI) — Показатель, который сообщает менеджменту постфактум, достиг ли ИТ процесс бизнес целей, обычно выражен в терминах информационных критериев.

Ключевой показатель эффективности (Key performance indicator, KPI) — Показатель, определяющий, насколько хорошо процесс ведет к намеченной цели. Это — «индикатор опережения», показывающий, что цель, вероятно, будет достигнута, а также индикатор возможностей, практик и навыков. Индикатор оценивает деятельность по достижению целей, то есть действия, которые владелец процесса должен предпринять для достижения эффективности процесса.

Ключевые практики управления (Key management practices) — Практики управления, которые необходимы для успешной реализации бизнес процессов.

Комитет спонсорских организаций Комиссии Тредуэя (Committee of Sponsoring Organisations of the Treadway Commission, COSO) — Доклад Комитета «Внутренний контроль — интегрированная структура» от 1992 года является признанным международным стандартом в области корпоративного управления. См. сайт www.coso.org

Консультирующий (Consulted) — В таблице ОУКИ, лица, чьи мнения учитываются в ходе определенной деятельности (двусторонний обмен информацией).

Контроль доступа (Access control) — Процесс, устанавливающий ограничения и контролирующий доступ к ресурсам компьютерной системы. Для защиты от несанкционированного доступа применяется логический либо физический контроль.

Контроль обнаружения (Detective control) — Контроль, применяемый для обнаружения явлений (желательных или нежелательных), ошибок и других инцидентов, которые, по мнению организации, могут материально влиять на процесс или конечный продукт.

Корпоративная архитектура (Enterprise architecture) — Описание фундаментального устройства компонентов бизнес системы или одного из ее компонентов (например, технологии), взаимосвязь между компонентами и способ, посредством которого компоненты системы обеспечивают достижение целей организации.

Корпоративное управление (Enterprise governance) — Группа ответственных лиц и комплекс практических действий, предпринимаемых Советом директоров и высшим руководством организации с целью обеспечить реализацию стратегических планов, удостовериться, что поставленные цели достигнуты, управление рисками осуществляется на должном уровне, ресурсы организации используются ответственно.

Критический фактор успеха (Critical success factor, CSF) — Наиболее важные вопросы или действия менеджмента, направленные на налаживание контроля над и внутри ИТ процессов.

Лучшие практики, рекомендуемые нормы (Best practice) — Проверенная деятельность (процесс), успешно применяемая многими организациями.

Мера (Measure) — Стандарт, применяемый для оценки эффективности в связи с ожидаемыми результатами. Мера обычно является количественным показателем и выражается в цифрах, долларах, процентах и т. д., но может также характеризовать качественную информацию, как, например, удовлетворенность потребителя. Отчетность и мониторинг мерам помогают организации оценить прогресс в реализации намеченной стратегии.

Методология (Framework) — См. Методология контроля (Control framework).

Методология контроля (Control framework) — Набор фундаментальных мер контроля, которые помогают участникам бизнес процесса предотвратить финансовые или информационные потери организации.

Модель зрелости CMM (Capability Maturity Model, CMM) — Модель зрелости для программного обеспечения, термин предложен Инженерным институтом программного обеспечения (Software Engineering Institute, SEI). Модель, используемая многими организациями для определения правильных практик, способствующих оценить и повысить уровень зрелости процессов разработки программного обеспечения.

Непрерывность (Continuity) — Предотвращение, нивелирование последствий и восстановление после прерывания или сбоя. Понятия «планирование восстановления бизнеса», «планирование восстановления после сбоя» и «планирование непредвиденных обстоятельств» также могут применяться в данном контексте, все эти термины обращаются к аспектам восстановления.

Общая стоимость владения (Total cost of ownership, TCO) — Включает в себя:

- Первичную стоимость компьютерного и программного обеспечения;
- Обновления аппаратного и программного обеспечения;
- Сопровождение;
- Техническую поддержку;

- Обучение;
- Определенные виды деятельности, выполняемой пользователями.

Общие компьютерные меры контроля (General computer controls) — Меры контроля (в отличие от мер контроля приложений) средой, внутри которой разрабатываются, поддерживаются и работают системы компьютерных приложений. Общие компьютерные меры контроля применимы ко всем приложениям. Цели общих мер контроля сводятся к должной разработке и реализации приложений, обеспечению целостности программ, данных и компьютерных операций. Как и меры контроля приложениями, общие меры контроля могут быть ручными или программными. Примерами общих мер контроля являются разработка и реализация стратегии ИТ и политик информационной безопасности, организация персонала ИТ таким образом, при котором исключены конфликты между должностными обязанностями, а также планирование предотвращения сбоев и во сстановления.

Объект конфигурации (Configuration item, CI) — Компонент инфраструктуры или объект, требующий настроек, связанных с инфраструктурой, которая находится под контролем (или должна находиться под контролем) должностных лиц, ответственных за конфигурацию. Объекты конфигурации могут весьма разниться по сложности, размерам и типам — от целой системы (включающей аппаратную часть, программное обеспечение и документацию) до отдельного модуля или небольшого аппаратного компонента.

Организация (Organisation) — Организационная структура, также может означать юридическое лицо.

Организация, компания (Enterprise) — Группа лиц, совместно работающих над достижением общей цели, обычно в рамках единой организации (корпорации, государственного учреждения, благотворительной организации или трастового фонда).

Ответственный (Responsible) — В таблице ОУКИ должностное лицо, которое должно обеспечить успешное выполнение работ (видов деятельности).

План технологической инфраструктуры (Technology infrastructure plan) — План в отношении технологий, кадровых ресурсов, оборудования и помещений, обеспечивающий работу и использование приложений в настоящем и будущем.

Показатель (Metrics) — Специфическое описание того, как должна измеряться количественная и периодическая оценка эффективности. В законченном виде показатель определяет использование отдельных единиц, частоту, целевую величину, процедуру проведения измерений и процедуру интерпретации оценки.

Политика (Policy) — Обычно, документ, в котором отражены общие принципы или выработанный курс действий. Предназначение политики — оказывать влияние на принятие решений в настоящем и будущем в соответствии с философией, целями и стратегическими планами, принятыми руководством организации. Кроме того, политика должна описывать последствия невыполнения своих положений, методы работы с исключениями, и способы проверки и измерения соответствия политике.

Положение об аудите (Audit charter) — Документ, утвержденный Советом директоров, который определяет цели, полномочия и ответственность внутреннего аудита.

Пользователь ИТ (IT user) — Лицо, которое использует ИТ для поддержки или достижения целей бизнеса.

Портфель (Portfolio) — Группа программ, проектов, услуг и активов, отобранных, управляемых и наблюдаемых для оптимизации результатов бизнеса.

Практика (мера) контроля (Control practice) — Ключевой механизм контроля, который ведет к достижению контрольных целей посредством ответственного использования ресурсов, соответствующего целям управления рисками и выстраивания ИТ в соответствии с целями бизнеса.

Превентивный контроль (Preventive control) — Вид внутреннего контроля, который применяется для предупреждения нежелательных событий, ошибок и других инцидентов, которые, по мнению организации, могут оказать негативное материальное воздействие на процесс или конечный продукт.

Проблема (Problem) — В ИТ — неизвестная причина, лежащая в основе одного или многих инцидентов.

Программа (Programme) — Структурированная группа взаимозависимых проектов, существующая в масштабах бизнеса, процессов, людей, технологии и организационной деятельности, требуемых (необходимых и достаточных) для достижения определенных результатов бизнеса.

Программное приложение (Application program) — Компьютерная программа, осуществляющая обработку бизнес данных, в частности, ввод данных, обновление или запрос. Бизнес приложение отличается от системных программ (таких как операционная система или программа контроля сети) и от сервисных программ (таких как копирование и сортировка данных).

Проект (Project) — Структурированный комплекс видов деятельности, имеющий целью создать для организации новую возможность (что необходимо, но недостаточно для достижения требуемых результатов бизнеса), основанный на согласованном графике и бюджете.

«Проекты в контролируемой среде 2» (PRINCE2) — Метод управления проектами, разработанный OGC, охватывает управление, контроль и организацию проекта.

Процедура (Procedure) — Документ, включающий в себя шаги, описывающие достижение результата. Процедуры определяются как часть процессов.

Процесс (Process) — В общем, процесс представляет собой набор процедур, на которые оказывает влияние политика организации и процедур, происходящих из различных источников, включая другие процессы. Процессы имеют четкие, обусловленные бизнесом, причины для возникновения, ответственных владельцев, должностные обязанности, связанные с исполнением процесса и средства измерения эффективности.

Раздел, домен (Domain) — В COBIT — группирование контрольных целей в логические этапы внутри жизненного цикла ИТ инвестиций («Планирование и организация», «Приобретение и внедрение», «Эксплуатация и сопровождение», «Мониторинг и оценка»).

Разделение обязанностей (Segregation/separation of duties) — Основной вид внутреннего контроля, который предотвращает или выявляет ошибки и несоответствия путем назначения различных лиц ответственными за инициации и осуществление операций, а также управление активами. Обычно применяется в крупных ИТ организациях с тем, чтобы никто не имел возможности незаметно произвести мошеннические или злоумышленные действия.

Результативные показатели (Outcome measures) — Показатели, отражающие последовательность ранее предпринятых действий и часто подразумеваются как «индикаторы задержки». Они зачастую концентрируются на результатах, полученных в конце определенного периода времени и характеризуют эффективность в прошлом. Они также понимаются как ключевые показатели достижения цели (KGIs) и используются для того, чтобы определить, достигнуты ли цели. Результативные показатели могут фиксироваться только после факта и поэтому они называются «индикаторами задержки».

Риск (Risk) — В бизнесе — потенциал, несущий в себе угрозу того, что по причине уязвимости будут утрачены (либо нанесен ущерб) актив или группа активов. Обычно риск измеряется соотношением воздействия (последствий) и вероятности инцидента.

Руководитель проектного офиса (Project management officer, PMO) — Лицо, ответственное за управление проектами и поддерживающее дисциплину управления проектами.

Свод знаний по управлению проектами (Project Management Body of Knowledge, PMBOK) — Стандарт в области управления проектами, разработанный Институтом по управлению проектами (PMI).

Сервис провайдер (Service provider) — Внешняя компания, которая оказывает услуги организации.

Система контроля качества (Quality management system, QMS) — Система, которая очерчивает политику и процедуры, необходимые для улучшения и контроля различных процессов, которые, в конечном счете, приведут к повышению эффективности организации.

Система сбалансированных показателей (Balanced scorecard) — Логически последовательный набор показателей эффективности, сгруппированных по четырем категориям. Включает в себя традиционные финансовые показатели, а также показатели, касающиеся потребителей, внутренних бизнес процессов и дальнейших перспектив развития. Система сбалансированных показателей была предложена Робертом С. Капланом (Robert S. Kaplan) и Дэвидом П. Нортоном (David P. Norton) в 1982 году.

Служба поддержки (Service desk) — Точка контакта пользователей ИТ услуг со службой ИТ.

Соглашение об уровне сервиса (Service level agreement, SLA) — Соглашение, желательно документированное, между сервис провайдером и потребителем (ями)/пользователем (ями), в котором определены минимальные цели по оказываемым услугам и методы измерения их эффективности.

Соглашение операционного уровня (Operational level agreement, OLA) — Внутреннее соглашение, специализирующее механизм оказания услуг по ИТ сервисам.

Справочник данных (Data dictionary) — База данных, включающая в себя название, тип, диапазон значений, источник и авторизацию доступа к каждому из ее элементов. Справочник данных также отображает, какое из приложений использует эти данные, таким образом, что во время работы с данными, можно получить список работающих с ними программ. Справочник данных может быть реализован как отдельная информационная система, используемая для управления или документирования процессов, либо может контролировать операции с базой данных.

Сравнительный анализ (Benchmarking) — Систематизированная методология сравнения показателей эффективности организации с аналогами, конкурентами для понимания лучших подходов к ведению бизнеса (например, сравнительный анализ качества, эффективности логистики и прочих характеристик).

Стандарт (Standard) — Обязательное требование. Примерами являются стандарт ISO/TEC 20000 (международный стандарт), стандарт по внутренней безопасности систем UNIX или правительственный стандарт ведения финансового учета. Термин «стандарт» также применяется в отношении свода практик или спецификаций, публикуемых такими организациями по стандартам, как ISO или BSI.

Стратегический комитет по ИТ (IT strategy committee) — Комитет создается на уровне Совета директоров с целью вовлечения Совета в обсуждение основных вопросов и решений по ИТ. Комитет в первую очередь ответственен за управление портфелями ИТ инвестиций, ИТ сервисами и другими ИТ ресурсами. Комитет является владельцем портфеля ИТ инвестиций.

Стратегический план по ИТ (IT strategic plan) — Долговременный (то есть от трех до пяти лет) план, в котором корпоративный и ИТ менеджмент совместно описывают, как ресурсы ИТ будут способствовать достижению стратегических целей организации.

Схема классификации данных (Data classification scheme) — Схема классификации данных (в масштабе организации) по таким факторам, как критичность, важность и принадлежность.

Таблица ОУКИ (RACI chart) — Иллюстрирует, кто из должностных лиц внутри организационной структуры является ответственным (О), утверждающим (У), консультирующим (К) и информированным (И).

Тактический план по ИТ (IT tactical plan) — Среднесрочный (от 6 до 18 месяцев) план, в котором положения стратегического плана по ИТ преобразуются в необходимые шаги, требования по ресурсам, и способы, посредством которых будут осуществляться управление и мониторинг ресурсов и преимуществ.

Технический директор (Chief technology officer, CTO) — Должностное лицо организации, ответственное за техническое обеспечение. Должность Технического Директора часто понимается как аналог должности Директора по информационным технологиям.

Указание (Guideline) — Описание определенного способа совершенствования чего либо; менее предписывающее, чем процедура.

Управление конфигурацией (Configuration management) — Управление настройками объектов конфигурации на протяжении их жизненного цикла.

Управление эффективностью (Performance management) — в ИТ — способность управлять любой системой мер, включая сотрудника, команду, процесс, операционную или финансовую систему мер. Термин ассоциирован с замкнутой системой контроля, и регулярным мониторингом показателей.

Устойчивость (Resilience) — В бизнесе — способность системы или сети к автоматическому восстановлению после сбоев, обычно с минимально заметным эффектом.

Утверждающий (Accountable) — В таблице ОУКИ, лицо, либо группа лиц, наделенных полномочиями утвердить или принять исполненную работу.

Факторы эффективности (Performance drivers) — Показатели, которые рассматриваются как «движители» индикаторов задержки. Эти показатели могут быть измерены до завершения и поэтому они называются «индикаторами опережения». Существует принятое мнение о взаимосвязи между этими двумя типами индикаторов, согласно которому, повышение эффективности, зафиксированное «индикатором опережения» ведет к повышению эффективности, которое будет зафиксировано «индикатором задержки». Они также понимаются как ключевые индикаторы эффективности (KPIs) и применяются для выявления ситуаций, когда велика вероятность достижения целей.

Финансовый директор (Chief financial officer, CFO) — Должностное лицо организации, в первую очередь ответственное за управление финансовыми рисками.

Цель контроля (Control objective) — Формулировка, содержащая желаемый результат или цель, которая должна быть достигнута при выполнении процедур контроля определенного процесса.

Эффективность (Performance) — В ИТ — воплощение или достижение целей процесса.