SOLUTIONACCELERATORS

Действуй быстрее. Достигни большего.

Microsoft® Operations Framework

Версия 4.0

SMF-функция «Управление, риск и соответствие нормативным требованиям»

Дата публикации: апрель 2008 г.

Последние сведения см. на веб-странице
microsoft.com/technet/solutionaccelerators

Microsoft

Содержание

Место SMF-функции «Управление, риск и соответствие нормативным требованиям» в жизненном цикле ИТ-услуги MOF

Жизненный цикл ИТ-услуги в модели процессов Microsoft® Operations Framework (MOF) охватывает все действия и процессы управления ИТ-услугой: планирование, разработку, эксплуатацию, обслуживание и, в итоге, вывод из эксплуатации. В модели MOF эти действия и процессы упорядочены в виде функций управления ИТ-услугами (SMF-функций), которые группируются по этапам жизненного цикла. Каждая SMF-функция входит в определенный этап жизненного цикла и содержит уникальный набор целей и результатов, отвечающих назначению этого этапа. SMF-функции можно использовать как автономный набор процессов, но только их взаимодействие обеспечивает наиболее эффективное предоставление услуги с требуемым качеством и уровнем риска.

SMF-функция «Управление, риск и соответствие нормативным требованиям» (GRC) относится к уровню «Управление», который является основой жизненного цикла ИТ-услуги. Следующий рисунок иллюстрирует место SMF-функции GRC в уровне «Управление» и положение этого уровня в жизненном цикле ИТ-услуги.

Рис. 1. Место SMF-функции GRC в жизненном цикле ИТ-услуги

Перед использованием этой SMF-функции стоит ближе ознакомиться с жизненным циклом ИТ-услуги в модели MOF и уровнем «Управление», прочитав следующие руководства по MOF 4.0:

- *Обзор MOF*
- *Обзор уровня «Управление»*

Назначение SMF-функции «Управление, риск и соответствие нормативным требованиям»

Эта SMF-функция будет полезна сотрудникам, которые принимают компромиссные решения о том, как использовать ИТ-ресурсы, чтобы достичь поставленных целей и обеспечить создание коммерческой ценности, управляют рисками разного происхождения (не только риски для безопасности ИТ), а также обеспечивают соблюдение ИТ-подразделением действующих требований и директив. Правила и принципы функции «Управление, риск и соответствие нормативным требованиям» применяются при выполнении процессов и действий на всем протяжении жизненного цикла ИТ-услуги.

Функция охватывает следующие задачи:

- Учреждение управления ИТ
- Оценка, мониторинг и контроль рисков
- Соблюдение директив

Обзор SMF-функции «Управление, риск и соответствие нормативным требованиям»

В рамках SMF-функции «Управление, риск и соответствие нормативным требованиям» выполняются имеющие большие перспективы взаимосвязанные действия, в которых должны участвовать все сотрудники организации. Обеспечить правильное понимание столь широкой темы всеми сторонами не всегда просто. Чтобы прояснить некоторые аспекты, в последующих разделах мы разобьем на фрагменты область действия SMF-функции GRC и обсудим следующие вопросы:

- Что такое GRC
- Почему три процедуры рассматриваются вместе
- ИТ-роли и их обязанности в разрезе SMF-функции GRC
- Место SMF-функции GRC в жизненном цикле ИТ-услуги

Что такое «Управление, риск и соответствие нормативным требованиям»

Управление ИТ — деятельность на уровне высшего руководства, которая, при условии надлежащего выполнения, проясняет, кто имеет право принимать решения, устанавливает ответственность за действия и результаты, а также определяет, как будет оцениваться ожидаемая производительность. Большинство организаций для управления ИТ создает группы (такие как руководящие комитеты), которые объединяют в своем составе все стороны, необходимые для принятия решений.

Общеорганизационное управление, помимо прочего, формирует положительные ожидания в отношении результатов деятельности и роста, а также определяет способы повышения качества обслуживания заказчиков, усовершенствования новых продуктов и освоения рынка (сферы, в которых ИТ-подразделение способно внести весомый вклад при условии координации всех управленческих усилий).

Управление происходит независимо от наличия планов. Отсутствие спланированных процессов управления может привести к произволу в постановке целей и принятии решений, политическим столкновениям и бессмысленной трате ресурсов в ходе беспорядочной и противоречивой деятельности. Спланированное управление обеспечивает следующие преимущества:

- Согласованные, эффективно взаимодействующие политики
- Четкое и ответственное принятие решений с согласованным планом выбора компромиссов
- Четко заявленные цели управления
- Сформированные ожидания в отношении производительности и оценки соблюдения требований
- Четкие ожидания в отношении приемлемых способов достижения целей управления

Риск олицетворяет возможное отрицательное воздействие на достижение целей и может появиться в результате выполнения или невыполнения каких-то действий. С помощью процессов управления организации определяют приоритеты и уровень усилий, необходимых для снижения вероятности или масштабов риска.

Качественные процессы управления позволяют идентифицировать риск, устроить открытое обсуждение и найти четкие подходы к устранению риска. Устоявшаяся процедура управления рисками предотвращает умышленное игнорирование или намеренное утаивание риска, а также уменьшает количество неизвестных рисков, способных вызвать негативные последствия.

Внутренние меры контроля — это процессы и системы, используемые для нейтрализации рисков и смягчения возможных последствий. В наиболее общем смысле внутренние меры контроля обеспечивают средства для достоверного достижения целей управления, формируя положительные результаты для заинтересованных сторон.

Процесс соблюдения требований гарантирует, что люди знают о правилах, политиках и процедурах, установленных высшим руководством. Кроме того, в его рамках производится оценка того, что в действительности происходит в организации по сравнению с ожидаемыми результатами, сформулированными посредством целей управления, политик и нормативных требований.

Соблюдение требований к ИТ улучшается, если организация установила и опубликовала четкие ожидания в отношении ИТ и обязательные политики, а также заблаговременно разработала способы оценки производительности и качества принимаемых решений.

На выполнение работ влияют внешние факторы, например регулятивные нормы, стандарты и отраслевые рекомендации. Более эффективной оценке и внедрению этих факторов способствует наличие адекватных процессов функции GRC. Например, существует ряд законов и норм, регулирующих надежность данных и доверие к организации. ИТ-подразделение обязано соблюдать предписания различных учреждений, от Комиссии по ценным бумагам и биржам (США) до Европейского Союза, а также законы в области управления данными, например акт HIPPA, закон о защите данных, первое и второе базельские соглашения, закон Сарбейнса — Оксли (SOX). Функция GRC дает компании и ее ИТ-подразделению следующие преимущества:

- Более надежное хранение данных
- Соблюдение нормативных требований
- Повышенная готовность к достижению целей управления
- Меньшая уязвимость в плане мошенничества

Почему три процедуры рассматриваются вместе как функция «Управление, риск и соответствие нормативным требованиям»

Три процедуры (управление ИТ, управление рисками и соблюдение требований) реализуют общие и взаимосвязанные задачи. Из-за перекрывающихся сфер ответственности и процессов эффективность процедур повышается в случае их интеграции и выполнения как одного целого. В результате снижается разобщенность данных и действий, которая ухудшает способность организации к реагированию и увеличивает риски, затрудняя их идентификацию и не позволяя адекватно оценить их воздействие. Объединение процедур оптимизирует процессы, а также улучшает прозрачность и подотчетность деятельности. Это достигается следующими способами:

- Объединение надлежащих групп людей (*управление*) с целью прояснения, что должно произойти, и оценки, что этому может помешать (*управление рисками*)
- Распределение ресурсов организации (*управление*), необходимое для достижения ее целей (*управление рисками*)
- Определение (*управление и соблюдение требований*) процессов и действий, которые должны или не должны выполняться (*управление рисками и соблюдение требований*)
- Регистрация и документирование процессов и их результатов (*соблюдение требований*)

Когда организация принимается за реализацию процессов функции GRC, определить контекст помогают несколько ключевых вопросов. Чтобы ответить на них, скорее всего, придется подключить к обсуждению внешние по отношению к ИТ-подразделению группы (внутренние аудиторы, юристы, специалисты по соблюдению требований, кадровые сотрудники и т. п.).

- Используемая организацией схема управления (кто решает, как и какие решения принимаются).
- Допустимые риски для организации (где допустим повышенный риск, а в каких сферах требуется максимальная осторожность).
- Конкретные нормативные и законодательные требования, которые применимы к отрасли.
- Культура соблюдения требований (т. е. метод, определяющий, делается ли то, что должно делаться).

Ответы на эти вопросы и использование интегрированных планов для процессов функции GRC повысит согласованность целей бизнеса и ИТ, поскольку решения будут своевременно приниматься компетентными людьми.

Исполнители процессов «Управление, риск и соответствие нормативным требованиям»

В той или иной мере участие в процессах GRC принимают все сотрудники организации, однако три группы являются основными: ИТ-руководители, ИТ-менеджеры и ИТ-специалисты. Эти группы имеют разные интересы и уровни вовлеченности в процессы функции GRC.

ИТ-специалисты обеспечивают применение решений, принятых в рамках процессов управления, при выполнении повседневных действий и процедур. В первую очередь они занимаются вопросами соблюдения нормативных требований и, используя глубокие технические знания, идентифицируют и нейтрализуют риски, а также ищут пути эффективной автоматизации мер контроля. ИТ-специалисты следят, чтобы выполнение действий и функционирование систем соответствовало инструкциям процесса GRC. Они располагают профильными знаниями, которые позволяют улучшать меры контроля с учетом технических возможностей и ограничений.

ИТ-менеджеры часто принимают участие в работе групп GRC, которые ищут компромиссные решения. Основной управленческой задачей является преобразование стратегических целей, установленных на уровне высшего руководства и совета правления, в тактические, конкретные директивы и политики, которые затем превратятся в услуги, решения, политики и повседневные действия. ИТ-менеджеры занимаются преобразованием стратегических целей в тактические, анализом рисков, которые связаны с достижением этих целей, а также поиском внутренних мер контроля для нейтрализации выявленных рисков.

И наконец, ИТ-директор отвечает на уровне руководства за весь процесс GRC внутри ИТ-подразделения. Необходимо разработать схемы, обеспечивающие своевременное объединение компетентных людей для эффективного управления реализацией стратегии. ИТ-директор следит, чтобы частью обсуждения на таких управленческих форумах было управление рисками, которое помогает делать обоснованный выбор и находить общий знаменатель в процессе принятия компромиссных решений.

Кроме того, ИТ-директору необходимо разбираться в функциях аудита, которые оценивают цели, внутренние меры контроля, а также их структуру и операционную эффективность. Аудит обеспечивает предоставление информации и рекомендаций высшему руководству и совету правления, обеспечивая разумное, обоснованное управление. Акционеры и другие внешние заинтересованные стороны могут получать представление о работе организации. Осведомленность ИТ-директора о результатах аудита гарантирует, что подход к управлению формируется высшим руководством организации, а действия в рамках процессов GRC понятны и выполняются на всех ее уровнях.

Связь SMF-функции «Управление, риск и соответствие нормативным требованиям» с жизненным циклом ИТ-услуги

Каждому этапу жизненного цикла ИТ-услуги соответствуют определенные цели и действия. Участниками отдельных этапов могут быть разные люди и группы, могут отличаться входные данные и конечные результаты, однако наличие ясности по поводу принятия решений, управления рисками и соблюдения нормативных требований имеет огромнейшее значение.

На этапе «Планирование» необходимо гарантировать, что бизнесу предлагаются ценные, предсказуемые, надежные и экономически эффективные ИТ-услуги, которые отвечают непрерывно меняющимся бизнес-потребностям.

В этом отношении внимание SMF-функции GRC сосредотачивается на следующих моментах:

- Воплощение корпоративной стратегии в стратегию ИТ
- Структура управления и право принятия решений
- Установленные цели управления
- Главные риски для достижения установленных целей
- Общая нормативно-правовая среда
- Заданная политика

Цель этапа «Внедрение» состоит в том, чтобы ИТ-услуги, согласованные бизнес- и ИТ-подразделением, эффективно разрабатывались, успешно развертывались и готовились к эксплуатации.

На этом этапе SMF-функция GRC ориентирована на следующее:

- Архитектура решения, поддерживающая организационные требования
- Заинтересованные стороны, методология и выявленные риски для проекта
- Процесс реализации ценности
- Цикл разработки ИТ-услуги
- Нейтрализация рисков
- Определение внутренних мер контроля
- Определение процедур

На этапе «Эксплуатация» необходимо обеспечить, чтобы развернутые услуги эксплуатировались, обслуживались и поддерживались в соответствии с требованиями SLA, согласованными бизнес- и ИТ-подразделением.

На этом этапе SMF-функция GRC ориентирована на следующее:

- Процедуры и меры контроля
- Запись и документирование
- Регистрация свидетельств того, что меры контроля функционируют надлежащим образом

Путем принятия решений, балансирования компромиссов, подготовки стратегии управления рисками и обеспечение адекватности управления рисками выполняемым действиям SMF-функция GRC создает упорядоченные последовательности процессов для всех этапов жизненного цикла. Надзирая за этими процессами, ИТ-подразделение вносит свой вклад в обеспечение долгосрочной жизнеспособности организации и совершенствование ее деятельности, а также четко формулирует свой подход к эксплуатации ИТ и управлению рисками.

Типы ролей для SMF-функции «Управление, риск и соответствие нормативным требованиям»

Основные ответственности SMF-функции «Рабочая группа» в отношении SMF-функции GRC (GRC) — ответственность «Управление» и ответственность «Соблюдение требований». В следующих таблицах описаны все роли в рамках ответственностей, а также основные действия для данной SMF-функции.

Таблица 1. Ответственность «Управление» и ее роли

Тип роли	Обязанности	Роль в данной SMF-функции
ИТ-директор	• Спонсирует ИТ-функцию GRC • Утверждает структуры и общие процессы • Использует показатели и их сопоставление для оценки производительности функции GRC • Участвует в принятии решений	• Владеет руководством процессами GRC и принятием ИТ-решений • Обеспечивает четкое владение и ответственность • Выявляет тенденции в производительности функции GRC • Обеспечивает наличие плана усовершенствования
ИТ-менеджер	• Контролирует процессы управления • Определяет и вовлекает участников процесса GRC • Управляет зависимостями для рисков и реализации коммерческой ценности ИТ • Отвечает за отношения между бизнесом и ИТ • Использует показатели для оценки производительности функции GRC	• Следит, чтобы функция GRC была интегрирована с принятием управленческих решений • Обеспечивает четкое понимание состояния дел в области соблюдения требований • Способствует согласованию бизнеса и ИТ через процессы GRC • Обеспечивает использование показателей функции GRC в отчетности и планировании усовершенствований
Менеджер ИТ-политик	• Понимает компромиссные решения в сфере GRC, а также результаты, отраженные в политиках	• Следит, чтобы политики отражали результаты процесса GRC и эффективно направляли организацию на путь выполнения надлежащих действий
Менеджер по рискам и нормативным требованиям в области ИТ	• Общее управление рисками и программами соблюдения нормативных требований	• Обеспечивает качественное информирование об ожиданиях и процессах GRC

Тип роли	Обязанности	Роль в данной SMF-функции
	• Информирует организацию о процессах и требованиях SMF-функции GRC	• Гарантирует, что сотрудники понимают свои обязанности в рамках функции GRC и действуют надлежащим образом
Специалист по аудиту и отчетности	• Проверяет дизайн и эксплуатационную эффективность структур и процессов GRC • Рекомендует изменения с целью улучшения	• Следит, чтобы SMF-функция GRC находилась под постоянным наблюдением и непрерывно совершенствовалась
Менеджер по изменениям	• Контролирует для организации процесс управления изменениями	• Следит, чтобы результатом процессов GRC были понятные изменения • Обеспечивает управление рисками
Администратор конфигураций	• Отслеживает изменения и их влияние • Отслеживает конфигурационные элементы • Обновляет систему управления конфигурациями	• Следит, чтобы результатом процессов GRC всегда было понятное изменение и известное состояние

Таблица 2. Ответственность «Соблюдение требований» и ее роли

Тип роли	Обязанности	Роль в данной SMF-функции
ИТ-директор	• Публикует ИТ-стратегию и утверждает цели управления ИТ • Утверждает политику • Формирует поведение в отношении управления и соблюдения нормативных требований	• Следит, чтобы стратегические цели достигались с использованием надлежащих и желательных действий
ИТ-менеджер	• Информирует о политике и следит за ее исполнением • Оценивает эффективность политик и их соблюдение • Делает запросы на изменение политики и запросы на исключения	• Обеспечивает соблюдение директив и политик • Обеспечивает достижение прогнозируемых и достоверных результатов надлежащим образом • Обеспечивает эффективное и своевременное реагирование на нарушение политики

Тип роли	Обязанности	Роль в данной SMF-функции
Менеджер по рискам и нормативным требованиям в области ИТ	• Общее управление рисками и программами соблюдения нормативных требований • Следит, чтобы сотрудники понимали нормативные требования и умели их соблюдать • Идентифицирует возможности усовершенствования процессов путем анализа непредвиденных событий и случаев несоблюдения требований	• Координирует и согласует управление рисками и соблюдение нормативных требований • Обеспечивает обучение и подготовку сотрудников по вопросам соблюдения • Обеспечивает реагирование на непредвиденные события
Менеджер ИТ-политик	• Управляет всем жизненным циклом политики • Информирует о политике сотрудников организации и собирает их отзывы • Координирует запросы на исключения из политик	• Следит, чтобы политики были четкими, актуальными, понятными и формировали надлежащий образ действий
Специалист по аудиту и отчетности	• Изучает случаи несоблюдения и обхода политик • Составляет отчеты и рекомендует изменения	• Осуществляет независимый контроль соблюдения требований • Выявляет случаи мошенничества и намеренного недозволенного поведения

Цели SMF-функции «Управление, риск и соответствие нормативным требованиям»

Самая главная цель SMF-функции GRC состоит в предоставлении эффективных и целесообразных ИТ-услуг, которые соответствуют нормативным требованиям. Это включает в себя следующие процессы:

- Формирование понятного и эффективного механизма принятия решений по управлению основными средствами ИТ
- Эффективное управление рисками
- Соблюдение применимых политик, законов и норм

Таблица 3. Результаты и критерии достижения целей SMF-функции GRC

Результат	Критерии оценки
Качественное управление	• Действия в области ИТ обеспечивают желаемый возврат инвестиций • Использование основных средств ИТ в соответствии с прогнозами • Своевременное принятие решений без потребности в перепроверке • Конфиденциальность, целостность и доступность основных средств ИТ соответствует бизнес-потребностям и директивам • Своевременное создание политик и управление ими
Эффективное управление рисками	• Проактивная идентификация возможных уязвимостей и угроз для основных средств компании и управление ими • Четкий, документированный процесс идентификации рисков, определения степени их воздействия и вероятности проявления, их приоритизации и управления ими путем нейтрализации, передачи и принятия, а также поиска надлежащих мер контроля и решений • Конфиденциальность, целостность и доступность основных средств ИТ
Соблюдение политик, законов и норм	• Управление воздействием законов и норм на реализацию коммерческой ценности • Идентификация применимых организационных политик, законов и норм • Проектирование, разработка и развертывание основных активов ИТ, поддерживающих соблюдение законов и норм • Поиск измеримых мер контроля для аудита и управления

Основные термины

В следующей таблице приведены определения основных терминов, которые встречаются в настоящем руководстве.

Таблица 4. Основные термины

Термин	Определение
Обеспечение соответствия нормативным требованиям	Процессы, обеспечивающие соответствие ИТ нормативным требованиям, законам и политикам компании. Иначе говоря, способ уведомить сотрудников о надлежащих действиях и убедиться в том, что организация действительно делает то, что она должна делать.
Непредвиденная ситуация	Процесс, который позволяет организации подготовиться к согласованному реагированию на запланированные результаты и незапланированные инциденты.
Свидетельство	Проверяемое доказательство того, что политики и процессы работают в штатном режиме.
Управление	Кто и как должен принимать решения, как и когда можно эффективно обмениваться данными, как отслеживать успехи ИТ-подразделения в сравнении с бизнес-целями.
Основные средства ИТ	Информация, данные, интеллектуальная собственность, система или компьютер, которые принадлежат компании и используются для осуществления коммерческой деятельности.
Меры контроля	Конкретное действие, которое выполняют люди или системы, чтобы обеспечить достижение бизнес-целей.
Нейтрализация риска	Процессы или действия, выполняемые с целью смягчения возможных последствий риска путем снижения его вероятности или степени его влияния.
Риск	Возможность неблагоприятного воздействия на достижение целей бизнеса или ИТ. Риск измеряется с точки зрения воздействия, вероятности и подверженности.
Управление рисками	Усилия организации, направленные на устранение рисков для ИТ-среды.

Связь между управлением, рисками и соответствием нормативным требованиям

Рис. 2. Связь между управлением, рисками и соответствием нормативным требованиям

С точки зрения процессов, SMF-функция GRC отличается от многих SMF-функций модели MOF. Ее применение не носит последовательного характера — сначала А, затем Б, потом В. Как видно из рис. 2, функция состоит из трех наборов процессов (управление, риски и соответствие нормативным требованиям), которые могут выполняться как одновременно, так и один за другим.

Для простоты понимания будем рассматривать эти взаимосвязанные действия как отдельные процессы:

- Учреждение управления ИТ
- Оценка, мониторинг и контроль рисков
- Соблюдение директив

Подробное описание действий представлено в последующих разделах. Тема управления рисками, которые связаны с безопасностью, очень тщательно рассмотрена в руководстве Майкрософт по управлению рисками в области безопасности: http://www.microsoft.com/technet/security/guidance/default.mspx (на английском языке)

Процесс 1. Учреждение управления ИТ

Управление описывает ответственность, процессы и структуру руководства и принятия решений, которые определяют, как организация ведет свою деятельность. Управление идет сверху, но требует участия на каждом уровне организации. Природа принимаемых решений и информация, которая передается другим участникам процесса GRC, представлены на рис. 3. Как видно из него, каждый член организации имеет возможность внести свой вклад в успешное управление.

Если взглянуть на разные группы, которые передают информацию в организации, то становится понятна полезность общей системы обмена данными GRC. SMF-функция GRC занимается механизмами объединения этих уровней путем управления рисками и контроля, что приводит к повышению качества принимаемых решений и установлению ответственности за результаты.

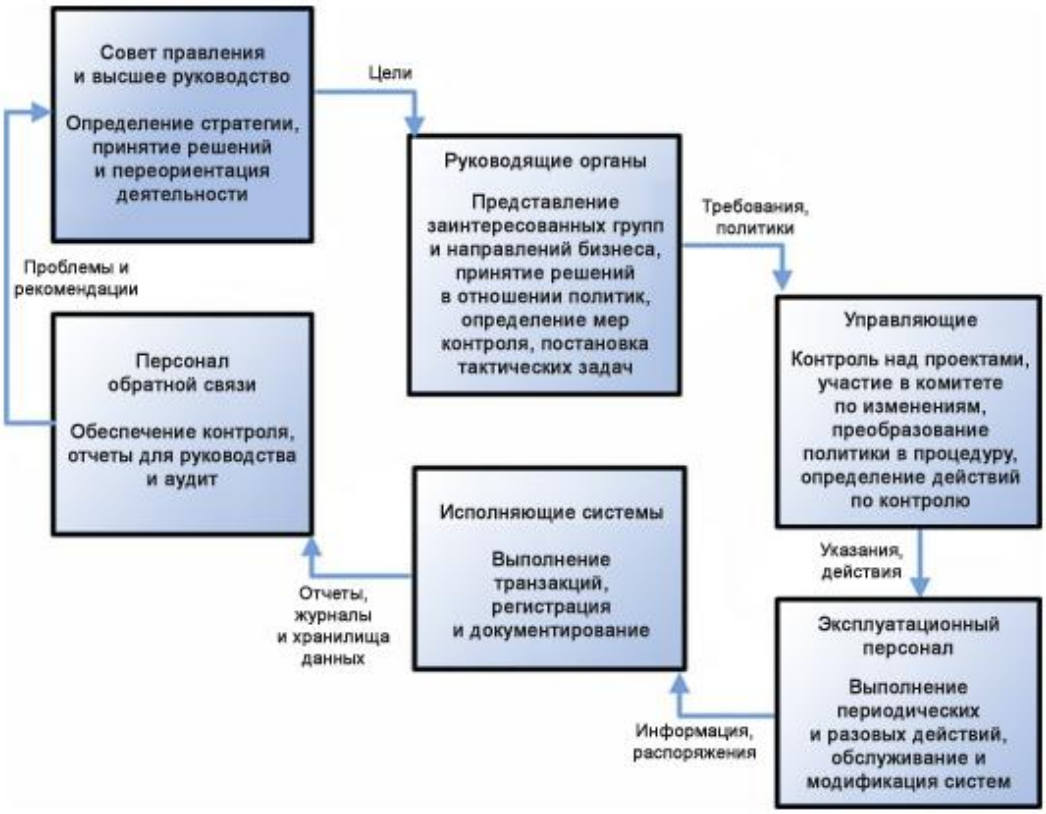

Рис. 3. Среда управления: участники и типы данных

Управление ИТ можно улучшить путем разъяснения целей, ролей и обязанностей, а также управления рисками на всех этапах жизненного цикла ИТ-услуги. Это позволяет ИТ-подразделению понимать бизнес-стратегию и требования, приносить пользу бизнесу, нейтрализуя риски, и определять сферы ответственности на каждом этапе жизненного цикла.

В повседневной деятельности конкретизация концепций происходит по ролям и выполняемым действиям. Например, ИТ-специалисту, который настраивает почтовые ящики Microsoft® Exchange Server, необходимо знать политики хранения и удаления электронной почты и обеспечить их эффективное применение через правила конфигурации и групповую политику. ИТ-менеджер должен иметь представление о целях руководства в отношении обмена корпоративной информацией и применимых нормативных требованиях, которые обеспечивают учет соответствующих юридических соображений при разработке политик.

ИТ-директору и другим руководителям высшего звена необходима уверенность в том, что стратегия организации и все нормы, регулирующие обмен корпоративной информацией, рациональны, а организации предоставлены надлежащие указания и политики.

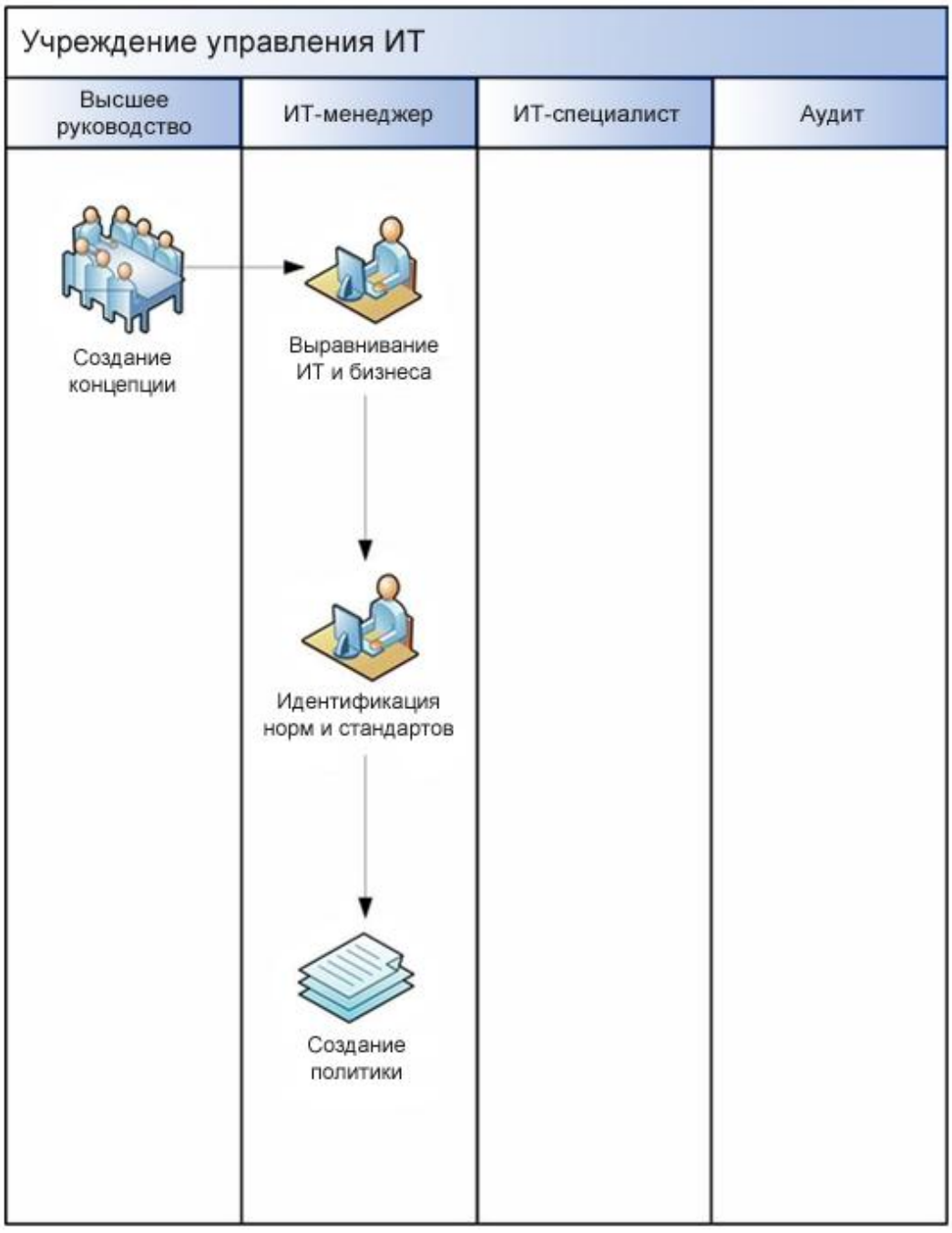

Рис. 4. Учреждение управления ИТ

Действия: учреждение управления ИТ

На практическом уровне процессы управления ИТ помогают согласовать ИТ с бизнесом через механизм принятия решений, позволяющий определять действия для достижения стратегических целей. Согласование происходит в ходе обсуждения компромиссов и принятия решения. Как упоминалось ранее, управление — это процесс, определяющий права на принятие решений, обеспечивающий учет допустимых рисков в принимаемых решениях и позволяющий формировать ожидания, которые можно оценить в процессе соблюдения нормативных требований. Сформировать структуру и процессы управления нужно до того, как возникнет необходимость принимать решения. Это помогает определить представителей бизнес- и ИТ-подразделений, которые будут совместно принимать решения и нести ответственность. Результаты управленческой деятельности влияют на выбор инициатив и технологий и обеспечивают контекст, в котором сотрудники (наиболее ценный ИТ-ресурс) реализуют возможности и преимущества.

Учреждение управления ИТ включает в себя следующие действия.

- **Создание концепции.** Создание концепции — не простая формальность. Это действие определяет общую структуру управления ИТ, а также права на принятие решений и соответствующие сферы ответственности. На стиль деятельности ИТ-подразделения значительное влияние оказывает подход к управлению и его практическое воплощение.
- **Выравнивание ИТ и бизнеса.** Это действие также определяет, насколько скоординированы управление организацией в целом и управление ИТ. Отсутствие такой координации приведет к ухудшению качества управления ИТ.
- **Идентификация норм и стандартов.** Отраслевые нормативные требования и стандарты играют ключевую роль в определении точности и строгости управления ИТ. Эти факторы следует изучать и применять надлежащим образом.
- **Создание политики.** Наличие правильной политики помогает выйти на производительность, которая обеспечивает желаемые результаты при условии ожидаемого поведения и надлежащего использования ресурсов.

Таблица 5. Действия и основные аспекты учреждения управления ИТ

Действия	Аспекты
Допущения	• На организацию распространяется действие нормативных и других внешних требований в отношении управления • Руководству требуется четкое понимание методов работы ИТ-подразделения • Бизнес-руководству необходимо знать вклад ИТ в результаты коммерческой деятельности
Создание концепции	**Основные вопросы** • Каковы главные стратегические цели бизнеса? • Какой уровень формальности необходим, чтобы выполнить требования функции GRC? • Как измеряется реализация ценности ИТ? • Как должна измеряться производительность ИТ? **Входные данные** • Четко заданные стратегические бизнес-цели • Релевантные требования применимых стандартов и нормативных актов • История соблюдения (или несоблюдения) нормативных требований организацией • Допустимые риски для организации • Рекомендации внутреннего аудита по поводу управления • Установленный подход к измерению реализованной ценности • Заданные индикаторы производительности **Конечные результаты** • Структура заседаний для выполнения управленческих действий • Политики управления и планы коммуникации • Общий план управления ИТ-рисками • Ответственность за управленческие решения • Мониторинг и показатели производительности • Требования в отношении реализации ценности • Устав управления ИТ и его владелец **Рекомендации** • Чтобы цели и последствия были понятны, требуется хорошая коммуникация. Предусмотрите достаточно возможностей задавать, переформулировать и перефразировать вопросы. • По возможности сопоставляйте действия по управлению ИТ существующим бизнес-процессам (определение стратегии, планирование и принятие решений). • Информационная архитектура должна быть такой, чтобы при мониторинге производительности и соблюдения нормативных требований по возможности использовались одни и те же данные.

Действия	Аспекты
	• Дополнительные сведения об определении концепции и выравнивании стратегии см. в документе *SMF-функция «Выравнивание бизнеса и ИТ»*.
Выравнивание ИТ и бизнеса	**Основные вопросы** • Участие каких заинтересованных сторон необходимо для принятия компромиссных решений? • Какие процессы классификации и принятия решений используются бизнес-руководством для определения общих инициатив и проектов? • Как организация относится к риску? Каков подход к соблюдению директив? **Входные данные** • Бизнес-цели, директивы руководства и идентифицированные владельцы • Интерпретация нормативных требований юридическим отделом • Понятные бизнесу и ИТ нормативные требования **Конечные результаты** • Установленные участники разных управленческих заседаний (например, руководящих комитетов) • Координация планирования между бизнесом и ИТ • Факторы, которые необходимо учесть при стратегическом планировании ИТ • Четкое понимание бизнесом и ИТ своих ролей и обязанностей **Рекомендации** • Чтобы предотвратить конфликты, создайте четкий процесс, в рамках которого заинтересованные стороны могли бы искать компромиссы и согласовывать пути эскалации проблем. • Выравнивание бизнеса и ИТ может происходить на разных уровнях организации; предусмотрите заседания для обсуждения на разных уровнях. • Дополнительные сведения об определении концепции и выравнивании стратегии см. в документе *SMF-функция «Выравнивание бизнеса и ИТ»*.
Идентификация норм и стандартов	**Основные вопросы** • Какими отраслевыми стандартами или нормативными требованиями регулируется деятельность организации? • Можно ли выделить общепринятую модель (например, COBIT или ISO 20000), которая хорошо подходит организации с точки зрения отраслевой и внутренней культуры соблюдения требований? **Входные данные** • Внутреннее представление применимых нормативных требований • Сделанный ИТ-подразделением анализ моделей управления ИТ-услугами • Возможности и ограничения ИТ (навыки и технологии)

Действия	Аспекты
	Конечные результаты • Модель управления, которая обеспечивает минимальную организационную нагрузку, позволяющую достичь максимальных преимуществ с точки зрения эффективности, производительности и согласованности с бизнесом **Рекомендации** • Каждая модель — это лишь отправная точка. Она содержит общие концепции, которые необходимо переработать и подогнать к особенностям реальной организации. • Чтобы адаптировать модель к уникальным особенностям своей компании, требуется глубокое понимание отраслевых и внутренних корпоративных факторов. • Учитывайте имеющиеся у ИТ-специалистов технические знания при применении выбранной модели. Это обеспечивает достижимость целей и условия для поддержки.
Создание политики	**Основные вопросы** • Для каких сфер компания хочет четко задать желаемый образ действия? • Каким процессам требуются показатели производительности, установленные в политике? • Каково мнение представителя юридического отдела о предлагаемой политике? **Входные данные** • Случаи несоблюдения или нарушения нормативных требований, когда компания не выполнила необходимые действия • Цели высшего руководства в отношении корпоративного поведения с четко сформулированными последствиями **Конечные результаты** • Документированная и опубликованная политика • Сопоставление требований политики мерам контроля • Примененная на практике политика **Рекомендации** • Дополнительные сведения о создании и использовании политик см. в документе *SMF-функция «Политика»*. • Аудит предоставляет подкрепленную свидетельствами оценку и рекомендации по поводу ввода политики в действие и требуемой среды контроля.

Процесс 2. Оценка, мониторинг и контроль рисков

Управляя рисками, ИТ-подразделение стремится нейтрализовать их и при этом достичь целей управления. Долгосрочный успех в управлении рисками достигается за счет эффективного использования внутренних мер контроля.

Внутренние меры контроля — это конкретные действия, которые выполняют люди или системы, чтобы убедиться в достижении бизнес-целей. Требуется обеспечить тщательное проектирование, документирование и эксплуатацию мер контроля на каждом уровне организации. Наличие мер контроля означает, что вероятность отрицательного воздействия нежелательных событий приемлемо низка, а шансы достижения целей достаточно высоки. Внутренние меры контроля тесно связаны с управленческой деятельностью и напрямую зависят от нее.

На рис. 5 представлены действия по управлению рисками. Важно понимать, что в процессе управления каждым риском все эти действия выполняются минимум один раз, а в ряде случаев количество циклов может быть намного больше. Поскольку каждый риск имеет свои временные рамки, в любой момент времени на отдельном этапе может существовать несколько рисков.

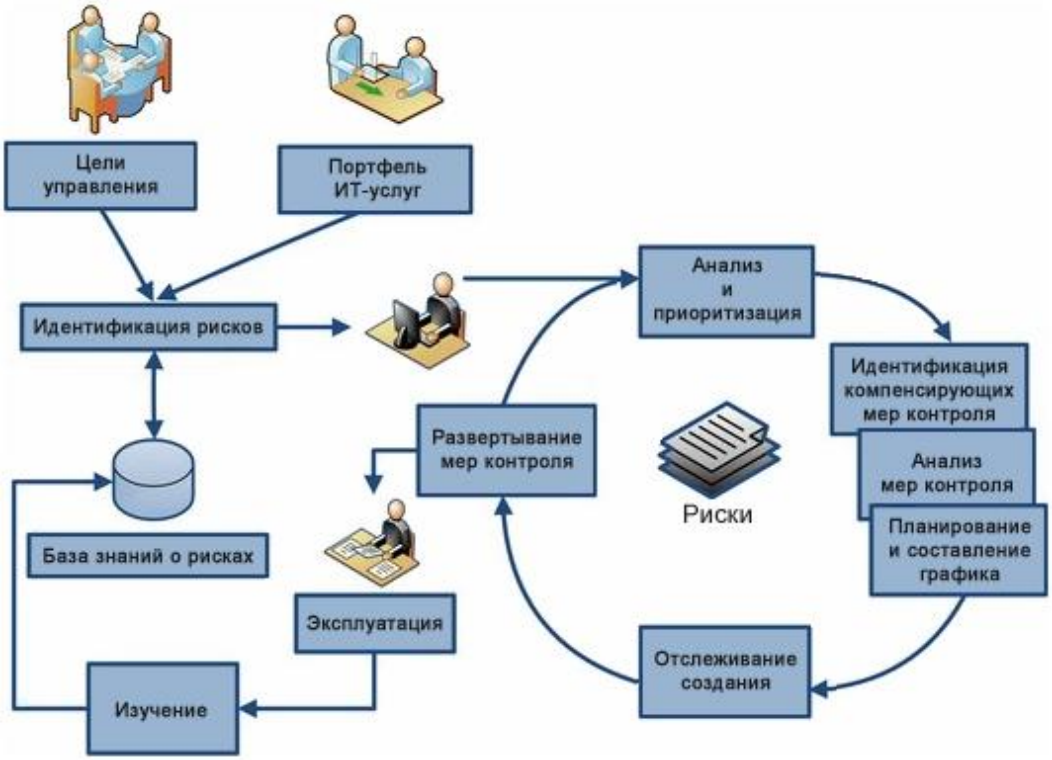

Рис. 5. Обобщенный цикл оценки, мониторинга и контроля рисков

Действия: оценка, мониторинг и контроль рисков

Процесс идентификации рисков и мер контроля затрагивает все компоненты компании. Он обеспечивает основу для корпоративных усилий по соблюдению нормативных требований, четко определяя взаимосвязи между целями, возможными препятствиями на пути их достижения и способами воздействия на эти препятствия.

Каждому этапу жизненного цикла ИТ-услуги соответствует набор типовых рисков и действий по управлению ими.

- На этапе «Планирование» в центре внимания находятся риски, связанные с конкретными стратегиями и информационными архитектурами, а также риски в портфеле ИТ-услуг.
- На этапе «Внедрение» риски оцениваются с точки зрения проектов, т. е. более целенаправленно и ограниченно по времени.
- Этап «Эксплуатация» сосредоточен на текущей деятельности и рисках, которые могут повлиять на надежность эксплуатации.
- В завершение на уровне «Управление» выполняется как общее, так и специализированное управление рисками: общее — в части структуры управления, организационной координации, принятия решений и планов коммуникации; специализированное — в части управления изменениями, конфигурациями и рисками, возникающими при изменении элементов среды ИТ-услуг, а также процессов и ресурсов, являющихся частью этой среды).

На каждом этапе жизненного цикла ИТ-услуги присутствуют разные категории рисков. В их числе риски, связанные с финансами, эксплуатацией, репутацией, рыночной долей, доходом и нормативными требованиями, а также риски, обусловленные отраслевой принадлежностью организации (например, здравоохранение) или происходящими в данный момент событиями (например, слияние или поглощение).

Правильное управление рисками, которое заставляет думать о возможных последствиях действий, оценивать их влияние, а затем использовать очень четкий подход к нейтрализации связанных с ними рисков, дает ИТ-подразделению значительные преимущества. Организация не сможет разумно противостоять рискам, если ИТ и бизнес совместно не определят допустимость рисков и меры их контроля. Поскольку последствия рисков оцениваются с точки зрения достижения бизнес-целей, это позволяет ИТ и бизнесу совместно обсуждать риски и принимать компромиссные решения, а также избежать перекладывания вины за ошибки друг на друга благодаря прозрачности процесса управления рисками.

Этот процесс включает в себя следующие действия:

- Усовершенствование процессов с учетом целей управления
- Идентификация рисков
- Анализ и приоритизация рисков
- Идентификация мер контроля
- Анализ мер контроля
- Планирование и составление графика внедрения
- Отслеживание рисков и мер контроля и составление отчетов по ним
- Использование мер контроля
- Изучение предшествующего опыта и обновление базы знаний

Таблица 6. Действия и основные аспекты оценки, мониторинга и контроля рисков

Действия	Аспекты
Допущения	• Управление рисками выходит за рамки защиты и обеспечения конфиденциальности данных, охватывая множество рисков, способных повлиять на достижение целей управления (в т. ч. финансовый риск, риск низкой производительности, проектный риск и риск для репутации).
Учет целей управления	**Основные вопросы** • Какие события могут повлиять на достижение целей управления? • Как можно улучшить способность достигать целей? • В каких бизнес-процессах, чувствительных к рискам, используются ИТ-системы? • Какой профиль допустимых рисков лучше всего подходит для описания компании? **Входные данные** • Стратегический план и определенные на его основе цели управления (см. документ *SMF-функция «Выравнивание бизнеса и ИТ»*) • Законодательно-правовые и коммерческие условия • Результаты управления рисками (успех, неудача) на текущий момент **Конечный результат** • Допустимые риски и подход организации к управлению рисками **Рекомендации** • Управление рисками происходит многократно на каждом этапе жизненного цикла ИТ-услуги. Понимание рисков, связанных с целями конкретного этапа, позволит определить область их действия. • Область действия рисков, а также их допустимость для компании позволят определить подход к управлению рисками на каждом этапе жизненного цикла ИТ-услуги. • Допустимость рисков — величина переменная, она меняется в зависимости от возможностей и потенциальных выгод, а также инцидентов и потенциальных наказаний.
Идентификация рисков	**Основные вопросы** • Какова классификация бизнес-услуг с точки зрения их важности для бизнеса и характера используемых в них данных? • Какова история изменения систем, составляющих каждую услугу? Какие изменения запланированы на будущее? • В чем заключается сложность полной системы (она имеет несколько интерфейсов, расширяется в системы деловых партнеров, зависит от неподконтрольных компании данных и услуг)? **Входные данные** • Миссия компании (и при необходимости миссии бизнес-подразделений) • Допустимые риски и подход к управлению рисками

Действия	Аспекты
	• Портфель ИТ-услуг (см. документ *SMF-функция «Выравнивание бизнеса и ИТ»*) • Карты ИТ-услуг (см. документ *SMF-функция «Выравнивание бизнеса и ИТ»*) • Отчеты об инцидентах и события безопасности • Нормативно-правовая среда и случаи несоблюдения нормативных требований **Конечный результат** • Отчет о рисках, связанных с ИТ-услугами **Рекомендации** • Высшее руководство должно поддерживать процесс управления рисками. • Следите, чтобы участники процесса управления рисками знали ИТ-системы и бизнес-процессы, а также осознавали их потенциальное воздействие на бизнес. • Проанализируйте критичные для бизнеса услуги, оцените стандартные риски по каждой из них, методом мозгового штурма определите возможные риски. Привлекайте к участию людей с разными точками зрения и специализациями. • Идентификация рисков включает в себя оповещение заинтересованных сторон. Производить идентификацию рисков необходимо часто. • Дополнительные сведения об идентификации рисков см. в документе NIST SP 800-30 по адресу http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (на английском языке).
Анализ и приоритизация рисков	**Основные вопросы** • Какое влияние риски и угрозы (ситуации и состояния, способные нанести вред) оказывают на организацию в целом? • Каково вероятное воздействие угроз на конкретные цели управления и соответствующие бизнес-процессы? • Можно ли в числе этих угроз и воздействий выделить те, которые снижают производительность ИТ-услуг, но не нарушают конфиденциальность данных? • Какие уязвимости имеются в системах, из которых состоят ИТ-услуги? • Каким угрозам подвержены индивидуальные системы? **Входные данные** • Риски предоставления ИТ-услуг • Угрозы • Уязвимости **Конечный результат** • Списки угроз и уязвимостей с указанием приоритета рисков **Рекомендации** • Преобразуйте оценки и данные, собранные в процессе идентификации рисков, в формат, позволяющий использовать их для приоритизации. • Оценивайте риски с точки зрения *вероятности, помноженной на воздействие*, и используйте полученную оценку для приоритизации.

Действия	Аспекты
	• Назначайте приоритеты таким образом, чтобы наиболее важным рискам выделялось достаточно ресурсов. • Методом мозгового штурма постарайтесь идентифицировать возможные, но пока не предвиденные риски. Оцените потенциальное воздействие (даже если вероятность возникновения низка) и решите, заслуживают ли они внимания. • См. ресурсы, посвященные нейтрализации угроз и уязвимостей, на веб-странице http://www.microsoft.com/technet/security/learning/threats/all/default.mspx (на английском языке).
Поиск мер контроля	**Основные вопросы** • Каковы наиболее подходящие для нейтрализации рисков контрольные точки и действия, определяемые на основе угроз и уязвимостей? • Какие уязвимости (конфиденциальность, целостность и доступ к данным) охвачены четкими мерами контроля? **Входные данные** • Списки угроз и уязвимостей с их приоритетами • Перечень основных и компенсирующих мер контроля (обычно служат для выявления проблем постфактум) • Интервью с сотрудниками, которые отвечают за бизнес-цели и соответствующие процессы • Интервью со специалистами по отдельным зонам контроля ИТ • Проблемы и аудиторские отчеты **Конечный результат** • Схема сопоставления мер контроля ИТ-услугам и бизнес-процессам **Рекомендации** • Меры контроля взаимодействуют, создавая среду контроля. При оценке меры контроля учитывайте ее связь с другими мерами и проанализируйте, как одна мера контроля может компенсировать другую.
Анализ мер контроля	**Основные вопросы** • Каким бизнес-целям соответствуют установленные меры контроля? • Какие имеются свидетельства того, что меры контроля функционируют надлежащим образом? • Какие требования предъявляются аудитом в отношении свидетельств и их хранения? **Входные данные** • Аудиторские отчеты • Список существующих мер контроля • Интервью со специалистами в каждой зоне контроля • Схема сопоставления мер контроля ИТ-услугам и бизнес-процессам **Конечный результат** • План разработки мер контроля

Действия	Аспекты
	Рекомендации • Аудиторский отчет содержит независимый анализ мер контроля и, обычно, рекомендации по усовершенствованию среды контроля. • Сосредотачивайте внимание на фундаментальных мерах контроля, которые должны правильно функционировать, поскольку от них зависят другие меры (например, контроль доступа к данным). • Разрабатывайте меры контроля со встроенными процессами сбора свидетельств, чтобы повысить эффективность и продуктивность аудита и других процедур тестирования мер контроля. Тестирование предполагает поиск свидетельств того, что мера контроля существует и функционирует надлежащим образом.
Планирование и составление графика внедрения	**Основные вопросы** • Какие из предусмотренных мер контроля еще не внедрены? • Какова очередность разработки мер контроля, которые еще не внедрены? **Входные данные** • Списки угроз и уязвимостей с приоритетами рисков • План разработки мер контроля **Конечные результаты** • План разработки мер контроля и управления рисками • Идентифицированные способы нейтрализации • График запросов на изменение, связанных с мерами контроля **Рекомендации** • Используйте при формулировании стратегий, планов, запросов на изменение и действий информацию, собранную в ходе анализа рисков. • Используйте процессы управления изменениями, чтобы гарантировать утверждение планов управления рисками и их включение в стандартные повседневные процессы и инфраструктуру. См. документ *SMF-функция «Изменение и конфигурация»*.
Отслеживание создания; развертывание мер контроля	**Основные вопросы** • Каков статус рисков и мер контроля? **Входные данные** • Мониторинг ИТ-услуг • Свидетельства, полученные в ходе контроля • Отчеты о состоянии проектов разработки мер контроля **Конечные результаты** • Отчеты о рисках • Отчеты о состоянии разработки мер контроля

Действия	Аспекты
	Рекомендации • Отслеживайте статус отдельных рисков и его изменение в соответствующих планах действий. • Отслеживайте вероятность, воздействие, подверженность и другие параметры риска для изменений, которые могут изменить приоритет или планы управления рисками и, в результате, доступность связанной с ними ИТ-услуги. • Эксплуатационный персонал, менеджер по обслуживанию и другие заинтересованные стороны должны знать о статусе основных рисков и планах по управлению ими.
Использование мер контроля	**Основные вопросы** • Меры контроля функционируют надлежащим образом? • Уровни допустимых рисков и триггеры действий функционируют надлежащим образом? • Планы управления рисками отслеживаются надлежащим образом? **Входные данные** • Отчеты о рисках • Отчеты о состоянии разработки мер контроля • Отчеты о соблюдении требований соглашений SLA **Конечные результаты** • Отчеты об использовании мер контроля • Воздействие на уровень ИТ-услуг **Рекомендации** • Выполняйте планы управления рисками, оценивая их статус с помощью отчетов о рисках. • Инициируйте запросы на изменение мер контроля, если изменение статуса рисков или планов управления рисками может повлиять на доступность ИТ-услуги или на выполнение условий соглашения SLA. • Собирайте и храните свидетельства того, что меры контроля функционируют. В качестве свидетельств могут выступать, например, системные журналы, документы, для которых действует контроль изменений, или документы, подписанные уполномоченными лицами. • Оповещайте заинтересованные стороны об изменении ИТ-услуг с целью нейтрализации рисков.
Изучение предшествующего опыта и обновление базы знаний	**Основные вопросы** • Довольно ли руководство тем, как меры контроля справляются с известными рисками? • Правильно ли установлены уровни допустимых рисков? Инициируются ли соответствующие действия, когда происходит превышение допустимых уровней? • Удалось ли идентифицировать новые риски? • Подтверждают ли результаты аудита эффективность среды контроля?

Действия	Аспекты
	Входные данные • Аудит в ходе обычной эксплуатации • Отчеты об эксплуатации мер контроля • Анализ затрат и результатов по мерам контроля **Конечные результаты** • Отчеты о рисках, составляемые не реже одного раза в месяц • Панель мониторинга рисков (при наличии) • Актуальная база знаний о рисках • Результаты, предназначенные для управленческого анализа «Эксплуатационное состояние» **Рекомендации** • Меры контроля применяются на основе анализа затрат и результатов, который должен отражать представление руководства о бизнес-цели, выявленном риске и преимуществах разработки и применения меры контроля. Анализ затрат и результатов должен отражать готовность компании принять на себя риск, признавая его существование и допуская возможное воздействие (в противоположность нейтрализации риска, которая подразумевает снижение уровня воздействия или вероятности возникновения риска). • В ходе изучения риска происходит формализация имеющихся знаний и применяются средства для регистрации, классификации и индексирования этих знаний в формате для многократного совместного использования сотрудниками организации.

Процесс 3. Соблюдение директив

Соблюдение нормативных требований — это применение управления рисками с целью обеспечить соответствие ИТ политикам компании, правительственным регулятивным актам и специфичным для отрасли законам. В следующей таблице перечислены наиболее известные из этих законов и их назначение.

Таблица 7. Некоторые законы и их назначение

Закон	Назначение
Закон Сарбейнса — Оксли (SOX)	Усовершенствованные стандарты и меры контроля для советов правления открытых акционерных обществ и независимых бухгалтерских компаний США.
Акт HIPAA	Национальные стандарты для электронных транзакций в сфере здравоохранения.
Второе базельское соглашение	Международные стандарты для банков.

Соблюдение требований требует большого усердия и ответственности со стороны ИТ-специалистов. Например, многие крупные корпорации автоматизировали свои системы управления финансами, что привело к автоматизации внутренних мер контроля. Эти *прикладные меры контроля* являются частью среды соблюдения требований, но в случае автоматизации становятся частью ИТ-среды. Кроме того, ИТ-специалистам необходимо помнить об *общих компьютерных мерах контроля* (например, отделение среды разработки от среды тестирования), т. е. процессах, действиях и конфигурациях, которые применяются ко многим компонентам инфраструктуры и обеспечивают надлежащее функционирование технологий.

Свидетельства и аудиторская отчетность

Аудит — это процесс предоставления высшему руководству информации о том, насколько хорошо организации удается достигать поставленных целей управления. Аудиторская отчетность составляется отделом аудита, который выполняет непредвзятую оценку. Эти отчеты основываются на данных, демонстрирующих вклад применяемых мер контроля в надлежащее достижение результатов. Такие данные называются свидетельствами, а тестирование — это процесс испытания мер контроля с целью получения свидетельств. Кроме того, речь может идти об оценке полученных свидетельств.

Это может сбить с толку ИТ-специалиста, который привык называть тестированием процессы контроля качества, используемые при разработке ПО и развертывании систем. Сохранение конкретных данных, используемых для тестирования (получения свидетельств), не является привычной ИТ-специалисту методикой тестирования. С другой стороны, чтобы иметь возможность составить мнение об эффективности и целесообразности мер контроля, аудиторам требуются свидетельства за достаточно длительный период времени. Кроме того, разница между аудиторским тестированием и привычным ИТ-специалисту тестированием обычно заключается в том, что аудиторское тестирование обычно выполняется для мер контроля и процессов в рабочей среде. При этом проверке подвергается реальная деятельность организации, а не изолированная среда тестирования, в которой функциональные проблемы можно отделить и разрешить.

Аудиторские отчеты могут быть получены из нескольких источников (аудит соблюдения требований, аудит системы безопасности, аудит выполнения договорных обязательств и т. п.), из-за чего у ИТ-специалистов иногда по несколько раз запрашивают похожие свидетельства. ИТ-специалисты смогут повысить результативность процесса аудита и сократить создаваемые им помехи, если они будут осведомлены об аудиторской деятельности в организации, усвоят требования в отношении хранения свидетельств и поймут способы использования последних.

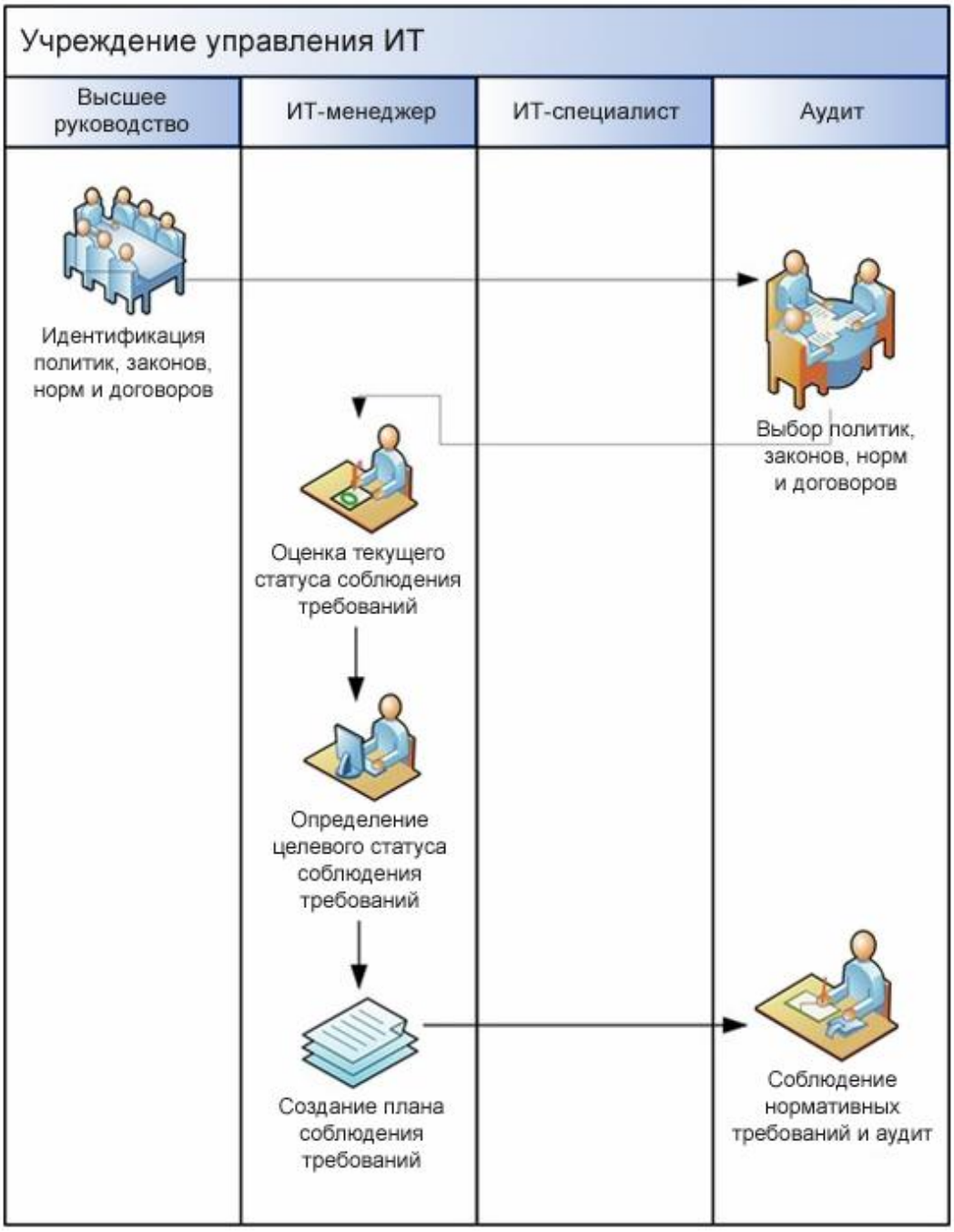

Рис. 6. Соблюдение директив

Действия: соблюдение директив

Процесс соблюдения нормативных требований является итеративным; ИТ-подразделение обязано вести непрерывный мониторинг среды, адаптировать ее к меняющимся нормативным требованиям и реагировать на директивы руководства. ИТ-специалистам необходимо сверяться с политикой компании, а не заниматься интерпретацией нормативных требований без учета мнения других подразделений. Нормативные требования должны проходить оценку в разных подразделениях (юридический отдел, отдел кадров, финансовая служба и пр.), которые определяют позицию компании по отношению к каждому требованию в отдельности.

ИТ-специалисты обязаны обращать внимание бизнес-подразделений на нормативные требования, которые касаются ИТ. Затем требования оцениваются, определяется позиция компании и создаются необходимые политики и директивы, регулирующие принятие решений и другие виды деятельности. Когда направление задано, аудитор может взять цели управления (в форме директив) и проверить их соблюдение.

В этот процесс включены следующие действия:

- Идентификация политик, законов, норм и договоров
- Выбор политик, законов, норм и договоров
- Оценка текущего статуса соблюдения требований
- Определение целевого статуса соблюдения требований
- Создание плана соблюдения требований
- Соблюдение нормативных требований
- Аудит соответствия нормативным требованиям

Таблица 8. Действия и главные аспекты соблюдения директив

Действия	Аспекты
Допущения	• Организация стремится обеспечить соблюдение директив независимо от того, распространяются ли на них формальные требования в отношении управления. • ИТ-подразделение может владеть услугами, для которых предусмотрены конкретные уровни производительности и наказания за их несоблюдение. • В прошлом результаты аудита показали, что среда контроля неэффективна или нерациональна либо имело место несоблюдение компанией нормативных требований.
Идентификация политик, законов, норм и договоров	**Основные вопросы** • Какие законы и нормативные требования (местные, национальные или международные) применяются в отношении компании? • Какие органы могут регулировать деятельность компании? • Какие цели требуют, чтобы политика отражала намерения руководства и обеспечивала выполнение желаемых действий? • Каковы обязательства ИТ-услуги в отношении соблюдения нормативных требований? **Входные данные** • Международные, национальные и местные законы и требования • Требования правительственных органов • Директивы руководства • Анализ соблюдения требований, выполненный юридическим отделом • Требования к производительности, заданные в соглашениях об уровне обслуживания **Конечные результаты** • Законы и требования, а также внутренние директивы, которые необходимо соблюдать • Подлежащие соблюдению директивы, которые направлены на выполнение стратегических планов компании **Рекомендации** • Соблюдение требований имеет много аспектов, но в основном речь идет о целях управления, директивах компании и законодательных требо-ваниях. Кроме того, услуги должны функционировать в соответствии с соглашениями и договорами. Данные для обеих сфер соблюдения требований могут обеспечить мониторинг и системы показателей.

Действия	Аспекты
Выбор политик, законов, норм и договоров	**Основные вопросы** • Занималась ли компания оценкой того, какими законами и нормами регулируется ее деятельность? • Располагает ли компания эффективной моделью управления такими законами и нормами? **Входные данные** • Проверенный список законов и норм, а также их интерпретация • Допустимые риски • Прошлые аудиторские отчеты • Возможные меры контроля, предусмотренные соответствующими моделями, **Конечный результат** • Перечень законов, норм, мер контроля и уровней производительности, которые должны быть учтены в политике компании **Рекомендации** • Корпоративная культура и применяемые способы достижения стратегических целей оказывают значительное влияние на соблюдение требований. Чтобы согласовать культуру и соблюдение требований, решения должны приниматься открыто, с привлечением соответствующих заинтересованных сторон. • Участниками обсуждения должны быть представители юридического отдела и специалисты по аудиту.
Оценка текущего статуса соблюдения требований	**Основные вопросы** • Как обстоят дела с соблюдением применимых законов, норм и директив? • Как обстоят дела с соблюдением уровней производительности? • Были ли случаи несоблюдения нормативных требований и какова тенденция соблюдения? **Входные данные** • Оценка рисков для систем и бизнес-процессов (см. раздел «Процесс 2. Оценка, мониторинг и контроль рисков»). • Существующие политики и директивы • Отчеты о соблюдении требований, свидетельская активность • Соблюдение показателей производительности, установленных в соглашениях SLA **Конечный результат** • Состояние дел с соблюдением требований (отчет или панель мониторинга)

Действия	Аспекты
	Рекомендации • Статус соблюдения требований может быть непостоянным. Чтобы уменьшить непостоянство, жесткая программа соблюдения требований должна предусматривать активный мониторинг мер контроля и выявление тенденций. Панель мониторинга, регулярно обновляемая с учетом последних данных, позволит высшему руководству оставаться в курсе дела, не перегружая себя подробными отчетами о соблюдении требований. На панели мониторинга следует предусмотреть возможность более подробного изучения случаев несоблюдения требований.
Определение целевого статуса соблюдения требований	**Основные вопросы** • В каких областях наблюдаются повторяющиеся случаи несоблюдения требований? • Какие риски несоблюдения требований для компании недопустимы? • Применялось ли наказание за несоблюдение требуемого уровня производительности ИТ-услуг? **Входные данные** • Текущий статус соблюдения требований • Изменения в каталоге и портфеле ИТ-услуг • Изменения в нормативно-правовой среде, в которой функционирует бизнес • Правовые тенденции и решения, которые могут повлиять на бизнес • Изменение допустимых границ риска • Возможное изменение, сужение или расширение среды контроля **Конечный результат** • Документированная программа соблюдения требований, позволяющая достичь целевого статуса **Рекомендации** • Несоблюдение требований нужно рассматривать с нескольких точек зрения. Возможно ли, что применяются неподходящие или запутанные процедуры и инструкции? Возможно ли, что политика слишком строга или громоздка, что ведет к конфликту между производительностью и соблюдением требований? Прошли ли сотрудники надлежащее обучение? • Посоветуйтесь с юристом перед созданием заключительной версии политики, которая учитывает требования. Важно иметь независимое мнение по поводу того, как компании следует соблюдать требования. Для этого необходимо знать существующие юридические прецеденты и понимать уровень развитости требований.

Действия	Аспекты
Создание плана соблюдения требований	**Основные вопросы** • Каким образом компания, соблюдающая нормативные требования (целевой статус), будет отличаться от сегодняшней компании? • Какие элементы текущей программы соблюдения требований функционируют неэффективно? • Какие ресурсы, обучение, а также изменения в политиках, процессах и системах потребуются для обеспечения соответствия требованиям? • Нужно ли изменять договоры о предоставлении ИТ-услуг с установленными уровнями производительности? **Входные данные** • Документированная программа соблюдения требований, позволяющая достичь целевого статуса • Анализ целевого статуса, стратегических и бизнес-целей, выполненный высшим руководством • Соглашение, подтверждающее, что намеченный целевой статус компании совместим со стратегическими целями • Планы проектов по изменению ИТ-услуг, для которых необходимо обеспечить соблюдение заданных уровней производительности **Конечный результат** • Рекомендованный план соблюдения требований, утвержденный всеми заинтересованными сторонами **Рекомендации** • Обращайте внимание на культуру соблюдения требований. Если компания принадлежит к отрасли, которая жестко регулируется извне, то, скорее всего, соблюдение требований является неотъемлемой частью повседневной деятельности. Если же отрасль относится к числу динамично растущих и развивающихся, то соблюдение требований может считаться бременем, которого следует избегать. Планы соблюдения требований должны учитывать этот момент и содействовать трансформации культуры в нужном направлении.
Соблюдение нормативных требований	**Основные вопросы** • Какие случаи несоблюдения требований все еще наблюдаются? • Можно ли снизить затраты на соблюдение требований, но так, чтобы не увеличивать риск? **Входные данные** • План соблюдения требований • Управление услугами и контрольная отчетность (см. документ *SMF-функция «Мониторинг и контроль услуг»*) • Аудиторские отчеты, мониторинг мер контроля • Допустимые риски и уровни соблюдения требований

Действия	Аспекты
	Конечные результаты • Отчет о соблюдении требований • Обновляемая панель мониторинга с данными о соблюдении требований **Рекомендации** • Вопросы соблюдения требований часто имеют конфиденциальный характер. Некоторые сотрудники не должны видеть определенные части этой информации. Многоуровневое представление данных и ролевой доступ к отчетам и панелям мониторинга позволяют обеспечить требуемую конфиденциальность. • Среда соблюдения требований весьма динамична и нуждается в регулярных ревизиях мер контроля. Эти ревизии должны включать в себя анализ затрат и результатов с учетом масштабов риска и эксплуатационной эффективности.
Аудит соблюдения нормативных требований	**Основные вопросы** • Меняются ли законы и нормы, применимые к компании? Появляются ли новые законы и нормы? • Приемлем ли текущий статус соблюдения требований для высшего руководства? • Обеспечивается ли обновление и надлежащее хранение достаточного количества свидетельств и выполнение действия по контролю, тестированию и соблюдению нормативных требований? **Входные данные** • Создаваемые и обновляемые юридическим отделом обзоры нормативных требований • Аудит обычной деятельности • Отчеты и брифинги руководителей высшего звена по поводу статуса соблюдения требований **Конечные результаты** • Результаты аудита соблюдения требований • Обновленный план соблюдения требований **Рекомендации** • Несоблюдение нормативных требований может иметь четкие последствия (штрафы и тюремное заключение), но сами требования зачастую сформулированы в общих чертах. Юристы и аудиторы помогут вам выяснить, что нужно сделать, чтобы ИТ-среда соответствовала нормативным требованиям. • Храните для последующей оценки надлежащее и достаточное количество свидетельств мер контроля. За несколько месяцев до планируемого аудита в определенной области обсудите с внешними и внутренними аудиторами требования в отношении сбора и хранения свидетельств. • Использование SLA помогает определить качество ИТ-услуг. Установите уровень производительности и требования по его соблюдению. Дополнительные сведения о SLA см. в документе *SMF-функция «Выравнивание бизнеса и ИТ»*.

Заключение

В рамках SMF-функции «Управление, риск и соответствие нормативным требованиям» (GRC) предоставляются инструкции по интеграции задач GRC в контекст процессов и действий на всех этапах жизненного цикла ИТ-услуги. При этом механизмы управления рисками и меры контроля, присутствующие в каждой SMF-функции, обеспечивают единообразное принятие решений и управление ИТ-операциями.

В составе SMF-функции GRC описаны следующие процессы:

- Учреждение управления ИТ
- Оценка, мониторинг и контроль рисков
- Соблюдение директив.

Обратная связь

Вопросы и комментарии к данному руководству присылайте по адресу rakmeev@microsoft.com или ruslan@akmeev.ru