SOLUTIONACCELERATORS

Действуй быстрее. Достигни большего.

Microsoft® Operations Framework

Версия 4.0

Обзор уровня «Управление»

Опубликовано: апрель 2008 г.

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

Microsoft

Содержание

Общие сведения о MOF

Инструкции в Microsoft® Operations Framework охватывают все действия и процессы управления ИТ-услугами: планирование, разработку, эксплуатацию, обслуживание и, наконец, 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 ИТ-услуги. Каждая SMF-функция относится к определенному этапу жизненного цикла и обладает уникальным набором целей и результатов, соответствующих назначению этого этапа. Готовность ИТ-услуги к переходу на следующий этап определяет управленческий анализ, который проверяет путь достижения целей и их соответствие общим целям организации.

Обзор уровня «Управление»

Как координируется деятельность ИТ-подразделения? От чего зависит выбор методов, используемых ИТ-подразделением? Решение этих задач является основной целью уровня «Управление», объединяющего процессы принятия решений, управления рисками и управления изменениями на всех этапах жизненного цикла ИТ-услуги. Этот уровень обеспечивает согласованное планирование и внедрение ИТ-услуг, создает базу для разработки и эксплуатации устойчивой ИТ-среды и охватывает процессы, связанные с определением ответственности и соответствующих ролей.

Уровень «Управление» является основой для трех этапов жизненного цикла («Планирование», «Внедрение» и «Эксплуатация») и поэтому считается уровнем, а не этапом. Этап состоит из взаимосвязанных процессов и действий, обеспечивающих наибольшую эффективность при их использовании в ограниченный период времени. Уровень менее ограничен временными рамками, включает все этапы и влияет на способы выполнения действий.

Уровень «Управление» устанавливает надлежащий контекст управления, меры контроля, процессы и действия, при которых добавляется коммерческая ценность, управляемость рисками и распределяется ответственность при использовании SMF-функций на различных этапах.

Уровень «Управление» содержит следующие три функции управления ИТ-услугами (SMF-функции): «Изменение и конфигурация», «Управление, риск и соответствие нормативным требованиям» и «Рабочая группа». Дополнительные сведения об этих SMF-функциях см. в разделе «Функции управления ИТ-услугами в составе уровня "Управление"».

Рис. 1. Уровень «Управление»

Цели уровня «Управление»

Основная цель уровня «Управление» — обеспечение интегрированного подхода к управлению ИТ-услугами. Такой подход помогает координировать процессы, описанные в SMF-функциях трех этапов жизненного цикла

Чтобы повысить эффективность координирования, применяются процессы принятия решений. Во всех процессах используются управление рисками и меры контроля, внедряются надлежащим образом управляемые процессы изменения и конфигурации, а выполняемые задания распределяются таким образом, чтобы ответственности за достижение результатов были четко определены и не конфликтовали между собой.

Уровень «Управление» предоставляет рекомендации, повышающие вероятность получения следующих преимуществ.

- Инвестиции в ИТ приводят к созданию ожидаемой ценности.
- Решения о распределении инвестиций и ресурсов принимаются соответствующими людьми.
- Обеспечивается приемлемый уровень риска.
- Используются контролируемые и документированные процессы.
- Известны сферы ответственности и их владельцы.
- Эффективные и надежные политики и внутренние меры контроля.

Достижению этих целей способствуют следующие факторы.

- Четкие структуры и процессы управления ИТ.
- ИТ-отдел и бизнес-подразделения компании используют единый подход к управлению рисками.
- Регулярно проводится управленческий анализ политик и внутренних мер контроля.

Уровень «Управление»

Чтобы помочь ИТ-специалистам в планировании и оптимизации ИТ-стратегии, в модели MOF предусмотрены функции управления ИТ-услугами (SMF-функции), которые предназначены для определения процессов, людских ресурсов и действий и позволяют привести ИТ-услуги в соответствие с потребностями бизнеса. Эти функции определяют и описывают основные действия, выполняемые ИТ-специалистами на разных этапах жизненного цикла ИТ-услуги. Каждую SMF-функцию можно представить в виде автономного набора процессов, однако их взаимодействие обеспечивает наиболее эффективное и полное внедрение услуги с требуемым качеством и уровнем риска.

Функции управления ИТ-услугами в составе уровня «Управление»

Уровень «Управление» является основой всех этапов жизненного цикла и объединяет отдельные действия всех SMF-функций с помощью следующих собственных SMF-функций:

- *SMF-функция «Управление, риск и соответствие нормативным требованиям» (GRC SMF)*
- *SMF-функция «Изменение и конфигурация» (CC SMF)*
- *SMF-функция «Рабочая группа»*

Более подробно эти SMF-функции описаны в следующей таблице.

Таблица 1. SMF-функции уровня «Управление»

SMF-функция	Конечный результат/цель	Результат
Управление, риск и соответствие нормативным требованиям	**Конечный результат:** достигнуты цели ИТ, изменения и риски контролируются и документируются **Цель:** поддержка, укрепление и развитие организации при одновременном управлении рисками и ограничениями	ИТ-услуги соответствуют бизнес-стратегии и целями
Изменение и конфигурация	**Конечный результат:** известные конфигурации и прогнозируемая адаптация **Цель:** изменения планируются, число незапланированных изменений минимально, ИТ-услуги надежны	Прогнозируемые, надежные и заслуживающие доверия ИТ-услуги

SMF-функция	Конечный результат/цель	Результат
Рабочая группа	**Конечный результат:** четкие сферы ответственности, роли и назначение работ **Цель:** динамичные, гибкие и масштабируемые рабочие группы выполняющие запланированные работы	ИТ-решения внедряются с соблюдением установленных ограничений, без незапланированного ухудшения качества услуг и эксплуатируются нужным для бизнеса образом.

Хотя действия «Управление, риск и соответствие нормативным требованиям» и «Изменение и конфигурация» встречаются на протяжении всего жизненного цикла, однако их представление, область действия и цели зависят от конкретного этапа. Например, действия по управлению изменениями на этапах «Планирование» и «Эксплуатация» будут иметь другую значимость и отличаться по составу участников и используемым факторам. Аналогичным образом цели SMF-функции «Управление, риск и соответствие нормативным требованиям» отражают основные цели соответствующего этапа. Это приводит к изменению целей с точки зрения принятия решений, анализа рисков и соответствия нормативным требованиям.

SMF-функции «Изменение и конфигурация» и «Управление, риск и соответствие нормативным требованиям» создают поток процессов с более высоким уровнем унификации на всех этапах жизненного цикла, предоставляя средства принятия решений и выбора компромиссных вариантов и обосновывая стратегию путем управления рисками. Уровень «Управление» является основой жизненного цикла ИТ-услуг и предоставляет ИТ-подразделению структурный и планируемый подход к повышению жизнестойкости и эффективности организации в долгосрочной перспективе.

Роли SMF-функций уровня «Управление» на различных этапах жизненного цикла ИТ-услуги

В следующей таблице перечислены способы, используемые SMF-функциями уровня «Управление» в достижении целей трех других этапов жизненного цикла ИТ-услуги. Более подробное описание роли и ценности SMF-функций уровня «Управление» см. в описаниях этих SMF-функций в разделах, посвященных соответствующим этапам.

Таблица 2. Цели SMFs-функций уровня «Управление» на различных этапах жизненного цикла ИТ-услуги

Этап и его цель	Цель SMF-функции «Управление, риск и соответствие нормативным требованиям»	Цель SMF-функции «Изменение и конфигурация»	Цель SMF-функции «Рабочая группа»
Планирование Обеспечить, чтобы ИТ-услуги, предлагаемые компании, были полезными, прогнозируемыми, надежными, экономически эффективными и отвечали непрерывно меняющимся потребностям бизнеса	• Воплощение корпоративной стратегии в стратегию ИТ • Структура управления, право принятия решений • Высокоуровневые риски • Общая нормативно-правовая среда • Определение политик • Определение инвестиций • Определение целей управления	• Участие выбранных руководителей в оценке изменений • Изменение бизнес-процессов • Изменение архитектуры • Разностороння я оценка изменения (с точки зрения финансирования, портфеля приложений, безопасности и т. д.)	• Вовлечение в работу сотрудников, принимающих решения • Распределение обязанностей по определению допустимых рисков • Экспертный анализ финансовой деятельности • Представление правовых и регулятивных требований
Внедрение Обеспечивает эффективную разработку, успешное развертывание и готовность к эксплуатации услуг, согласованных бизнес- и ИТ-подразделением.	• Поддержка архитектурой решения функциональных и эксплуатационных организационных требований • Определены заинтересованные стороны, методология и риски проекта • Процесс реализации ценности • Жизненный цикл разработки услуги • Смягчение последствий риска • Определены внутренние меры контроля • Определены процедуры	• Границы изменений • Выделение ресурсов • Управление проектом • Финансовое влияние	• Принципы эффективной организации проектных групп • Ответственности и типы ролей • Выравнивание ответственностей • Назначение ролей

Этап и его цель	Цель SMF-функции «Управление, риск и соответствие нормативным требованиям»	Цель SMF-функции «Изменение и конфигурация»	Цель SMF-функции «Рабочая группа»
Эксплуатация Гарантирует, что развернутые ИТ услуги эксплуатируются, обслуживаются и поддерживаются в соответствии с условиями соглашения об уровне обслуживания, одобренными бизнес- и ИТ-подразделениями	• Процедуры и меры контроля • Сохранение информации и документация	• ИТ-среда и конфигурация • Процесс и процедура • Изменение стандартов	• Принципы организации оперативной работы • Принципы организации работ по мониторингу • Принципы организации работ по поддержке

Внутренние меры контроля

Внутренние меры контроля основаны на достаточно простой концепции. Представьте себе, что вы хорошо знаете, как выполнить какое-то простое задание, и можете гарантированно достичь желаемого результата. А теперь представьте, что вам нужно, чтобы это же задание выполнило еще несколько человек. Ваши действия, проверки и соотношение сил, необходимые, чтобы эти люди выполнили поставленную задачу и достигли требуемого результата, и будут являться внутренними мерами контроля для этого задания.

Однако эти начальные меры относятся только к самому заданию. Если в выполнении задания участвует несколько человек, его сложность возрастает. Предположим, что для повышения эффективности задание следует разделить между несколькими людьми, каждый из которых будет выполнять свою часть. В этом случае внутренние меры контроля должны обеспечить надлежащее объединение результатов, полученных разными людьми, и гарантировать, что никому не удалось уклониться от выполнения. В финансовых вопросах проблемы контроля являются еще более важными. Отсутствие эффективного контроля может привести к ошибкам в бухгалтерском учете или даже мошенничеству и хищению. Это происходит, когда добавленные уровни мер контроля, относящиеся к доступу, ролям и разделению обязанностей, становятся частью общей картины.

Внутренние меры контроля представлены во всех областях, с которыми работает ИТ-подразделение. Одни меры контроля предназначены для физической среды, в которой находится инфраструктура центров данных, а другие используются непосредственно для технологий (например, определяют конфигурацию и перечень лиц, которым предоставлен доступ к административным функциям). Некоторые меры контроля используются при доступе к данным и применяются на различных этапах жизненного цикла данных — от шифрования до авторизации, восстановления и защиты данных.

Многие внутренние меры контроля, относящиеся к бизнес-подразделениям, но при этом затрагивающие ИТ-специалистов, используются в бизнес-приложениях, которые являются основой производственных и финансовых систем, а также систем управления персоналом и взаимоотношениями с заказчиками. В этих областях меры контроля должны быть представлены в виде бизнес-требований, определяющих возможности приложений. Кроме упомянутых выше мер контроля, относящихся к бизнес-процессам, ИТ-специалисты должны использовать меры контроля, ориентированные на операционные системы и технологии, формирующие платформу приложений.

Разделение мер ИТ-контроля на общие категории помогает определить характер мер контроля и выбрать подход для мониторинга, тестирования и оценки эффективности проекта, а также эксплуатационной эффективности мер контроля. Более подробно меры контроля описаны в следующей таблице.

Таблица 3. Типы, содержимое и примеры мер контроля

Тип мер контроля	Содержимое	Примеры
Административные	Стандарты, политики, процедуры и вспомогательные меры контроля (такие как программы обучения и информирования)	• **Политика классификации информации** обеспечивает классификацию информации и прав доступа на каждом уровне • **Политика непрерывности бизнеса** гарантирует, что в случае аварийной ситуации или прерывания работы будут учтены все аспекты бизнеса • **Процесс управления изменениями** гарантирует, что все изменения в ИТ-среду будут вноситься надлежащим образом
Технические	Управление доступом, механизмы шифрования и другие технологии, применяемые для защиты логических информационных активов от несанкционированного использования	• Шифрованная файловая система (EFS) • Списки управления доступом (ACL) • Физический доступ к компьютерам через защищенные паролем заставки
Физические	Меры контроля, предназначенные для защиты физических устройств, используемых для хранения и передачи информации	• Защита кабелей компьютера предотвращает несанкционированное изъятие оборудования • Запирание окон и дверей позволяет контролировать физический доступ к устройствам

Тип мер контроля	Содержимое	Примеры
		• Универсальные источники питания позволяют поддержать работоспособность компьютеров в случае прекращения подачи электроэнергии • Для обеспечения непрерывности бизнеса создаются восстанавливаемые на удаленных компьютерах резервные копии операционных систем и данных

Подтверждением того, что ИТ-услуга фактически контролируется на протяжении всего жизненного цикла, является следующее:

- Определение общих целей для каждого этапа жизненного цикла
- Определение рисков, связанных с достижением этих целей
- Определение методов управления рисками в виде мер внутреннего контроля по смягчению последствий рисков

Управленческий анализ для уровня «Управление»

Руководство несет ответственность за выработку целей, оценку хода работ и достижение результатов. В частности, управление включает процессы принятия решений (меры контроля), помогающие руководству выполнять эти требования. Каждый этап жизненного цикла ИТ-услуги содержит одну или несколько процедур управленческого анализа, функционирующих как управленческие меры контроля. Это означает, что нужные люди будут собраны вместе в надлежащее время и обеспечены информацией, необходимой для принятия управленческих решений. Поскольку все этапы имеют собственные управленческие цели, каждому этапу сопоставлены свои процедуры управленческого анализа, соответствующие заинтересованные стороны, требуемые решения и типы данных, необходимые для принятия обоснованных и взвешенных решений. На уровне «Управление», как и на различных этапах жизненного цикла ИТ-услуги, необходимы средства контроля и управления. Для использования на этом уровне был разработан специализированный управленческий анализ.

Управленческий анализ «Политика и контроль»

Управленческий анализ «Политика и контроль» выполняется не реже двух раз в год и оценивает эффективность используемых политик и мер контроля в рамках жизненного цикла ИТ-услуги. Политики и меры контроля влияют на производительность ИТ-подразделения и его партнеров, надежность и доверие к качеству предоставляемых услуг, а также способность ИТ—подразделения реагировать на требования бизнеса. Во всех SMF-функциях и на всех этапах жизненного цикла ИТ-услуги особое внимание уделяется выявлению целей управления, рисков, которые могут отрицательно влиять на достижение этих целей, и мер контроля, используемых для смягчения последствий этих рисков. Такой управленческий анализ позволяет руководству оценить политики, меры контроля и их влияние в масштабах всего жизненного цикла с точки зрения достижения целей управления. Этот анализ позволяет определить, насколько эффективным является управление рисками, какова вероятность достижения целей управления и показывает «управление в действии» для уровня «Управление».

Управленческий анализ «Политика и контроль» дает ответы на следующие основные вопросы:

- Верны ли применяемые политики? (с учетом целей управления, нормативных требований, стандартов и отраслевого опыта)
- Эффективны ли эти политики? (отчеты о соответствии нормативным требованиям, запросы на изменение политик и допустимые исключения)
- Верны ли применяемые меры контроля? (исходя из затрат на меры контроля и предоставляемых ими выгод, оценок риска и мер по смягчению рисков, а также событий и инцидентов, не устраняемых с помощью мер контроля)
- Эффективны ли меры контроля на протяжении жизненного цикла?
    - Рассматривая изменения и конфигурацию: достигнут ли желаемый результат, были ли сбои при внесении изменений и требуются ли исправления, чтобы внести изменения?
    - Рассматривая реализацию ценности: оценивается соответствие политики и среды контроля и ценность, которую бизнес-подразделение стремится получить от ИТ-систем. Правильно ли выбран уровень контроля для определенных рисков и ожидаемых результатов?

Управленческий анализ «Политика и контроль» позволяет получить общее представление о контроле и политике, а сами процессы, используемые для управления политиками, описаны в документе *SMF-функция «Политика» модели MOF*.

Данный управленческий анализ позволяет руководителям ИТ-подразделений:

- определять, каким образом нейтрализуются риски, влияющие на достижение целей;
- оценивать сложность реализации мер контроля и изменять их в соответствии с желаемыми преимуществами;
- оценивать поведение как индикатор понимания и принятия политики.

Организация должна внедрить набор соответствующих мер контроля, чтобы достичь следующих целей:

- реализовать требования политики организации, включая политику защиты информации;
- управлять рисками, сопоставленными целям управления и определенным общим мерам ИТ-контроля (например, надлежащий доступ к системам или услугам);
- документировать меры контроля и подтверждения действий по осуществлению контроля.

Поскольку меры контроля являются основным элементом, необходимым для предоставления безопасных и надежных услуг, изменение этих мер всегда должно быть управляемым. Управленческий анализ «Политика и контроль» оценивает влияние изменений, внесенных после предыдущего анализа, на меры управления. Поэтому должны быть задействованы соответствующие средства, позволяющие оценить возможное влияние изменений до их фактического внесения.

Одной из целей этого управленческого анализа является оценка эффективности управления изменениями в среде мер контроля. Соответствующие действия отличаются от действий, выполняемых в рамках *SMF-функции «Изменение и конфигурация»*. Основное внимание здесь уделяется рекомендациям по управлению, обеспечивающим соблюдение политики и эффективность мер контроля.

Управленческий анализ «Политика и контроль» оценивает также политику и меры контроля, являющиеся частью соглашений с внешними организациями (например, соглашений и контрактов, касающихся доступа к информационным системам и данным, а также требований в области безопасности и конфиденциальности этих услуг).

В большинстве случаев участниками этого управленческого анализа должны быть руководители ИТ-подразделений, которым помогают специалисты из групп политики, безопасности и обеспечения соответствия нормативным требованиям. Аудиторы могут предоставить полезные сведения об эффективности мер контроля и факторах,

которые должны учитываться при корректировке этих мер. Партнеры тоже могут принимать участие в анализе, чтобы убедиться, что цели мер управления и политики достижимы в данных средах. Все стороны должны обладать информацией о рисках, а также применяемых мерах по смягчению последствий рисков и гарантировать эффективность исполнения соответствующих мер.

Таблица 4. Компоненты управленческого анализа «Политика и контроль»

Входные данные	Аналитика	Решения	Конечный результат

• Политики эксплуатации и безопасности
• Нарушения политик, инциденты, связанные с несоответствием нормативным требованиям и действия по управлению, предпринятые после последнего управленческого анализа
• Запросы на изменение политик
• Результаты выполнения процесса «Применение и оценка» *SMF-функции «Политика»*
• Изменение норм, стандартов или отраслевой практики
• Аудиторские отчеты, проблемы, рекомендации
• Непредвиденные риски и инциденты
• Невыполняемые или неэффективно выполняемые меры контроля
• Самооценка мер контроля
• Протоколы и мероприятия последней встречи, посвященной управленческому анализу
	• Оценивание инцидентов и нарушений нормативных требований, определение корневой причины
	• Анализ действий по применению политики
	• Анализ аудиторских отчетов и рекомендаций
	• На каждом этапе жизненного цикла оценивается влияние мер контроля и политик, чтобы определить, выполняются ли следующие условия.
	  • **Планирование:** являются ли предоставляемые услуги ценными, прогнозируемыми, надежными и экономически эффективными с точки зрения бизнес-подразделений
	  • **Внедрение:** является ли разработка услуг — эффективной, а развертывание — успешным, готовы ли услуги к эксплуатации
		• Отвечают ли применяемые политики и меры контроля ожиданиям руководства
		• Согласование главной причины несоответствия нормативным требованиям и любых изменений в управлении политикой
		• Используется ли надлежащая среда контроля или требуются изменения
			• Документация управленческого анализа с описанием действий и ответственности
			• Запросы на изменение определенных политик или мер контроля
			• Запросы на изменение управления политиками
			• Запросы на изменение управления мерами контроля

Входные данные	Аналитика	Решения	Конечный результат
	• **Эксплуатация:** соответствуют ли услуги политике, а эксплуатация, сопровождение и поддержка услуг — условиям соглашений OLA/SLA • Анализируется полнота и эффективность оценки рисков и мер по смягчению последствий рисков		

Результатом выполнения управленческого анализа «Политика и контроль» должны являться запросы на изменение, которые позволят усовершенствовать управление, применение политик, управление рисками и среду контроля в целом. Действия по усовершенствованию, выявленные в ходе этого управленческого анализа, должны быть документированы, а соответствующие сведения сохранены, чтобы продемонстрировать участие ИТ-подразделения в основных процессах, связанных с управлением мерами контроля, рисками и политиками. Это обеспечит прозрачность деятельности, а также предоставит данные и факты, которые исполнительное руководство и совет директоров компании смогут использовать для оценки управления ИТ.

Цели SMF-функции «Рабочая группа»

Объектом внимания уровня «Управление» являются две ответственности SMF-функции «Рабочая группа: «Управление» и «Обеспечение соответствия нормативным требованиям». Эти ответственности участвуют в выполнении каждой из трех SMF-функций уровня «Управление». Для каждой SMF-функции существуют таблицы целей и обязанностей, непосредственно относящиеся к действиям в рамках соответствующей SMF-функции.

В следующих двух таблицах описываются типы ролей и их общие цели и обязанности.

Таблица 5. Ответственность «Управление» и ее роли

Тип роли	Обязанности	Цели
Исполнительный директор по ИТ	• Спонсор ИТ-инициатив • Утверждает структуры и общие ИТ-процессы • Владеет показателями и определяет контрольные точки; отвечает за отношения с Комитетом по изменениям и руководством	• Надежная работа и эффективность ИТ-услуг • Непрерывное повышение производительности ИТ с помощью плана усовершенствования
Менеджер по ИТ	• Управляет процессами • Находит и привлекает участников к принятию решений • Управляет зависимостями между рисками и реализацией коммерческой ценности ИТ • Отвечает за отношения между бизнесом и ИТ	• Эффективные управленческие решения • Соответствие ИТ-систем требованиям • Надлежащий баланс риска и реализованной ценности • Использование показателей для отчетов и планирования улучшений
Менеджер ИТ-политик	• Следит, чтобы управленческие решения принимались с учетом политик, а политики в ИТ-подразделении использовались эффективно	• Эффективное применение политик в управлении работой организации при выполнении надлежащих действий
Менеджер по рискам и нормативным требованиям в области ИТ	• Общее управление рисками и программами соблюдения нормативных требований • Информирует организацию о процессах и требованиях SMF-функции «Управление, риск и соответствие нормативным требованиям»	• Качественное информирование о процессах и ожиданиях, связанных с SMF-функцией «Управление, риск и соответствие нормативным требованиям» • Сотрудники знают свои обязанности в рамках SMF-функции «Управление, риск и соответствие нормативным требованиям» и действуют соответствующим образом

Тип роли	Обязанности	Цели
Специалист по обеспечению эффективности и ведению отчетности	• Проверяет структуру и операционную эффективность ИТ-подразделения, процессов и контрольной среды • Рекомендует изменения с целью улучшения	• Деятельность ИТ-подразделения постоянно анализируется и совершенствуется • Управленческие решения и результирующие процессы отражают мнение Комитета по изменениям и заинтересованных сторон
Менеджер по изменениям	• Руководит управлением изменениями в ИТ-подразделении	• Планируемое и понятное изменение с управляемыми рисками
Администратор конфигураций	• Отслеживает изменения и их влияние • Отслеживает конфигурационные элементы • Обновляет систему управления конфигурациями	• Изменение утверждено, а результаты всегда в известном состоянии

Таблица 6. Ответственность «Соответствие нормативным требованиям» и соотнесенные ей типы ролей

Тип роли	Обязанности	Цели
Исполнительный директор по ИТ	• Информирует об ИТ-стратегии и утверждает цели управления ИТ • Утверждает политику • Поддерживает на должном уровне культуру контроля и соответствия нормативным требованиям	• Движение к выбранным целям через выполнение желаемых и соответствующих ситуации действий
Менеджер по ИТ	• Обеспечивает информирование и соответствие политике • Оценивает эффективность политики • Отправляет запросы на изменение политик и создание исключений	• Соответствие политикам и указаниям • Надежные и прогнозируемые результаты, получаемые с помощью надлежащих средств • Устранение нарушений политики
Менеджер по рискам и нормативным требованиям	• Отвечает за управление рисками, планы действий по обеспечению соответствия, а также за применение этих планов и оценку уровня соответствия	• Организация не нарушает нормативные и правовые требования • Риски выявлены и управляемы • Применяются политики

Тип роли	Обязанности	Цели
Специалист по обеспечению эффективности и ведению отчетности	• Выполняет аудит проекта и эксплуатационной эффективности процессов • Анализирует случаи несоответствия нормативным требованиям • Отвечает за отчеты и рекомендации	• Хорошо изученная среда контроля • Независимая проверка программ обеспечения соответствия нормативным требованиям • Обнаружение нежелательных и мошеннических действий
Менеджер по внутреннему контролю	• Управляет средой внутреннего контроля • Документирует цели и проект мер контроля • Сохраняет информацию о выполнявшихся действиях по контролю	• Эффективная среда контроля, документирование среды с сохранением аудиторских следов • Надлежащее сохранение информации о действиях по контролю
Юридическое оформление	• Анализирует нормативные акты и определяет влияние политики • Оценивает правовое положение с точки зрения соблюдения нормативных требований • Предоставляет юридическое заключение в процессе принятия решений	• Политики отражают желаемую реакцию на нормативные акты • Осуществляется управление правовыми рисками
Менеджер ИТ-политик	• Управляет созданием, изменением и сопровождением политик • Отвечает за информирование о политиках и повышение их эффективности	• Эффективное использование политики для управления действиями • Наличие необходимых сведений благодаря понятному описанию политик и информированию о них

Заключение

В документе содержатся общие сведения об этапе «Управление» модели MOF и связанных с ним SMF-функциях, видах управленческого анализа и мерах контроля. Далее при внедрении модели MOF 4.0 нужно определить потребности организации, а затем изучить и применить соответствующие SMF-функции. Подробные руководства для SMF-функций будут полезны ИТ-подразделениям, которые стремятся предоставлять надежные, эффективные и полезные ИТ-услуги.

SMF-функции уровня «Управление»

- *Управление, риск и соответствие нормативным требованиям*
- *Изменение и конфигурация*
- *Рабочая группа*

Обратная связь

Вопросы и комментарии к данному руководству присылайте по адресу mof@microsoft.com.