Microsoft®
Operations Framework
Proven Practices for Operational Excellence

1.Обзор MOF

Введение

Microsoft Operation Framework (MOF) – это структурный подход к работе на платформе Microsoft, который дает пользователям ряд преимуществ. MOF содержит собрание лучших практик, принципов и моделей, которые обеспечивают руководство по достижению высокой доступности, надежности и безопасности особо важных производственных систем, построенных на продуктах и технологиях Microsoft.

MOF и ITIL

Microsoft считает IT Infrastructure Library (ITIL) ведущим общедоступным собранием лучших методов, опробованных на практике. Поэтому Microsoft выбрал ITIL как основу для Microsoft Operation Framework (MOF). В двух центральных разделах ITIL (Service Support & Service Delivery) наименее развит подход к управлению функционированием ИТ-среды. Руководством по взаимодействию ИТ-продуктов и технологий, в частности разработанных Microsoft, MOF расширяет совместную с ITIL область стандартов. В дополнение MOF представляет некоторые концепции, релевантные современной все более и более связанной и подвижной деловой среде. Эти концепции включают в себя интерактивный жизненный цикл, сфокусированный на постоянном развитии и структурированных обзорах управления, для того чтобы обеспечить внимание менеджеров к ключевым моментам этого жизненного цикла. Microsoft содействует ITIL и уже принял участие в написании двух новых книг «Осуществление Управления Сервисами (Implementing Service Management)» и «Управление Приложениями (Application Management)». Вместе с акцентом на управлении функционированием MOF является более ценным подходом к управлению ИТ. Основная часть MOF может быть использована с тем же успехом для других платформ.

Основные соображения разработчиков

Microsoft разрабатывал MOF, руководствуясь следующими соображениями:

- *Усовершенствовать лучшие практические методы достижения цели в индустрии*. Перенимая ITIL, Microsoft улучшил наиболее распространенные практические методы индустрии и взял их за основу MOF.
- *Объединять проверенные идеи и практические методы*. В дополнение к лучшим практическим методам ITIL Microsoft добавил опробованные идеи и методы своих собственных групп ИТ-специалистов, специалистов сервисных групп, а также своих партнеров и клиентов.
- *Обеспечить руководство людьми и процессами*. Microsoft разрабатывал MOF, чтобы дополнить свои продукты специальным руководством по организации процессов и деятельности людей, работающих в сфере данной технологии.
- *Использовать преимущества метода предоставления полного цикла Сервисов*. Предоставлению индивидуальных технических компонентов (таких как рабочие станции или серверы) Microsoft предпочитает предоставление полного цикла ИТ-Сервисов (таких как передача сообщений, печать и т.п.), более того, делает на него главную ставку.
- *Объединиться, составить единое целое со всем жизненным циклом ИТ*. Microsoft разрабатывал MOF, чтобы объединить планирование и развертывание действий в пределах всего жизненного цикла ИТ.

Почему Microsoft создал MOF

Продолжает увеличиваться использование серверных платформ Microsoft для бизнеса (включая Windows, Exchange Server и SQL Server) в наиболее важных компьютерных системах на производстве. В результате такой ситуации возникла потребность в инструкции по рентабельной эксплуатации этих платформ для достижения высокой доступности, надежности и безопасности. Microsoft создал MOF, чтобы предоставить эту инструкцию.

Модели MOF

MOF создавался из трех основных моделей, каждая из которых должна была представлять главные компоненты ИТ-операций. Модели MOF это:

- *Модель процессов* - функциональная модель процессов, представленная сервисными организациями для управления и поддержки ИТ-Сервисов.

- *Командная модель* - упрощенный обзор ролей в команде, который помогает менеджменту сфокусировать внимание на организации эффективной деятельности штата.
- *Модель риска* - объединение ключевых принципов, стандартной терминологии, структурированного и повторяющегося пятиступенчатого процесса для управления рисками, с которыми штат сервисных организаций встречается ежедневно.

Более подробные сведения о каждой из этих моделей представлены в последующих секциях этого руководства.

Основная терминология

Определения следующих трех терминов очень важны для полного понимания моделей MOF:

- *Сервисные решения* - это определенные в терминах функциональности на уровне конечного пользователя возможности, которые ИТ предоставляет бизнесу. Различие делается между полными Сервисами и их компонентами. Примерами могут служить бизнес-приложения, передача сообщений, хранение данных и услуги печати.
- *Функции Управлениями сервисами (SMF)* - это процессы, которые управляют ИТ-сервисами на основе сервисного подхода. Примерами SMF могут служить управление изменениями, системное администрирование и Service Desk.
- *Обзоры Управления функционированием (OMR)* - ключевые контрольные точки, сфокусированные на SMFs в пределах квадранта процессной модели.

2. Что такое Управление ИТ-Сервисами?

Быстрый обзор

Чтобы понять термин «Управление ИТ-Сервисами» (ITSM), лучше всего начать с определения его составных частей:

- Традиционное определение *Информационных Технологий (ИТ)* по ITIL – это такие технологии, которые используются при поддержке ИТ-инфраструктуры: комплектующих, программного обеспечения, сетевых компонентов, документации, процедур и процессных ролей.
- *Сервис* - это набор компонентов, физических и логических, ИТ и не ИТ, требуемых для осуществления поддержки бизнес-операций. Клиенты будет судить о его эффективности по поддержке, которая оказывается их бизнес-операциям, и «видеть» этот набор целиком, как единый объект, не рассматривая каждый компонент в отдельности.

- В этом контексте термин *ИТ-Сервис* относится к набору родственных ИТ и не ИТ-функционалов, который поставляется конечному пользователю в качестве Сервиса. Примерами ИТ-Сервисов являются: передача сообщений, бизнес-приложения, файловые услуги и услуги печати, сетевые Сервисы и служба поддержки.
- В этом контексте термин «*Управление*» относится к концепциям и практическим методам, задействованным в поддержке и предоставлении этих сервисов на стратегическом, тактическом и операционном уровнях. Управление связано с использованием ресурсов, включая оборудование, штат, процессы и идеи, для того, чтобы достигнуть в итоге, в данном случае, предоставления Сервиса.

Центральная идея *Управления ИТ-Сервисами* состоит в том, что ИТ-организации, внутренние или внешние, являются поставщиками ИТ-Сервисов. Их работа заключается в предоставлении высококачественных и рентабельных ИТ-Сервисов. Качество и рентабельность ИТ-Сервисов определяется клиентами (теми, кто оплачивает Сервисы) и пользователями (теми, кто использует Сервисы).
Задача управления ИТ-Сервисами – выстраивать предоставление услуг в соответствии с текущими и будущими требованиями клиентов и пользователей. Предоставление ИТ-Сервисов считается достигнутым, когда предоставлены все требуемые Сервисы, достигнут установленный уровень качества по оговоренной цене. В конце концов, от управления ИТ-Сервисами может зависеть возможность ведения бизнеса.

Почему необходимо Управление ИТ-Сервисами?

Все большая зависимость бизнеса от ИТ-Сервисов увеличивает потребность в эффективном управлении этими Сервисами. ИТ нельзя представлять как набор устройств и приложений, предоставляемых пользователю. ИТ нужно рассматривать как серию объединенных Сервисов. Сейчас уже очевидно, что многие первичные бизнес-процессы не могут функционировать без участия ИТ-Сервисов. Во многих отраслях ИТ уже стали частью бизнес-процессов. А в некоторых - даже самостоятельными бизнес-процессами. Развитие электронной коммерции также показало, что ИТ стали критическим фактором для ежедневных бизнес-операций. Поэтому бизнесу необходимо контролировать ИТ и ИТ-Сервисы, чтобы по возможности уравнять относительно друг друга бизнес-процессы и ИТ-Сервисы.

Возникновение Управления ИТ-Сервисами

В основе лучших практических методов управления ИТ-Сервисами лежит сборник лучших практик, который разработан и постоянно пополняется в

Великобритании, под названием ITIL (IT Infrastructure Library – Библиотека Инфраструктуры ИТ). Первоначально библиотека ITIL развивалась британским правительством в конце 80-х на основе информации от многих экспертов в этой отрасли. Целью разработки ITIL было создание открытого стандарта для управления ИТ-Сервисами, который могли бы перенять и адаптировать поставщики ИТ-услуг. В данный момент ITIL находится под управлением Ведомства Государственной Торговли Британского Правительства, ведомства Министерства Финансов Ее Величества.
Текущее издание ITIL содержит 7 книг: «Поддержка Сервисов», «Поставка Сервисов», «Управление приложениями», «Управление инфраструктурой ICT», «Планирование Управления Сервисами», «Управление безопасностью» и «ITIL с точки зрения бизнеса». «ITIL Поддержка Сервисов» и «ITIL Поставка Сервисов» являются основными публикациями, в которых описаны функции Службы Поддержки и следующие ключевые процессы управления Сервисами:

ITIL Поддержка Сервисов	ITIL Поставка Сервисов
• Управление Инцидентами • Управление Проблемами • Управление Конфигурациями • Управление Изменениями • Управление Релизами	• Управление Уровнем Сервиса • Управление Доступностью • Управление Мощностью • Управление Финансами для ИТ-Сервисов • Управление Непрерывностью ИТ-Сервисов

Руководство ITIL продается, вне зависимости от платформы, и поддерживается всемирной индустрией обучения, общепризнанными уровнями сертификации и консалтинговыми службами, также как и программными продуктами, которые позволяют упростить весь процесс.

С момента своего создания ITIL стал всемирным стандартом де-факто для управления ИТ-Сервисами.

3. Осуществление Управление Сервисами

Управление ИТ-Сервисами является задачей, которую нельзя не принимать всерьез. Оно требует специальных навыков, которыми обычно ИТ-сотрудники не владеют. Вместо решения, в основном, технических проблем, деятельность ИТ-отделов фокусируется на поставке услуг. Главные различия между продуктами и сервисами можно резюмировать:

1. Услуги, по своей сути, неосязаемы.

2. Значительная часть сервисов фактически состоит из соглашений и взаимодействий. Обычно они представляют собой согласованные действия клиентов и технического персонала.
3. Производство и потребление сервиса неразделимы, поскольку они работают одновременно.
4. Клиенты зачастую больше, чем просто потребители – они, как правило, принимают участие в производстве сервиса.
5. Современные сервисы поставляются через цепочку партнеров, состоящую из клиента, ИТ-провайдера и третьих лиц (поставщиков).

Это означает, что качество оказанного сервиса можно установить лишь в момент получения этого сервиса. Этот момент часто упоминается как «Момент истины» (Normann, 2000). Можно также сказать, что «момент истины» преимущественно зависит от настроения и отношений между всеми участвующими сторонами. И в этом есть как свои минусы, так и плюсы.
Как показывает опыт лучших практик, для того чтобы определить ожидания клиентов и возможности поставщиков сервисов, между сторонами необходимо заключать соглашение. Такое соглашение должно быть построено на метрике, которая поможет определить качество полученных услуг.

Важно осознавать, что управление ИТ-Сервисами повлечет за собой изменения в организационной культуре. Основное внимание сотрудников ИТ-отдела будет сфокусировано не на поставляемой продукции (программное обеспечение, сети и прочее), а на результате (какой эффект это производит на клиента). Поведенческие проблемы, такие как управление отношениями, управление рисками и деловая хватка, становятся главными аспектами. Для таких проблем легкого решения не существует.

Успешное управление ИТ-Сервисами – это осязаемый показатель пользы, который можно применить при проработке различных ситуаций в бизнесе и для доказательства успешности. Это требует от ИТ-отдела существенных усилий в обучении и общении с клиентом.
Долговременная проблема касается «устойчивости курса»: не отклоняться от установленных процессов и не возвращаться к старым способам решения проблем с предоставлением Сервисов. Общеизвестно, что фокусировка внимания на процессах стимулирует внимание к клиентам в области предоставления Сервисов и повышает их качество.

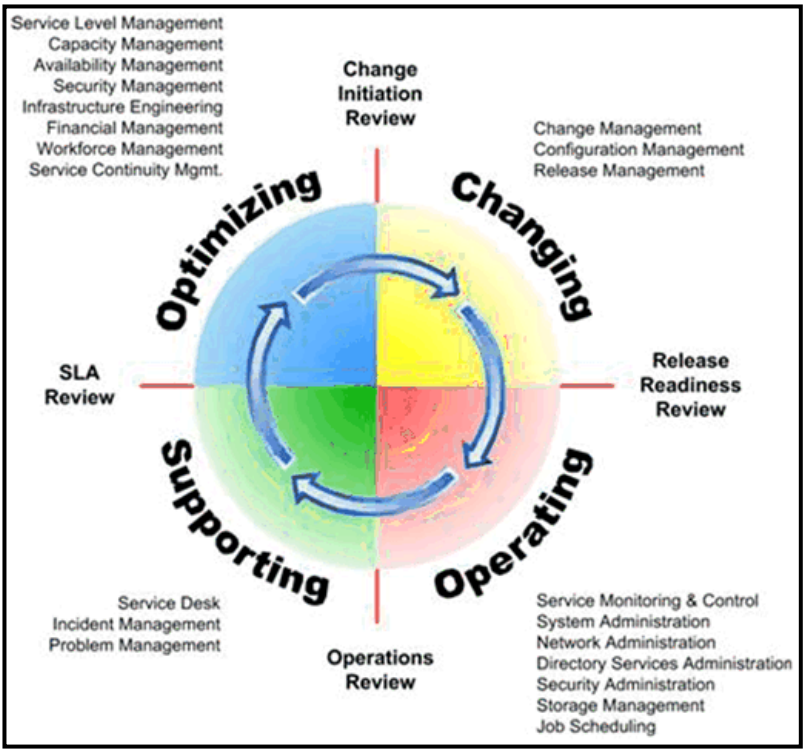
4. Модель процессов MOF

Обзор

Модель процессов MOF содержит четыре основные концепции, которые являются ключом к пониманию этой модели:

- Управление ИТ-Сервисами, например, развитием программного обеспечения, имеет свой жизненный цикл.
- Жизненный цикл состоит из ясных, логических фаз, которые запускаются согласованно.
- На каждой фазе работает процесс Обзора Управления Операциями (Operation Management Review - OMR).
- Управление ИТ-Сервисами касается каждого аспекта предприятия.

Модель процессов MOF представляет жизненный цикл каждого сервисного решения. Цель Модели процессов - обеспечить простое представление взаимоотношений между компонентами в пределах данной модели.



Модель процессов разделяет MOF SMF по связанным функциям на четыре квадранта: Изменений, Управления, Поддержки и Оптимизации.

Квадранты составляют наивысший уровень в работе Модели процессов и называются поэтому:

- **Квадрант изменений** – SMF используются для идентификации, обзора, утверждения, записи и объединения изменений в управляемое ИТ-окружение:
  - *Управление изменениями.*
  - *Управление конфигурациями.*
  - *Управление релизами.*
- **Квадрант управления** – SMFs используются для проверки, контроля, управления и администрирования решений для Сервиса и ежедневного достижения согласованного уровня Сервиса:
  - *Администрирование систем.*
  - *Администрирование безопасности.*
  - *Мониторинг и контроль Сервисов.*
  - *Планирование заданий.*
  - *Сетевое администрирование.*
  - *Администрирование служб каталогов.*
  - *Управление печатью и производством*
  - *Управление хранением данных.*
- **Квадрант поддержки** - SMFs используются для идентификации, установления, диагностики, прослеживания и решение инцидентов, проблем и запросов, основанных на согласованных уровнях Сервиса:
  - *Служба поддержки.*
  - *Управление инцидентами.*
  - *Управление проблемами.*
- **Квадрант оптимизации** - SMFs используются для управления стоимостью вместе с поддержкой и улучшением согласованных уровней Сервиса:
  - *Управление уровнем Сервиса.*
  - *Управление мощностью.*
  - *Управление доступностью.*
  - *Управление финансами.*
  - *Управление персоналом.*
  - *Управление непрерывностью.*

Обзоры Управления

Модель процессов объединяет два типа обзора управления, основанных на критериях: релиз (готовность и испытанность релиза) и время (операции и соглашение об уровне Сервиса (Service Level Agreement — SLA)). Причиной для такого смешения типов обзора является необходимость поддержки двух концепций в среде ИТ-операций:

- Необходимость управлять введением изменений посредством использования управляемых релизов.
- Потребность в беспрестанной оценке и адаптации операционных процедур, процессов, инструментов и людей, необходимых для поставки специфических решений для Сервиса.

Обзор Управления Операциями (OMR) взаимодействует с каждым квадрантом. Каждый Обзор Управления Операциями представляет собой контрольный пункт с акцентом на SMF, находящихся в пределах соответствующего квадранта.

Квадрант	Обзор	Цель
Изменение	Готовность релиза	Утвердить готовность релиза, плановое состояние, выполнение планируемых и определение возможных улучшений в будущих релизах.
Управление	Операции	Улучшить эффективность текущих процессов, процедур и технологии управления, обеспечить получение и документирование знаний.
Поддержка	Соглашение об уровне Сервиса (SLA)	Предоставить клиенту адекватный уровень ИТ-Сервиса.
Оптимизация	Испытанность релиза	Получить одобрение предлагаемых изменений в решениях для Сервиса, основанных на анализе и приоритете затрат/доходов.

Следующие разделы описывают квадранты Модели процессов MOF, SMF и Обзоры Управления Операциями.

5. Квадрант Изменений MOF

Обзор

Целью Квадранта Изменений является эффективное, быстрое внесение одобренных изменений в ИТ-среду с минимальными последствиями для Сервиса. Изменение определяется как изменения в технологиях, системах, программном обеспечении и комплектующих, а также изменения в процессах, ролях и обязанностях. Квадрант Изменений включает в себя SMFs, используемые для идентификации, обзоров, одобрения и объединения изменений в управляемую ИТ-среду. Этими SMF являются:

- Управление изменениями

- Управление конфигурациями
- Управление релизами

Управление Изменениями

Обзор

Управление изменениями контролирует все изменения в ИТ-среде и обеспечивает запись и наблюдение изменений в этой среде. Управление изменениями пытается определить все затронутые системы, процессы и стороны до внесения изменений, для того чтобы уменьшить или полностью исключить любые потери для бизнеса или неприятные последствия.

Обычно, ИТ-среда является реальной производственной областью, но Управление изменениями может также применяться при объединении, тестировании и организации сред. Область Управления изменениями обычно ограничивается Конфигурационными Единицами (Configuration Items — CIs) в базе данных Управления Конфигурациями (CMDB).

Ключевые понятия

- *Запрос на изменение (Request For Change — RFC).* Это формальный запрос, который предлагает некоторые изменения. Он включает в себя описание изменения, затрагиваемые компоненты, потребности бизнеса, оценку затрат, оценку риска, потребности в ресурсах и результаты утверждения.
- *Консультативный совет по изменениям (Change Advisory Board — CAB).* CAB — это группа сотрудников предприятия, имеющих разные специализации, которая организована для оценки запросов на изменение с точки зрения потребностей бизнеса, приоритета, затрат и выгод, а также потенциального влияния на другие системы или процессы. Как правило, CAB дает рекомендации по внедрению, дополнительному анализу, последующему рассмотрению или отмене изменений.
- *Контроль изменений* - Управление изменениями является управлением рисками. Поэтому изменениями необходимо управлять, оценивая сложность, затраты, влияние, и каждый шаг процесса должен быть точно согласован.

Управление Конфигурациями

Обзор

Управление конфигурациями отвечает за определение, запись, отслеживание и отчетность по компонентам (относящимся к Конфигурационным единицам - КЕ)

ИТ-среды. Существуют три основные цели Управления конфигурациями:

1. Обеспечить доступ к ИТ-среде только авторизованным КЕ.
2. Обеспечить запись и прослеживание в течение всего жизненного цикла всех изменений среди КЕ.
3. Обеспечить тщательное документирование взаимоотношений между КЕ.

КЕ могут включать в себя комплектующие, программное обеспечение, документацию, процессы, процедуры и людей. Различные держатели информации в CMDB отвечают за специфическую информацию, которая собирается и отслеживается. В общем случае такая информация по КЕ включает в себя описание, версию, составные компоненты, отношения с другими КЕ, положение/назначение, финансовую информацию и текущий статус.

Оригиналы копий и программные продукты, используемые для системных установок, стандартного сервера, следует держать в репозитории - защищенном хранилище всех авторизованных версий программных КЕ (Definitive Software Library – DSL), которое относится к CMDB. DSL является надежным местом для расположения программных компонентов, доступных для использования внутри ИТ-организации и управляемых в пределах SMF управления релизами.

Детализация авторизированных компонентов конфигураций, версий, моделей и т.д. содержится в Хранилище авторизованных аппаратных КЕ (Definitive Hardware Store - DHS).

Управление конфигурациями часто путают с учетом ОС, бухгалтерской практикой, которая отслеживает дорогие и материальные ИТ-компоненты в целях оценки и снижения их стоимости. Сходство этих систем в том, что и там, и там содержится информация по имуществу, включая данные о бизнес-подразделении, дате закупки, снабженце и местоположении имущества. Но в учете ОС, в отличие от управления конфигурациями, никакие взаимоотношения обычно не записываются. Для многих ИТ-организаций учет ОС часто является предшественником управления конфигурациями.

Ключевые понятия

- *Планирование управлением конфигурациями* - планирование и определение границ, задач, политик, процедур, организационных и технических контекстов управления конфигурациями.
- *Определение конфигурации* - выбор и определение конфигурационной структуры для всех КЕ, их «владельца», их взаимоотношений и конфигурационной документации. Также включает в себя уникальные номера КЕ и их версии.

- *Контроль конфигурации* - Обеспечение допуска только авторизированных и опознаваемых КЕ, а также ведение записи с момента их получения и до удаления КЕ из конфигурации.
- *Определение статуса конфигурации* - Отчетность по текущей и архивной информации, касающейся каждой КЕ в течение всего ее жизненного цикла. Таким образом, можно вносить изменения в КЕ и отслеживать записи. Например, допускать отслеживание статуса КЕ в таких состояниях, как разработка, тестирование, использование и списание.
- *Проверка и аудит конфигурации* - Серия обзоров и аудитов, которые подтверждают физическое существование КЕ и проверяют, что они правильно записаны в систему управления конфигурациями.

Управление Релизами

Обзор

Управление релизами облегчает введение релизов программного обеспечения и комплектующих в управляемые ИТ-среды, включая подготовку и непосредственно само производство. Цель управления релизами - обеспечение успешного развертывания изменений в ИТ-среде с минимальными потерями для бизнеса. Управление релизами координирует взаимодействия между командой, отвечающей за разработку решений для Сервиса, и управляющими командами, отвечающими за осуществление решений для Сервиса на этапе производства.

Релиз должен находиться под контролем изменений и состоять из любых комбинаций между комплектующими, программным обеспечением, программируемым оборудованием и документацией по КЕ. Абсолютно все релизы должны быть испытаны SMF управления изменениями до того, как они будут внедрены.

Управление релизами работает совместно с процессами управления изменениями и конфигурациями для поддержания совместной CMDB в актуальном состоянии при изменениях, внесенных новыми релизами. Программное содержание этих релизов помещается в DSL. Спецификации комплектующих, собрание инструкций и конфигурации сети также содержатся в DSL/CMDB.

Ключевые понятия

- *Планирование релиза - в отношении* получения одобренного RFC, определения заданий и действий, которые необходимы для успешного развертывания релиза в реальной среде.

- *Построение релиза* - обобщение и разработка процессов, инструментов и технологий, требуемых для развертывания релиза в реальной среде.
- *Тестирование* - тестирование релиза на модели производственной среды с целью убедиться, что релиз не окажет вредного воздействия на реальную среду.
- *Обзор готовности релиза* - последняя контрольная точка и шаг согласования до того, как команда релиза начнет детальное планирование развертывания.
- *Планирование отката* - расстановка приоритетов и детальное планирование возвращения релиза к ИТ-окружению.
- *Приготовление релиза* - приготовление производственной среды к новым релизам. Может включать общение с пользователями, обучение службы поддержки и технического персонала и создание резервных копий особо важных компонентов.
- *Развертывание* - введение релиза в производственную среду и обновление CMDB, чтобы отразить все изменения среди КЕ.
- *Обзор после релиза* - после каждого развертывания в производственной среде обзор после внедрения позволяет судить об успешности процесса и разрабатывать улучшения.

Обзор Готовности Релиза

Обзор готовности релиза представляет собой Обзор Управления Функционированием в Квадранте Изменений. Он определяет, готов ли релиз и работает ли он в целевой среде. Процесс-субстрат (случайный процесс) в этом обзоре является ключевой точкой объединения Microsoft Solution Framework (MSF) и MOF. При помощи этого процесса ключевые свойства релиза сравниваются со стандартами, политиками и метриками качества так же, как и с факторами готовности, вроде существования и качества планов осуществления, планов коммуникаций, уровней и навыков персонала, определений процессов и документации.

Целью готовности релиза является подтверждение того, что релиз соответствует всем установленным стандартам продвижения в реальную среду, и что управляющая команда готова к его установке, менеджменту и поддержке. Основываясь на этой оценке, релиз считается готовым к презентации в целевой среде (или производству), или возвращается на предыдущий этап с перечислением недостатков.

8. Квадрант Оптимизации MOF.

Обзор

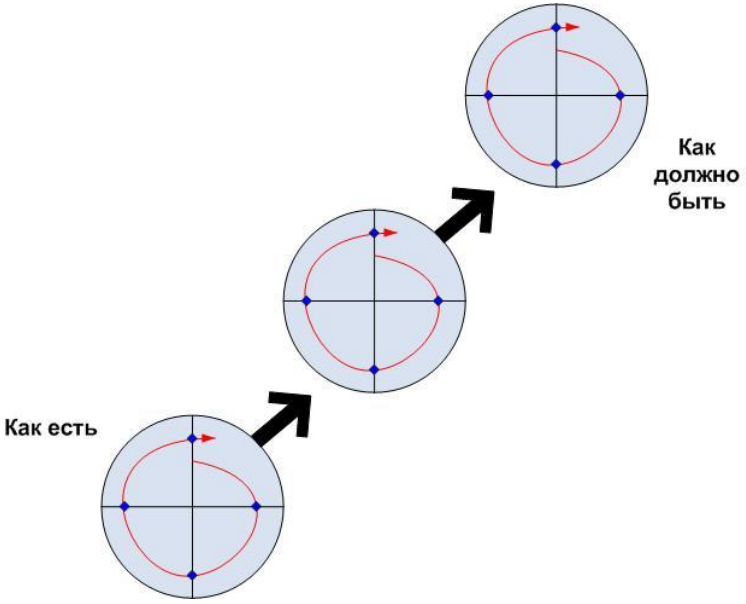
Цель Квадранта Оптимизации – это оптимизация затрат, производительности, мощности и доступности предоставляемых ИТ-

сервисов. Квадрант Оптимизации включает в себя SMF, которые позволяют управлять затратами при поддержке и улучшении уровней Сервисов. Этими SMF являются:

- Управление уровнем Сервиса.
- Управление финансами.
- Управление непрерывностью.
- Управление доступностью.
- Управление мощностью.
- Управление персоналом.

Также цель состоит в понимании текущего состояния операционной среды. Оно достигается исследованием сбоев/инцидентов, рассмотрением структуры затрат, оцениванием персонала, анализом доступности и производительности и прогнозированием мощности.

Главным результатом любой SMF этого квадранта считается идентификация, определение и, в конце концов, утверждение затрат на изменения в виде новых релизов и/или удаление некоторых Сервисов. Улучшения, произведенные с четким пониманием текущего состояния, будут повторяться. Диаграмма иллюстрирует эту концепцию, используя Модель Процессов MOF для непрерывного улучшения. Иерархия SMF в пределах Квадранта Оптимизации проиллюстрирована ниже.



MOF осознает, что от успешного выполнения ИТ-операций зависит успех на конкурентном рынке. Квадрант Оптимизации особенно заостряет внимание на этом факте, фокусируясь на двух фундаментальных элементах операций:

- Бизнес-ориентированное управление уровнем Сервиса.
- Осведомленность и управление затратами на предоставление Сервисов.

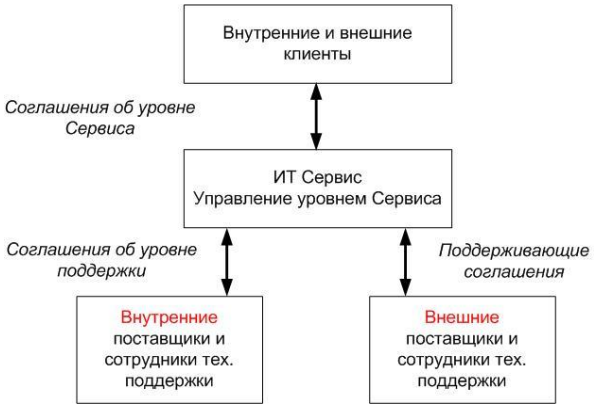
Управление Уровнем Сервиса

Обзор

Управление уровнем Сервиса (SLM) нацелено на обеспечение того, что должным образом заданы ожидания обеих сторон (и ИТ-организации, и клиентов/пользователей), и что требуемые уровни Сервиса поддерживаются. SLM отвечает за выполнение обязательств, оговоренных в Соглашениях об Уровне Сервиса (SLA), Соглашениях об Уровне Операций (OLA) и Поддерживающих Соглашениях (UC). А также следит, чтобы возможный ущерб нормальному функционированию Сервисов был минимальным. Это достигается при использовании цикла соглашений, проверок и отчетов об успехах ИТ-Сервисов и проведении необходимых действий для поддержания баланса между потребностями и затратами.

SLM обеспечивает структурированный подход дискуссии между клиентами и поставщиками ИТ-сервисов и оценки того, насколько хорошо поставляются сервисы.

Следующая диаграмма показывает иерархию соглашений:



Ключевые понятия

- *Создание сервисного каталога* - *Он* содержит в себе список всех Сервисов, предоставляемых в данный момент, резюме характеристик Сервисов, данные о пользователях Сервисов и служащих, несущих ответственность за поддержку.
- *Разработка SLA* - SLA является соглашением между поставщиком ИТ-Сервисов и сообществом клиентов/пользователей. SLA формализует требования клиента/пользователя к уровню Сервиса и определяет ответственность всех участвующих сторон.
- *Согласование обязательств из SLA, OLA и UC* - Поддерживающие соглашения и Соглашения об Уровнях Операций должны иметь метрики Сервисов, согласованные относительно обязательств SLA.
- *Управление процессом* - Управлению уровнем Сервиса требуется использование постоянного цикла соглашений, проверок и отчетов об успехах ИТ-Сервисов и проведении соответствующих действий для поддержания баланса между потребностями и затратами.

Управление Финансами

Обзор

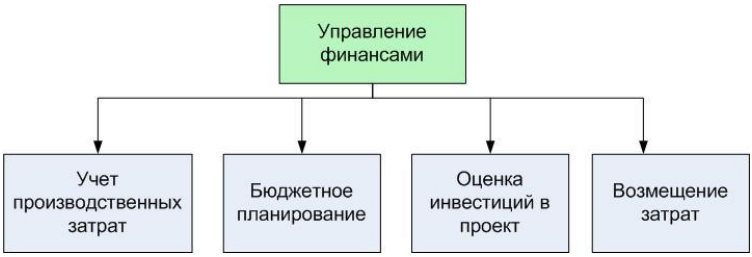
Управление финансами является управлением денежными ресурсами, обеспечивающими достижение целей организации. Управление финансами гарантирует, что любое решение, предложенное основными

SMF (управление непрерывностью ИТ-сервиса, управление доступностью, управление мощностью, управление персоналом) в соответствии с требованиями управления уровнем Сервиса, обосновано с точки зрения стоимости и бюджета. Это часто называется анализом рентабельности. Управление финансами также помогает связать затраты с конкретными ИТ-Сервисами. Таким образом, ИТ-подразделение может принимать более продуманные решения, и клиенты лучше понимают, какие именно затраты с какими Сервисами связаны.

Управление финансами основано на тех же принципах бухгалтерского учета, которые сегодня широко используются во многих сферах производства. В современных компаниях управление финансами для ИТ включает в себя бюджетное планирование, учет производственных затрат, распределение расходов, модели возмещения расходов, и учет доходов. Важнейшими аспектами управления финансами являются связи управления финансами с другими функциями управления Сервисами.

Управление финансами занимается расходной частью процесса при принятии бизнес-решений относительно изменений в ИТ-инфраструктуре, системах, штате, или процессах. Знание о расходах на конфигурацию и о единицах, подлежащих изменению, необходимо для принятия правильных бизнес-решений.

Управление финансами занимается также доходной стороной финансового процесса. Так сложилось исторически, что ИТ-отдел всегда рассматривался просто как центр расходов; однако в последнее время ИТ-отдел приобретает все большее значение как центр доходов. Схема слева демонстрирует основные компоненты управления финансами.



Ключевые понятия

- *Учет производственных затрат* - Определение объектов и деятельности, которые требуют расходов, и разработка схемы распределения расходов для предъявления клиентам детального счета за полученные Сервисы.

- *Бюджетное планирование* - Разработка бюджета для запланированной деятельности и оценка бюджетной эффективности текущей деятельности. Финансовый менеджер занимается сбором данных от каждого отдела организации, использующего ИТ-сервисы, а также данных по каждой функции управления Сервисом.
- *Оценка инвестиций в проект* - Анализ стоимости и выгоды предлагаемых изменений и новых Сервисов. Управление финансами использует несколько методов оценки предполагаемых финансовых последствий заявленных изменений, включая анализы периода окупаемости, чистой приведенной стоимости, дохода на инвестиции, совокупной стоимости собственности и чистой стоимости собственности.
- *Возмещение затрат* - Возмещение затрат включает развитие методов возмещения и объявление клиентам стоимости Сервисов.

Управление непрерывностью

Обзор

Цель Управления непрерывностью - обеспечить предоставление Сервисов даже в случае непредвиденных или неприятных событий в ИТ-организации. Это выполняется при помощи анализа влияния бизнес-процессов на организацию и анализа уязвимых мест в ИТ-инфраструктуре, относящихся к этим процессам.

Многие факторы влияют на доступность ИТ-Сервисов, например, отказ оборудования, стихийные бедствия и человеческие ошибки. Эти факторы относятся к рискам доступности, а действия, направленные на уменьшение их негативных последствий, называются контрмерами. Контрмеры включают тщательную разработку процедур тестирования и релиза, а также соответствующие планы по обучению персонала. Если контрмеры оказываются неудачными, необходимо перейти к более решительным действиям: эти меры обычно выделяются в документе, под названием «план действий в чрезвычайных ситуациях».

Управление доступностью и управление непрерывностью тесно связаны между собой, так как оба стараются устранить все помехи доступности ИТ-сервисов. В то время как управление доступностью сосредотачивается на тех помехах, появление которых можно ожидать каждый день, управление непрерывностью обращает внимание на редкие, неожиданные или требующие чрезмерно дорогих контрмер риски.

Ключевые понятия

- *Достижение требований непрерывности* - Определение рисков, не устраняемых управлением доступностью.
- *Предложение возможных решений* - Создание рентабельных планов действий в чрезвычайных ситуациях. Эти планы должны состоять из двух равносильных, но независимых друг от друга частей:
    - Преодоление сбоя – Перенесение работы компонента с его основного расположения на побочное.
    - Восстановление – Восстановление работы компонента на его основном месте расположения.
- *Формализация Соглашения об Уровне Операций* - Формализация соглашения между внутренними поставщиками ИТ-Сервисов для эффективного по затратам решения в чрезвычайной ситуации.
- *Формализация плана действий в непредвиденных ситуациях* - Формализация плана действий в чрезвычайных ситуациях, включающая в себя предписывающее руководство по преодолению сбоев и восстановлению, процедурам эскалации и оповещения, пуска и остановки, требования по отчетности о состоянии.

Управление Доступностью

Обзор

Целью управления доступностью является рентабельное и последовательное выполнение требований клиентов по доступности ИТ-Сервисов. Управление доступностью отвечает за предотвращение инцидентов, оказывающих влияние на доступность Сервисов, и обеспечивает принятие своевременных и эффективных мер при инцидентах такого типа. Управление доступностью фокусируется на двух областях:

- *Новые ИТ-Сервисы* - наилучшая возможность для достижения уровня доступности с разумным соотношением цена-качество, потому что соображения доступности могут закладываться на самых ранних этапах разработки. Это позволяет выбирать наиболее подходящие технологии и создавать инфраструктуру ИТ-поддержки требуемого уровня. В данном случае заказчику и ИТ-организации предоставляется отличная возможность вместе поработать над определением и уровнем доступности, который будет предоставляться ИТ-Сервисом и согласовать количество необходимых инвестиций.
- *Существующие ИТ-Сервисы* - могут существенно улучшить или стабилизировать свой уровень доступности с помощью внедрения формального процесса управления доступностью. В данном случае подход к управлению ИТ-Сервисами очень похож на создание новых ИТ-Сервисов и начинается с совместного с

заказчиком определения доступности и определения соответствующего бюджета для улучшений и эксплуатации.

Ключевые понятия

- *Определение целей и препятствий в обеспечении доступности* – отражается в Соглашении по требованиям к доступности и по бюджету между поставщиками ИТ-Сервисов и клиентами. Эта работа должна быть основана на четком понимании бизнес-целей клиента и стоимости простоя или недоступности Сервиса.
- *Предложение решений по доступности* – пошаговый процесс, в котором требования доступности сбалансированы с бюджетом, чтобы определить рентабельную комбинацию технологий, людей и процессов, необходимых для достижения поставленных требований.
    - Идентификация основных Сервисных компонентов – определение основных технологических компонентов, инфраструктуры, людей и процессов, поддерживающих поставку сервисов от начала до конца.
    - Разработка с учетом требований к доступности – определение рисков доступности, оказывающих влияние на каждый компонент Сервиса, и разработка рентабельных контрмер; рассмотрение нужд каждого компонента жизненного цикла и обеспечение определенной их направленности.
    - Разработка с учетом требований к восстановлению – обеспечение эффективного обнаружения инцидентов, средств и процессов восстановления, которые принимают на себя все происходящие сбои в сервисах.
- *Формализация Соглашений о рабочем уровне* – Формализация соглашений между внутренними поставщиками ИТ-Сервисов с целью доступности механизма и частоты отчетов и информации, докладываемой клиенту.

Управление Мощностью

Обзор

Управление мощностью – это процесс планирования, сортирования и контроля мощности решений Сервиса для достижения обязательств из SLAs и OLAs. Целью управления мощностью является оптимизация мощности ИТ-инфраструктуры и вспомогательных структур, для того чтобы поддерживать рентабельность и стабильную доступность на таком уровне, который гарантирует выполнение задач бизнеса.

Управление мощностью постоянно ищет способы оптимизации существующих и будущих потребностей в ИТ-ресурсах. Оптимизация

определяется как использование ресурсов в наилучшем сочетании места, времени, количества и цены. Исходя из этого, процесс управления мощностью обеспечивает реализацию плана по мощности и инициирует запросы на изменения, в результате которых объекты инфраструктуры обновляются или появляются. При этом чаще всего обозреваются процессы функционирования. А процессы, развернутые для доставки решений Сервиса, не пересматриваются при постоянном увеличении нагрузки со стороны пользователей до тех пор, пока время в отклика в системе не станет причиной разнообразных проблем.

Ключевые понятия

- *Управление производительностью* - обеспечивает соответствие возможностей по обработке информации, хранению и мощности сетевых ресурсов, изменяющимся требованиям бизнеса, при условии оптимизации временных и финансовых затрат.
- *Определение размера приложений* – определение мощности оборудования и сети, требуемой для поддержки новых или модификации существующих приложений, включая загрузку персонала (с детализацией требований приложения по мощности).
- *Моделирование* – использование математических моделей и других техник моделирования для определения влияния альтернатив развертывания мощности (доступных в данный момент или приобретаемых в течение некоторого периода). Например, рассмотрение нескольких сценариев повышения требований к ИТ-Сервисам.
- *Планирование мощности* – внесение изменений в план мощности, анализ текущей ситуации (предпочтительно, с использованием сценариев) и предугадывание будущего использования ИТ-инфраструктуры и ресурсов, необходимых для достижения ожидаемых требований к ИТ-Сервисам.
- *Согласование с бизнес-планом* – бизнес-план сообщества пользователей должен быть главным компонентом плана мощности.

Управление Персоналом

Обзор

Управление персоналом обеспечивает привлечение, развитие и удержание надлежащим образом подготовленного ИТ-персонала, который выполняет ежедневные задачи по эксплуатации и функционированию вычислительной среды организации. Основной задачей управления персоналом является обеспечение нужной укомплектованности кадров, когда специалисты принимаются на работу для управления действующим производственным оборудованием. Кроме того, должны существовать процедуры, которые гарантируют, что

кадровые потребности выполняются на надлежащем уровне. Управление персоналом также занимается вопросами техники безопасности, чтобы обеспечить безопасное, эффективное, постоянное рабочее место.

Ключевые понятия

- *Построение организации эксплуатации* - включает в себя определение требований к кадровому обеспечению, обучение и удержание, а также анализ приема персонала.
- *Вопросы производительности персонала* - управление производительностью персонала, включая выбор реальных и достижимых целей, проверки, измерения и оценку производительности и управление наградами и поощрением.
- *Поддержка надежного и подготовленного персонала* - подготовка, обеспечивающая удержание персонала, способного обеспечить надежное функционирование ИТ-операций и производительность.

Обзор утвержденного Релиза

Обзор утвержденного релиза решает, одобрять или не одобрять субсидирование и передачу ресурсов релизу для специфического решения Сервиса. В этом обзоре специально сформированная группа обзора оценивает:

- Затраты/прибыль от удобства использования и поддержки сервисного решения.
- Затраты/прибыль подготовки целевой среды (организация и инфраструктура) для поддержки и использования Сервисного решения.
- Затраты/прибыль плана осуществления релиза.

Этот обзор является ключевым для среды ИТ-операций, потому что инициирует жизненный цикл инвестирования для развертывания данного релиза.

9. Командная модель MOF

Обзор

Командная модель MOF предлагает гибкий набор директив по организации команд эффективного использования ИТ. Важным аспектом Командной модели MOF является применимость к распределенным командам, управляющим распределенными средами.

Командная модель MOF основана на знании, что операционная команда должна достигать некоторого числа качественных ключевых целей. Структура Командной модели состоит из шести основных категорий задач. Важно понимать, что структура представляет собой группы задач,

служащих одной цели. Они не являются видами работ, и они не подразумевают организационную диаграмму в каком-либо виде.

Командная модель MOF описывает ключевые задачи и компетенции каждой части структуры, как сравнить группы различного размера и типа организации (какая комбинация ролей работает хорошо, а какая – нет) и руководящие принципы для успешного выполнения и использования распределенных вычислительных сред на платформе Microsoft.

Командная модель MOF предназначена, чтобы применять Модель процессов MOF к любой ИТ-среде. Структура Командной модели связана с SMF модели процессов; эта связь помогает установить, какие роли отвечают за какие задачи, вне зависимости от существующей организационной структуры.

Руководящие принципы
Командная модель MOF основана на принципе, что роль не является функцией. В пределах этой модели роли представляют объединения возможностей, которые могут быть представлены несколькими способами: индивидуально, функциональными группами или компетентными центрами.
Вне структуры и ответственности Командная модель MOF представляет несколько принципов для эффективных операционных групп ИТ:

- Удовлетворение клиентов также важно, как и все ИТ-роли;
- Хорошие ИТ-команды понимают бизнес-приоритеты, и хорошие ИТ способствуют бизнесу;
- Средства управление ИТ-автоматизацией и знаниями очень полезны для обеспечения высокого уровня Сервисов;
- Привлечение и удержание лучших людей необходимы для построения сильной ИТ операционной команды.

В центре графического представления Командной модели MOF и находится ключевое для эффективности общение. Недостаточное общение среди ИТ операционных групп может привести к таким проблемам, как недопонимание, раздробленность и повышение риска. Командная модель MOF поддерживает множество механизмов общения, включая регулярные совещания сотрудников, назначенных на роли, и проектных команд, отчеты о статусе и статистические отчеты.

Ролевой кластер	Цель качества
Релиз	Эффективное управление релизами и изменениями. Тщательное инвентарное прослеживание всех ИТ-Сервисов и систем.
Инфраструктура	Управление физической средой и

	оборудованием инфраструктуры.
Поддержка	Качественная поддержка клиента и культуры Сервисов.
Функционирование	Предсказуемое, повторяющееся и автоматизированное управление системой.
Партнерство	Взаимовыгодные отношения с обслуживаемыми и снабжающими партнерами.
Безопасность	Защищенное корпоративное имущество, контролируемая авторизация, проактивное планирование безопасности.

Цели качества
С каждым ролевым кластером связана специфическая цель качества. Эти цели нацелены на то, чтобы помочь командам определить их миссии и формы их деятельности. Эти цели качества описаны ниже:

Приложение Командной модели MOF может меняться организацией и командами. ИТ-организация осуществляет аспекты модели различными способами, в зависимости от размера кластера, границ системы, географического положения, доступности для команды ресурсов и специализации и навыков персонала. Число людей, представляющих каждую роль, может также варьироваться. В маленьких ИТ-организациях один человек вполне может совмещать сразу несколько ролей, а в больших одну роль может выполнять целая команда.

Ролевой кластер Релизов

Обзор
Ролевой кластер релизов служит простейшей связью между командой, разрабатывающей проект, и группами использования. Релиз затрагивает SMFs управления конфигурациями, управление релизами и управление изменениями. Релиз служит для улучшения и оптимизации процесса издания, предохраняя его, делая его исправимым и хорошо автоматизированным. Роль релиза в Командной Модели MOF непосредственно связана с управлением релизами Командной модели MSF. Это то место, где осуществляется переход от разработки/тестирования к производству/использованию, и оно же является основной точкой соединения для гладкого перехода от системы к производству.

Некоторые функции команд, относящихся к ролевому кластеру релизов, включает в себя:

- Управление изменениями;
- Системная инженерия и инженерия релизов;
- Управление настройками/имуществом конфигурации;

- Распределение и лицензирование программного обеспечения;
- Гарантия качества.

Обязанности

- Выступать в роли простейшей связи между командой, разрабатывающей проект, и группами использования.
- Управлять процессом изменений и работать с CAB и исполнительным комитетом.
- Идентифицировать, контролировать изменения и докладывать о состоянии системы и среды.
- Управлять CMDB и DSL.
- Управлять выбором и оптимизацией оборудования, относящегося к релизу.
- Вести Обзор Управления операциями готовности релиза.

Ролевой кластер Инфраструктуры

Обзор

Роль инфраструктуры состоит в том, чтобы обеспечить согласованное соответствие требованиям сети, коммуникаций, оборудования и программного обеспечения. Позиции в пределах этого ролевого кластера часто относятся к «инженерии инфраструктуры».

Инфраструктура отвечает за выбор и управление фундаментальными элементами, на которые полагаются приложения, включая программное обеспечение системного уровня, программное обеспечение управления системой, программное обеспечение управления сетями, межплатформное программное обеспечение и программное обеспечение безопасности. Инфраструктура также несет ответственность за управление общими данными, такими как клиентская или производственная информация, планирование пространства и хранения (центры данных, пространственные и удаленные офисы, тестовые лаборатории, лаборатории разработок) и оборудование, необходимое для поддержки инфраструктуры.

Инфраструктура работает в тесной связи с возможностями групп по планированию и координированию строительства и переезда офисов, расширением и приобретением, изменениями физической среды и другими событиями, для обеспечения того, что все ИТ-требования спланированы и документированы. В больших предприятиях инфраструктура часто включает в себя организацию и управление ИТ-политикой и процедурами, методологией, стандартами, такими как рабочее и серверное оборудование, распределенная вычислительная техника, обеспечивающая подключение и ресурсы для дистанционной работы, и техники для управления затратами. При возрастающем

использовании «виртуальных предприятий» многие опции работы «когда угодно и где угодно» должны быть технологически понятны и поддержаны.

Управление затратами ИТ-Сервисов является сложной и часто недооцениваемой функцией. При этом хорошо помогает специально предназначенная группа, которая определяет, каким образом затраты измеряются, прослеживаются и докладываются, и затем использует эту информацию для планирования и составления бюджета. Надежная, понятная информация от этой группы оказывает существенное влияние на другие SMFs.

Роль инфраструктуры работает в тесной связи с ролевыми кластерами поддержки и функционирования, обеспечивая эффективное развитие инфраструктуры и эффективное развертывание. Эти общие усилия допускают поддержку и действия, необходимые для разработки стабильного процесса гладкого функционирования решений для инфраструктуры.

Обязанности

- Согласование ИТ-инфраструктуры с требованиями бизнеса.
- Координирование физической среды планирования и функционирования (например, центры информации, лаборатории, филиалы).
- Разработка и документирование политики, процедур, методологии и стандартов управления инфраструктурой.
- Построение серверов и рабочих станций.
- Обеспечение отчетности по затратам и возмещению для управления и клиентской, основанной на установленных затратах/возмещении политики.

Ролевой кластер Поддержки

Обзор

Роль поддержки включает в себя функции Службы Поддержки, управления инцидентами и управления проблемами. Целью поддержки является обеспечение своевременной, тщательной и эффективной поддержки клиентов. Поддержка является ключевой не только для внутренних пользователей (служащих) корпоративных ИТ-Сервисов, но и для внешних клиентов продуктов и Сервисов компании, обычно относящихся к производственной и технической поддержке. Так как Служба Поддержки является первоначальным контактом с сообществом пользователей, на основе существующего интерфейса пользователи понимают качество ИТ-Сервисов.

Наиболее важной целью ролевого кластера поддержки является обеспечение своевременной, эффективной и тщательной поддержки клиента. План укомплектования персоналом Службы поддержки требует обеспечения пропорциональной зависимости количества поддерживаемого персонала от требований поддержки в периоды как пиковой, так и незначительной загруженности. Это помогает удерживать вспомогательные расходы при эффективной работе команды Службы поддержки и минимизирует время реакции на инциденты, таким образом, поддерживая цели, определенные в Соглашении об Уровнях Сервиса.

Устройства автоматизации дают возможность для персонала службы поддержки расставить приоритеты в их рабочей загрузке по инцидентам, основываясь на важности и влияния проблемы на бизнес. Эти устройства автоматизации поддержки также обеспечивают возможность отчитываться по таким составляющим успеха, как время реакции, количество инцидентов по данной проблеме и так далее. Каждый инцидент, в конце концов, может быть отнесен к проблеме для решения, и команда управления проблемами для этой производственной среды может определять базовую причину инцидента. Практически это приведет к сокращению числа инцидентов и проблем. Существенные инциденты или группы инцидентов могут обозреваться процессом управления проблемами, и решение будет принято в случае, если будет обоснована регистрация проблемы, и произведен необходимый анализ базовых причин.

Статистика показывает, что более 50 процентов запросов в Службу Поддержки является вопросами типа «Что мне делать?», обычно означающими, что пользователю требуется большая подготовка к работе с данным продуктом или направление к месту нахождения документации, содержащей в себе необходимую информацию. Лучшим практическим методом для наиболее эффективной Службы Поддержки является наличие проактивного хранилища информации по самостоятельной помощи, в виде часто задаваемых вопросов (FAQ) по телефонной линии или Web-сайта, содержащего ответы на наиболее распространенные звонки в Службу поддержки. Эти ресурсы могут помочь пользователю решить свои проблемы без обращения в Службу Поддержки, тем самым, сохраняя и время, и деньги каждого из участников и увеличивая удовлетворенность и знания пользователя в одно и то же время.

Для звонков, которые все-таки достигают Службы Поддержки, непрерывный процесс обратной связи Службы поддержки с соответствующей организацией, подготавливающей пользователя, обеспечивает обучающейся группе своевременную и релевантную

информацию по тому, какие области производят наибольшее количество инцидентов Службы Поддержки.

Некоторые из функциональных групп, относящихся к ролевому кластеру поддержки, включают в себя:

- Службу Поддержки / help desk / управление инцидентами;
- Производство / поддержку производства;
- Управление проблемами;
- Соглашение об Уровнях Сервиса.

Обязанности

- Обеспечивать элементарную связь между командой, разрабатывающей проект, и группами использования.
- Обеспечивать выполнения Соглашения об Уровнях Сервиса.
- Нести ответственность и управлять инцидентами, проблемами и Сервисными запросами.
- Автоматизация управления инцидентами и проблемами при помощи необходимых средств.
- Отчитываться за действия по поддержке.
- Обеспечивать обратную связь группам разработки и развития.

Ролевой кластер Функционирования

Обзор

Роль функционирования включает в себя квалифицированных специалистов, которые фокусируются на технических областях и задачах производственных систем, необходимых для работы бизнеса на ежедневной основе. Целью ролевого кластера функционирования является обеспечение выполнения обязательств, закрепленных в SLA.

Роль использования включает в себя каждодневные действия по использованию и администрированию систем, необходимые для выполнения и поддержки ИТ-Сервисов и приложений в пределах предприятия. Роль функционирования представляет составленный повторяющийся процесс, такой как резервное копирование, архивация и хранение данных, управление производством, мониторинг систем и управление регистрацией событий и управление серверами файлов и печати.

Обязанности

- Контролировать отчетность и системные настройки; создание и управление сообщениями и авторизацией пользователей.
- Нести ответственность за передачу сообщений, использование телекоммуникаций и сетей.

- Нести ответственность за администрирование систем и пакетную обработку.
- Отвечать за Сервисные приложения.
- Управлять брандмауэрами и администрировать безопасность.
- Объединять host-Сервисы.
- Нести ответственность за администрирование служб каталогов.

Ролевой кластер Партнерства

Обзор

Роль партнерства управляет обширным набором ИТ-партнеров, снабжающих партнеров и аутсорсеров, которые работают в качестве виртуальных членов персонала при предоставлении оборудования, программного обеспечения, сетей, хостинга, возможностей и поддержки Сервисов. Способ, которым ИТ-организация использует Сервисы партнеров, изменяется от бизнеса к бизнесу в широких пределах в зависимости от размера, размещения, типа отрасли и стратегических целей бизнеса. Рассматривая эволюцию е-бизнеса, внешние партнеры могут быть основными владельцами или поставщиками технологий.

Некоторые из функциональных групп, относящихся к ролевому кластеру партнерства, включают в себя:

- Поддержка продавцов.
- Поддержку окружения.
- Управляемые Сервисы аутсорсеров и торговых партнеров.
- Оборудование и программное обеспечение от снабжающих партнеров.

В Командной Модели MOF роль партнерства представляет точные партнерские взаимоотношения с внешним бизнесом, имеющие отношения к доставке Сервисов. Точный тип и природа взаимоотношений с партнером могут приобретать различные формы и перспективы; как бы то ни было, структура не должна быть недооцененной.

Определенные уровни Сервиса и связанные метрики являются неотъемлемой частью Подкрепляющих контрактов, необходимой, для того чтобы управлять высококачественными Сервисами, которые получаются от продавцов, снабжающих партнеров, аутсорсеров или любых других поставщиков. Менеджер по работе с крупными заказчиками партнера отвечает за определение терминов этих соглашений, затрат и деталей использования, относящихся одновременно и к поставщику-партнеру, и к получателю-клиенту для достижения их требований к соглашению.

Обязанности

- Управлять взаимоотношениями между ИТ-продавцами и партнерами-аутсорсерами.
- Контролировать эффективность поставщика Сервисов.
- Договариваться и управлять затратами поставщика.
- Создавать и управлять Подкрепляющими контрактами и SLAs между поставщиками и клиентами.
- Определять роли, обязанности и взаимодействия между поставщиками и пользователями.
- Оценивать выбор третьих сторон.
- Управлять функциями ИТ-поставок и покупок.

Ролевой кластер Безопасности

Обзор

Роль безопасности является очень важной, так или иначе, во всех ИТ-действиях, особенно в электронном бизнесе. Информационная система со слабой защитной основой со временем будет испытывать трудности, связанные с дырами в безопасности. Ролевой кластер безопасности обеспечивает конфиденциальность, целостность и доступность данных.

Некоторые из функциональных групп, относящихся к ролевому кластеру безопасности, включают в себя:

- Защиту интеллектуальной собственности.
- Антивирусную защиту.
- Безопасность сетей и систем.
- Планирование действий при непредвиденных обстоятельствах.

Архитектура информационной безопасности расширяет границы между корпоративным бизнес-процессом, директивами политики и измерениями безопасности со спецификацией по платформам. Другой обязанностью роли ИТ-безопасности является создание всестороннего плана аудита, сохранения, классификации и безопасной передачи данных.

Обязанности

- Содействовать в мониторинге корректного использования ИТ-ресурсов.
- Выявлять вторжения и защищать от вирусов и атак.
- Определять политику сохранения и безопасного размещения данных.
- Определять политику и процедуры безопасной поддержки.
- Разрабатывать и управлять эффективной безопасностью сети.
- Прослеживание и отчетность по аудиту.

Роли групп в пределах квадрантов Модели Процессов

Роли в пределах Командной Модели MOF и их функции во всеобщем жизненном цикле управления Сервисами согласуются по квадрантам с Моделью Процессов MOF. Квадранты Процессной Модели являются параллельными, но не совпадающими, поэтому составные роли могут быть (часто так и происходит) включены в каждый квадрат в зависимости от группы и системы. Каждая роль может также принимать участие более чем в одном квадранте в одно и то же время, если эта роль включена в управление Сервисами составных систем. Следующая диаграмма показывает на высоком уровне, как роли MOF приблизительно сопоставляются с четырьмя секторами Модели процессов MOF.

10. Модель Рисков MOF

Обзор

Модель Рисков MOF представляет собой пятиступенчатый процесс проактивного определения и управления рисками в ИТ-операциях. Риск определяется как возможность болезненной потери. В отношении ИТ потенциальные потери включают в себя потери Сервиса или данных, бреши в системе безопасности или неудачи в достижении и поддержании согласованных уровней Сервиса для клиентов.

Включение Модели Рисков в статусе центральной модели MOF является реакцией на увеличение важности ИТ-Сервисов и потенциально враждебного влияния при разрушении этих Сервисов. Модель Рисков MOF обеспечивает структуру управления рисками, которая может быть интегрирована в другие процессы ИТ-операций.

Модель Рисков MOF основана на Модели Рисков MSF. Так же, как и в MSF, Модель Рисков MOF характеризуется расширением и индивидуализацией, которые делают ее более подходящей для управления рисками, свойственными для ИТ-операций.

Зависимость бизнеса от ИТ-сервисов приводит к тому, что эти сервисы становятся большими источниками риска для бизнеса: неудачи в ИТ-среде все чаще могут вызвать сбои в бизнесе в целом. Кроме того, сегодня ИТ-окружение включает «пунктов неудач» больше, чем раньше. Растет число компьютеризированных рабочих мест, серверов, соединений, интерфейсов систем и сквозных Сервисов. Из-за постоянного усложнения и разнородности среды ИТ-окружение оказывает большее влияние на бизнес, чем раньше, и одновременно бизнес все больше зависит от ИТ-Сервисов.

Характеристики Рисков

Модель Рисков MOF имеет следующие характеристики, свойственные всем рискам:

- Неопределенность (например, «когда этот диск откажет?») в ИТ создает вероятность болезненной потери, так называемый риск.
- Риск является только вероятностью болезненной потери.
- Риск является не чем-то плохим, чего следует избегать, но тем, чем можно управлять, проактивно идентифицировать и направлять.

Принципы Успешного Управления Рисками

Основным принципом Модели Рисков MOF является проактивное управление рисками.

Модель Рисков MOF поддерживает следующие принципы в управлении рисками:

1. *Управление рисками является непрерывным процессом* - Группам ИТ использования следует всегда искать новые риски и согласованно переоценивать существующие.
2. *Управление рисками должно быть частью каждой роли и функции* - Управление рисками является не отдельной ролью или функцией, а всеобщей обязанностью. Поэтому управление рисками должно быть частью работы каждого.
3. *Идентификация рисков является позитивным явлением* - Идентификация рисков может доставлять неудобство ИТ-персоналу, однако, эта мера помогает предотвратить потенциальную опасность и является позитивным шагом вперед. Поэтому успешное управление рисками требует среду, в которой риски могут быть идентифицированы, без опасения сотрудника быть раскритикованным или наказанным.
4. *Выполнение действий, связанных с рисками должно быть тщательно спланировано* - Процедуры и изменения, связанные с высоким риском, логично осуществлять раньше прочих.
5. *Управление рисками должно сохранять баланс между формальностью и гибкостью* - Слишком формализованный процесс управления рисками наверняка будет обойден, обманут, в то же время слишком большая гибкость также не даст хороших результатов. Ключом является равновесие между этими двумя характеристиками, что обеспечит согласованность приложений и приведет к удовлетворительному результату.

Эти принципы можно объединить в термин «проактивный». Группа, которая практикует проактивное управление рисками, сознает, что риск является нормальной частью операций, и вместо того, чтобы игнорировать риски, рассматривает их как возможность обезопасить

будущее. Члены команды демонстрируют проактивное поведение, когда принимают видимый, измеримый, повторяющийся, непрерывный процесс, при помощи которого они оценивают риски, возможности, и совершают действия, исследуя базовые причины, словно симптомы болезни.

Процесс Управления Рисками

Процесс представлен в виде следующих шагов:

1. *Идентификация* - Этот шаг обеспечивает возможности, сигналы и информацию, которые позволяют группе устранять основные риски до того, как они неблагоприятно повлияют на операции и, следовательно, на бизнес. Группа идентифицирует состояния, источники и модели сбоев, относящиеся к этому риску.
2. *Анализ* - На данном этапе группа переводит информацию, полученную на шаге идентификации, в информацию, способствующую принятию решения. Она включает в себя вероятность риска, влияние и воздействие.
3. *Планирование действий* - На этом шаге группа превращает информацию о рисках в решения и действия. Планирование включает в себя развитие действий для направления индивидуальных рисков, расстановки приоритетов действий, относящихся к каждому риску, и создание интегрированного плана управления рисками. Ключевые задания в пределах данного шага состоят из определения еще трех элементов риска: смягчение, триггеры и соприкосновение.
4. *Отслеживание* - Группа собирает информацию о том, как изменяются риски, чтобы поддержать решения и действия, которые будут сделаны на следующем шаге (контроле). Группа наблюдает изменения инициированных значений, состояние, последствия, вероятность и влияние, а также наблюдает за прогрессом в планировании смягчения.
5. *Контроль* - Группа собирает информацию о риске с предыдущего шага (отслеживания) и, когда что-нибудь меняется, они реагируют запланированным на этапе контроля для этого изменения образом. Эти реакции могут включать в себя планирование действий при непредвиденных обстоятельствах, уход от риска, дополнительный анализ риска или пересмотр плана смягчения.

Эти пять этапов снабжают информацией три списка рисков:

- Список основных рисков.
- Список максимальных рисков.
- Список удаленных рисков.

Эти списки описаны ниже.

Список основных рисков
В течение каждого шага процесса группа собирает информацию об отдельных рисках и добавляет эту информацию в список основных рисков. Каждый последующий шаг строится на предыдущем при помощи добавления новых элементов рисков или использования уже существующих, что облегчает принятие решения. К примеру, на шаге анализа добавляется информация о влиянии рисков и их вероятность. Процесс является циклическим, поэтому будущие проходы на шаге анализа могут содержать обзор, исправление оценок их влияния и вероятности. Примечательно, что размер списка основных рисков является скорее индикатором тщательности работы, чем индикатором жизнеспособности и стабильности группы.

Список максимальных рисков
Управление рисками требует времени и усилий, отличных от каждодневной деятельности, поэтому для группы важно сохранять баланс между накладными и ожидаемыми расходами управления рисками. Обычно это означает определение небольшого числа основных рисков, более других заслуживающих времени и ресурсов группы.

Можно считать список основных рисков приоритетным, а максимальные риски – наиболее важными для активного управления, составляющими отдельный список рисков. Размер этого списка может варьироваться как между ИТ-группами, так и в пределах одной группы.

Список удаленных рисков
Список основных рисков содержит все риски, которые группа идентифицировала, как наиболее важные, чтобы быть занесенными в список максимальных рисков. Некоторые из этих рисков никогда не исчезают, например, риски, связанные с природным фактором. Другие в определенный момент перестают быть релевантными. К примеру, группа может свести вероятность риска к нулю. Или же источник риска может покинуть среду. Таким образом, риски, относящиеся к устаревшему программному обеспечению, не являются релевантными, как только приложение перестает использоваться.

Когда бы риск ни стал нерелевантным, его переносят из списка основных в список удаленных рисков. Этот список служит исторической справкой, при помощи которой группа может сокращать риски в будущем. К примеру, если группа уже отслеживала риски, относящиеся к процессам службы поддержки, а затем ее функции стала выполнять аутсорсинговая компания, то некоторые из тех рисков могут быть убраны. Если функции службы поддержки позже возобновятся, группе придется руководствоваться списком удаленных рисков. Также люди могут

использовать этот список для консультации в качестве отсчетной точки идентификации новых рисков. Наконец, если группа снизит вероятность риска или влияния до нуля, то замечания о том, что было для этого предпринято, может помочь тем, кто столкнется с похожими рисками.

Шаг 1: Идентификация Риска

Идентификация риска является первым шагом в процессе проактивного управления рисками. Она обеспечивает благоприятные возможности, сигналы и информацию, которые позволяют группе устранять основные риски до того, как они неблагоприятно повлияют на операции и, следовательно, на бизнес.

На этом шаге группа определяет компоненты изложения риска:

- Состояние
- Последствия для функционирования
- Последствия для бизнеса
- Источник риска
- Вид сбоя

«Интуитивный путь обсуждения будущих изложений».
Состояние является частью «если» изложения, а последствия - частью «то».

Существует четыре основных источника рисков в ИТ-операциях:

- *Люди* - Человеческие ошибки.
- *Процесс* - Поврежденный или плохо документированный процесс.
- *Технология* - Проблемы с оборудованием, программным обеспечением и так далее.
- *Внешние* - Факторы, которые выходят из-под контроля ИТ-групп.

Существует четыре основных пути, по которым ИТ-использование может дать сбой в бизнесе:

- *Затраты* - Инфраструктура не может работать должным образом, при слишком высоких затратах, вызванных слишком малой окупаемостью инвестиций.
- *Быстрота* - Инфраструктура может работать должным образом, но не способна изменяться так быстро, как этого требует бизнес.
- *Производительность* - Инфраструктура не может достичь уровня ожиданий пользователя.
- *Безопасность* - Инфраструктура может дать сбой в бизнесе, если не обеспечена достаточная защита данных и ресурсов или установлен такой уровень безопасности, при котором даже авторизованный пользователь не сможет получить доступ к данным и ресурсам.

До того момента, как группа сможет управлять риском, его суть должна быть четко изложена.

Шаг 2: Анализ Риска

Анализ риска основан на переводе информации, полученной на шаге идентификации, в информацию, способствующую принятию решения. На шаге анализа группа добавляет еще три элемента внесения риска в список основных рисков:

- *Вероятность риска* - Вероятность того, что состояние того, что событие произойдет, будет достигнуто.
- *Влияние риска* - Измерение силы негативного воздействие или размера потерь, вызванных последствиями.
- *Незащищенность от рисков* - Результат умножения вероятности на влияние. Риски, имеющие высокую вероятность и оказывающие сильное влияние, являются одними из наименее управляемых, и потому имеющие высокую степень незащищенности.

Шаг 3: Планирование Действий, связанных с наступлением рисков

На шаге планирования информация о рисках превращается в решения и действия. Планирование включает в себя развитие действий для направления индивидуальных рисков, расстановки приоритетов действий, относящихся к каждому риску, и создание интегрированного плана управления рисками.

Ключевой задачей в пределах этого шага является определение еще трех элементов риска:

- *Смягчение* - Шаги, предпринимаемые группой до того, как событие произойдет, и каждый имеет один из трех влияний на риск:
    - Уменьшение – Минимизация вероятности риска, или его влияния, или того и другого.
    - Избежание – Предотвращение совершения командой действий, при которых выгоды не оправдывают незащищенность.
    - Перенос – Оставление риска нетронутым, передавая ответственность за него другой группе.
- *Триггеры* - Индикаторы, показывающие группе, что событие вот-вот произойдет или уже произошло, поэтому пора переходить к плану «действий в непредвиденных обстоятельствах».
- *Соприкосновение* - Шаги, предпринимаемые группой, когда событие происходит, или триггер становится истиной.

Шаг 4: Отслеживание Рисков

В течение этого шага, группа собирает информацию об изменениях рисков, чтобы поддержать решения и действия, которые будут сделаны на следующем шаге (контроле). Это шаг следит за тремя основными изменениями:

- Значениями триггеров.
- Состоянием, последствиями, вероятностью и влиянием рисков.
- Прогрессом в плане смягчения.

Этот шаг следит за основными изменениями в трех основных временных рамках:

- Постоянно.
- Циклически.
- Для конкретного случая.

Для обзоров использования, группе следует знать основные риски и состояние действий управления рисками.

Шаг 5: Контроль Рисков

Группа собирает информацию о риске с предыдущего шага (отслеживания) и, когда что-нибудь меняется, они реагируют запланированным для этого изменения образом на этапе контроля:

- Если значение триггера является истиной, запустить план «действий в непредвиденных ситуациях».
- Если риск перестал быть релевантным, удалить его.
- Если состояние или последствия изменились, перенаправить на шаг идентификации для переоценки этого элемента.
- Если вероятность или влияние изменились, перенаправить на шаг анализа для обновления.
- Если шаг смягчения не появляется на отслеживании, перенаправить на шаг планирования для обзора и проверки плана.

Отношение Модели Рисков с MOF

Модель Процессов определяет набор SMFs и четыре этапа обзора, которые обеспечивают операционное внедрение в ИТ-инфраструктуру. Командная Модель состоит из набора ролевых групп команд использования, эффективно поддерживающих операционный процесс. Модель Рисков управляет рисками, свойственными ИТ-операциям.