

Аудит в ИТ

Захар Кириллов, MSc
zahhar@gmail.com

Mainori Kõrgkool
2010

Организационные вопросы

- 4 встречи по 6 часов
 - 3.10, ???, 28.11, 17.12
- Экзамен - дата уточняется
 - 50% - тест в Moodle
 - 50% - защита и обсуждение домашней работы
- Домашняя работа
 - Проведение аудита в организации :)
 - Если нет организации – доклад (реферат) по малоизученной теме курса

Темы курса

- *IT Governance (IT valitsemine)*
- Стандартизация в ИТ
- Аудит: терминология, принципы, методики
- Фреймворки ISKE, COBIT и ITIL
- Планирование, проведение и документирование аудита, представление и обсуждение результатов

Ожидаемые результаты

- Понимать философию *IT governance*
- Знать терминологию аудита в ИТ, роли участников, их цели и задачи
- Ориентироваться в существующих отраслевых стандартах, в т.ч. COBIT и ITIL
- Уметь поэтапно планировать и проводить аудит, предоставлять его результаты

Как можно применить знания курса аудита в ИТ?

- **Свой бизнес в области консалтинга, разработки ПО, ...**
- **При устройстве на работу**
 - на должность руководителя по ИТ (IT juht)
 - в аудиторские фирмы (KPMG, Deloitte, PWC, Ernst & Young)
- **Устроившись в организацию "айтишником"...**
 - и оказавшись в ней единственным (для знакомства с организацией и управления её ИКТ)
 - и попав в большой коллектив (100+) большой организации
- **Не в ИТ-сфере: для внедрения новых технологий**
- **Чтобы не остаться без работы в случае...**
 - недальновидного начальства, самодуров, "гидры"
 - внешнего ИТ-аудита, желающего вас "разоблачить"

Что читать самостоятельно?

- Никлас Карр: Блеск и нищета ИТ
- Билл Гейтс: Дорога в будущее; Бизнес со скоростью мысли
- Фредерик Брукс: Мифический человеко-месяц
- Что-нибудь несложное про ITIL и COBIT (например, "ITIL at a Glance" или "COBIT for Dummies" – google it :)

IT governance

Strategy & Business Alignment

Organization

Projects

Processes

**Human
Resources**

**Information
Systems**

Infrastructure

**Financial
Resources**

Что такое IT governance?

- *В двух словах: как внедрить использование ИКТ с максимальной пользой для бизнеса?*
- тесная интеграция ИКТ с бизнес-процессами, целями и задачами организации
- использование ИКТ для поддержки бизнеса
- управление качеством и производительностью в ИКТ
- риск-менеджмент

Проблемы использования ИКТ в бизнесе

- Руководители "верхнего уровня" зачастую некомпетентны в ИКТ, вследствие чего...
 - Пытаются рулить ИТ сами: инвестиции, выбор и внедрение технологий, обучение сотрудников
 - Делегируют руление ИТ "сисадминам и программистам" (без обид! :)
- Результаты
 - Нерациональная трата ресурсов (все занимаются ерундой и тратят много денег зря)
 - Начальство ругает и меняет "айтишников"

Как должно быть в идеале?

Каждая сторона вносит посильный вклад в рамках своей компетенции для управления ИКТ

Руководство (совет директоров)

Финансовый отдел (бухгалтерия)

Все внутренние потребители ИКТ-услуг

Отдел ИКТ (сисадмины и программисты)

Цели *IT governance*

- Гарантировать целенаправленное использование выделенных на развитие и поддержку ИКТ ресурсов
- Сделать возможным не только измерение расходов на ИКТ, но и измерение достигнутых при их помощи доходов или экономии
- Учесть имеющиеся риски и минимизировать негативные последствия в случае возникновения внештатных ситуаций

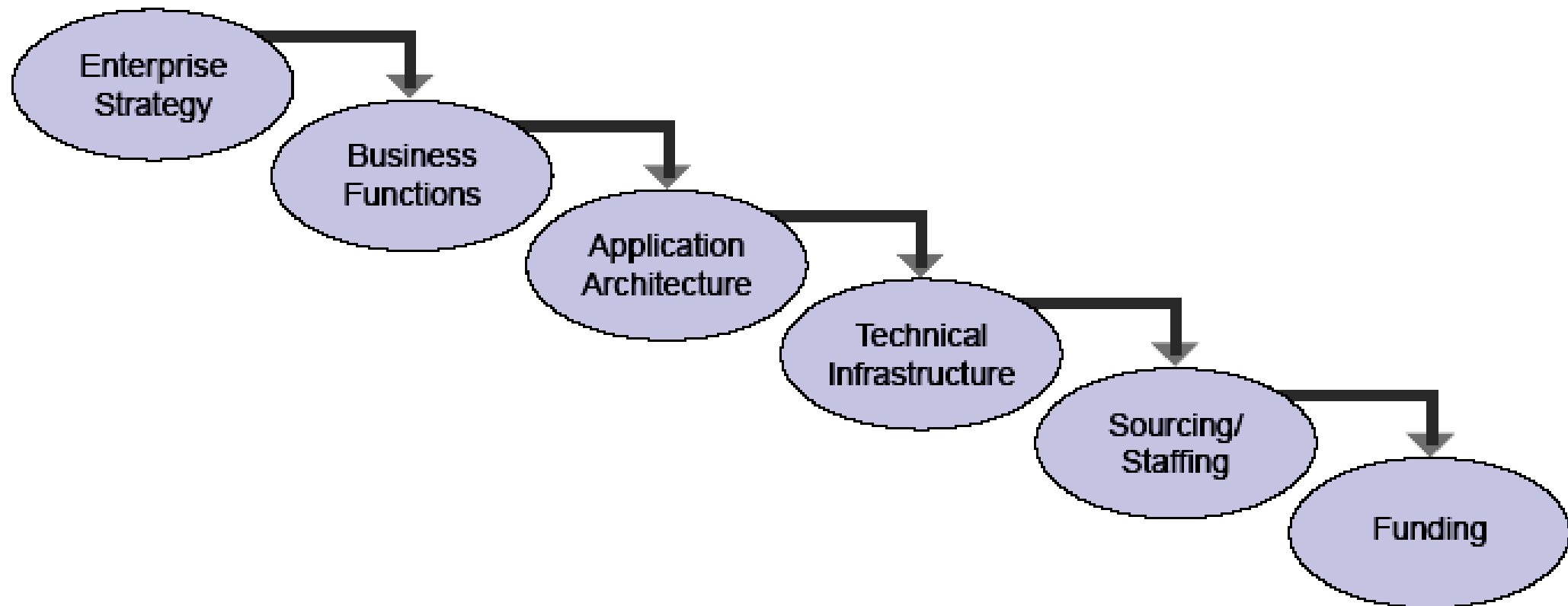
Как же добиться эффективности?

- Прекратить считать ИКТ чьей-то блажью
- Составить бюджет и действовать в его рамках
- Определить ответственных за каждый элемент ИТ-инфраструктуры
 - Движение информации в организации
 - Правила, стандарты, политики
 - Пользователи (права и обязанности)
 - Технологии (приложения, оборудование)

Из чего состоит IT Governance?

- Asset Management - имущество
- Security Assessment - безопасность
- Portfolio Management - инвестиции
- Enterprise Architecture - архитектура
- Project Management - проекты
- Service Management - услуги

Как включить ИКТ в поддержку стратегических целей организации?



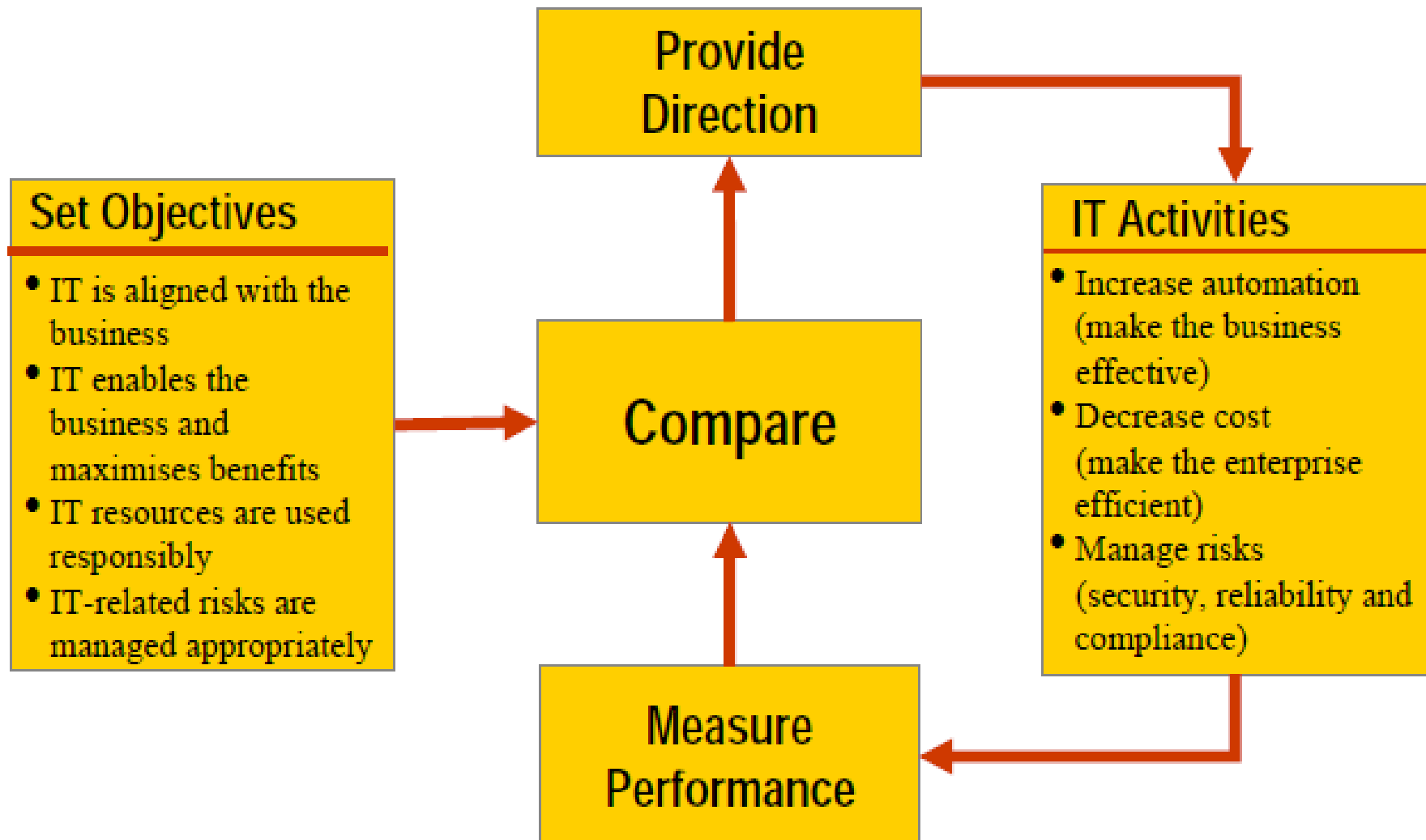
Для чего усложнять?

- Использование ИКТ становится критичным в конкурентной борьбе даже не в ИТ-отраслях
- Ожидания от ИТ расходятся с реальной их отдачей (забивание гвоздей микроскопом)
- ИТ живёт своей жизнью
- Инвестиции в ИТ не обоснованы потребностями организации в ИКТ услугах
- В случае форс-мажора нет ответственных или же отвечают за всё только "айтишники"

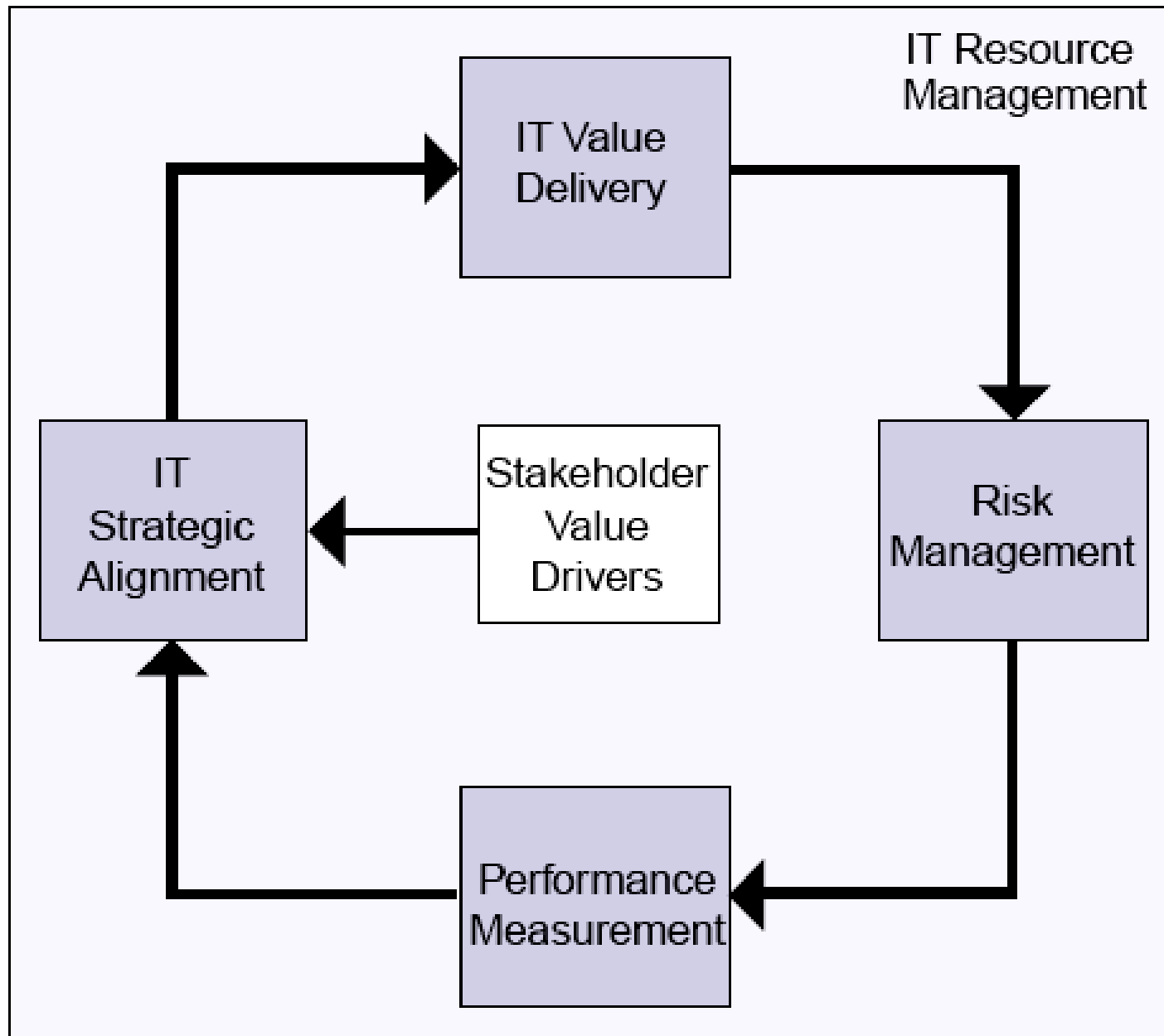
Что должно получиться?

- ИКТ тесно интегрированы в бизнес-процессы (а не существуют отдельно в подвале организации, как герои сериала IT Crowd)
- Все знают, чем и для чего занимаются ребята из отдела ИТ
- Расходы на ИКТ запланированы исходя из бизнес-целей и контролируются
- Риски, связанные с использованием (или неиспользованием) ИКТ учтены и организация способна реагировать в случае форс-мажора

Каркас для IT Governance



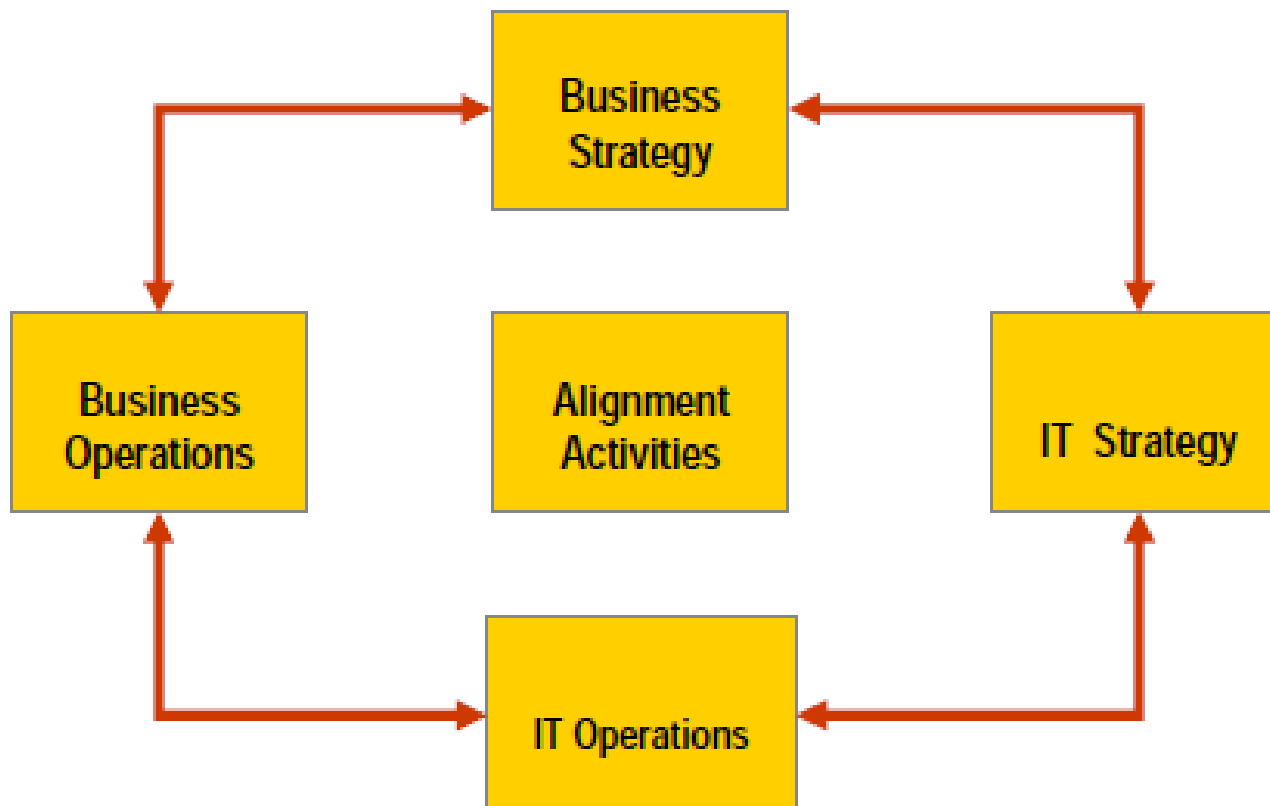
Цикл развития IT Governance (1/2)



Цикл развития IT Governance (2/2)

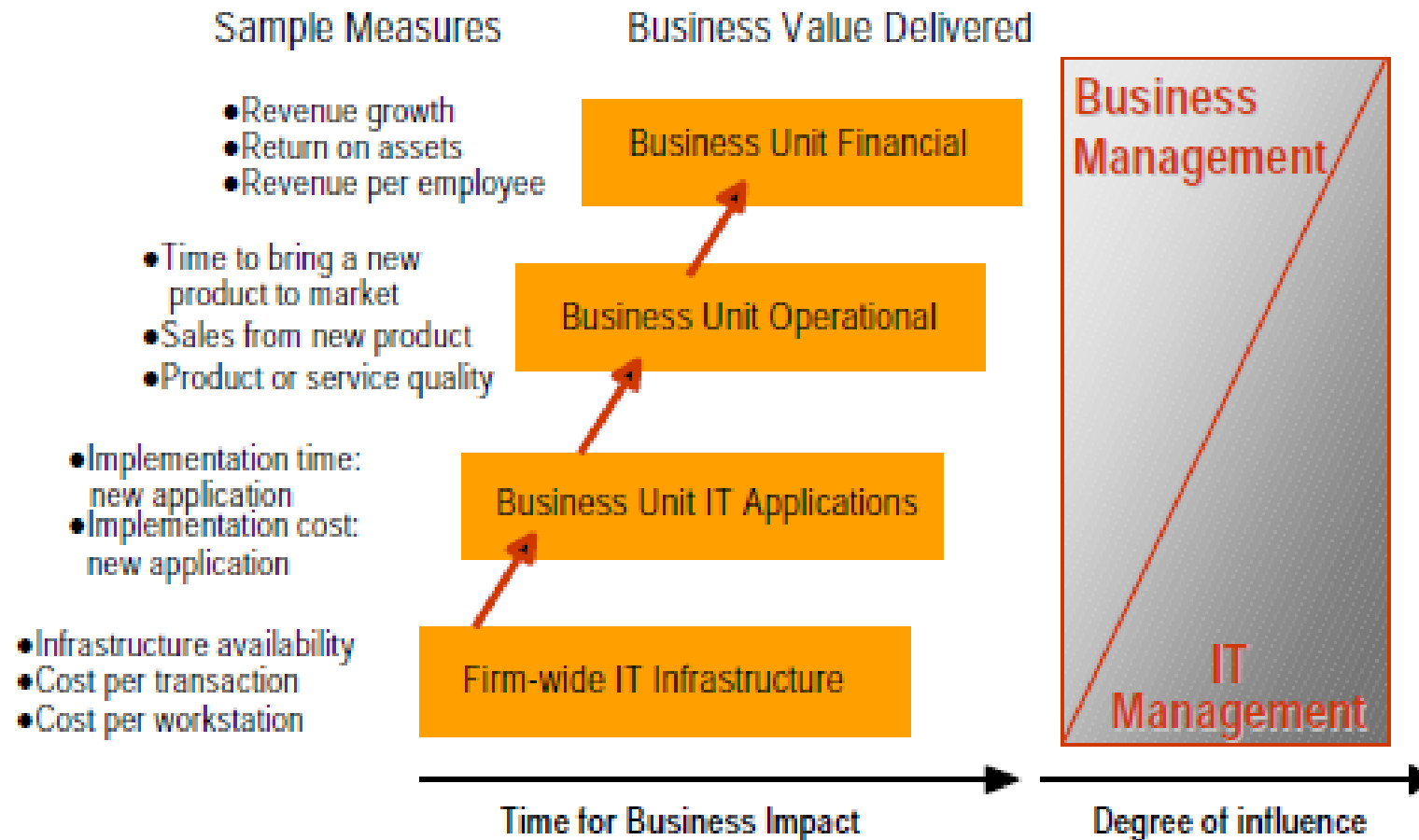
- *Stakeholder Value Drivers* – руководство (владельцы) организации определяют, какой отдачи (от бизнеса) они хотят?
- *IT Strategic Alignment* – проекция бизнес-целей на ИКТ: чем ИКТ могут помочь?
- *IT Value Delivery* – пытаемся помочь, оставаясь при этом в рамках бюджета :)
- *Risk Management* – обеспечиваем работоспособность и отказоустойчивость
- *Performance Measurement* – оцениваем эффективность внедренных решений

Проекция бизнес-целей на ИТ



- Проекция – это процесс (постоянное, повторяющееся действие)
- Необходимо выполнять каждый раз после корректировки или изменения бизнес-целей

Заставляем ИТ помогать бизнесу



- Начальство оценивает результат субъективно
- Хотя у нас есть объективные показатели
- Из которых сложно извлечь влияние ИТ

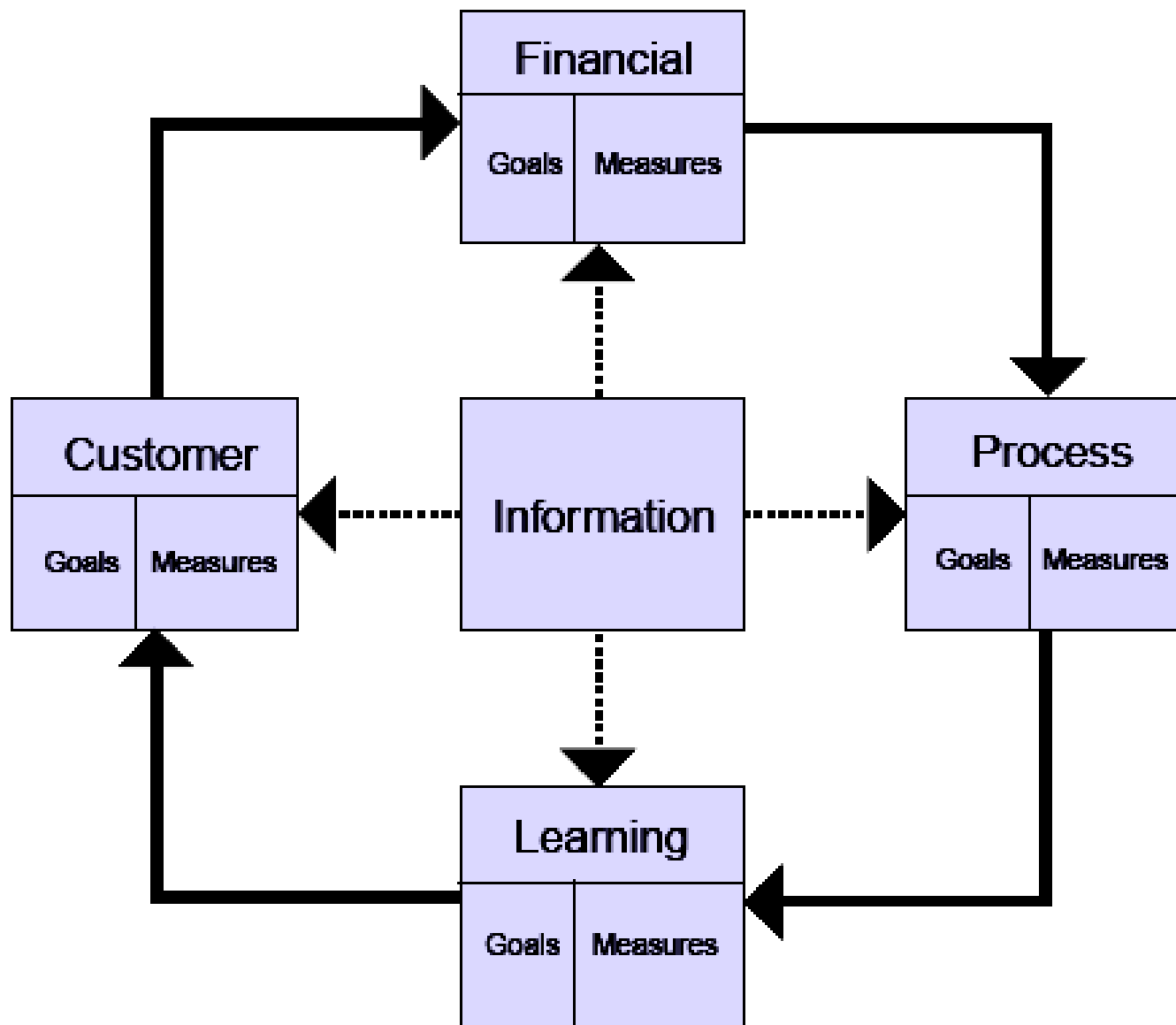
Оценка и управление рисками

- Прозрачность относительно рисков: все знают, что может случиться и чем это грозит
 - Для чего делать бэкапы и как часто?
- Отдает имеющий обязательства, если их нет – то его начальник
- Оценка рисков – это выгодно (посчитали и сравнили рентабельность затрат)
- Управление рисками должно быть проактивными (на чужих ошибках, а не на своих)

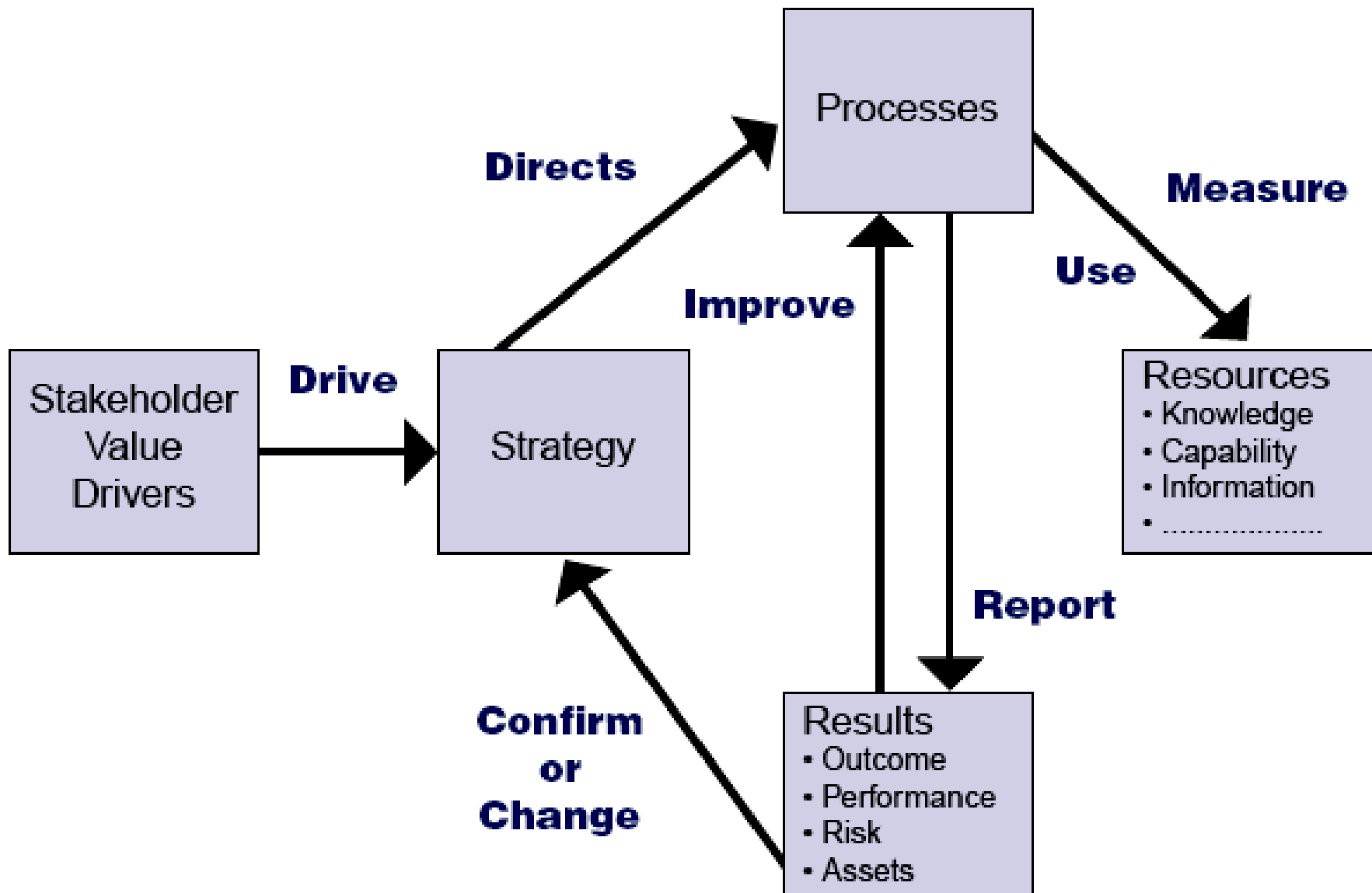
Оценка эффективности ИКТ

- С т.з. Финансов: совокупные расходы на ИТ не превышают извлекаемой выгоды
- С т.з. Пользователей: какие нужды пользователей должны удовлетворить ИКТ?
- С т.ч. Руководства и владельца: как изменилась конкурентоспособность, рентабельность и репутация организации после задействования ИКТ?

Balanced Scorecard для оценки эффективности ИКТ



Управление ИТ как процесс



Модель "зрелости" ИКТ в организации

Non-existent Initial Repeatable Defined Managed Optimised



LEGEND FOR SYMBOLS USED

-  Enterprise current status
-  International standard guidelines
-  Industry best practice
-  Enterprise strategy

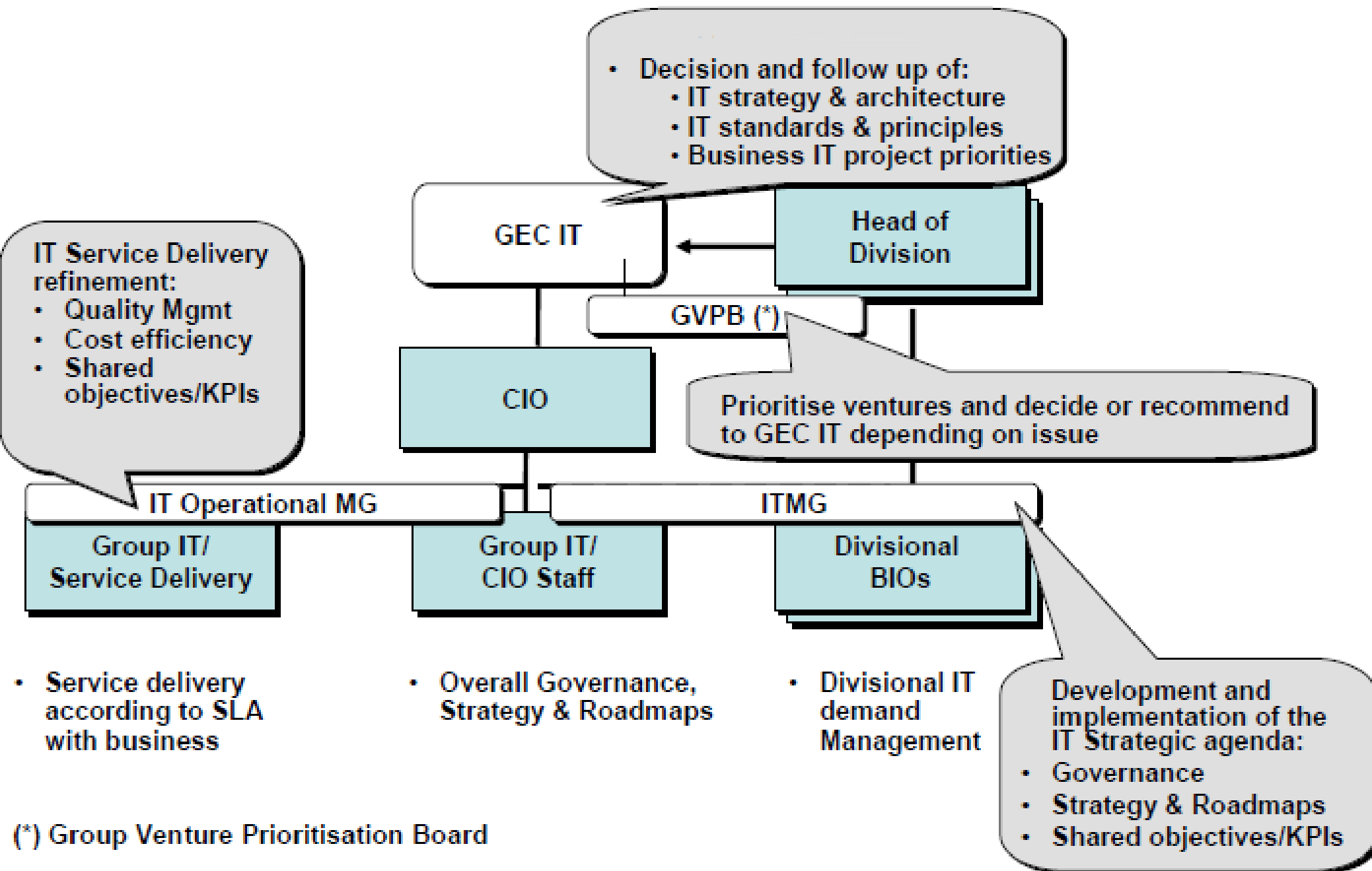
LEGEND FOR RANKINGS USED

- 0 Nonexistent – Management processes are not applied at all
- 1 Initial – Processes are *ad hoc* and disorganised
- 2 Repeatable – Processes follow a regular pattern
- 3 Defined – Processes are documented and communicated
- 4 Managed – Processes are monitored and measured
- 5 Optimised – Best practices are followed and automated

Как использовать "модель зрелости"?

- Собраться всем вместе и определить, где сейчас находится организация? (сравнив с действующими стандартами и лучшими практиками)
- Определить долгосрочные и краткосрочные цели (например, "догнать и перегнать")
- Выяснить, что нуждается в изменении, сколько они будут стоить и что нужно для их проведения
- Приоритезировать работы и сделать их
- Подождать и повторить с первого пункта

Пример ИТ-группы банка



(*) Group Venture Prioritisation Board

**Аудит в ИТ:
терминология, принципы,
методики**

Что такое ИТ-аудит?

- Консультационная услуга
- Независимый анализ или обзор текущего использования средств ИКТ в организации
- Проверка или тестирование эффективности, достаточности, надёжности и целесообразности использования конкретных ИКТ в организации
- Аттестирование персонала, процессов и документации по поддержке, обслуживанию и действиям в нештатных ситуациях

Цель аудита

- Выявить потенциально уязвимые компоненты инфосистемы
- Проверить добропорядочность поставщиков оборудования, подрядчиков, персонала
- Оценить компетентность персонала и дать рекомендации по её повышению
- Проверить полноту документации, особенно – сценарий действий в случае форс-мажора
- Рассказать руководству понятным языком, как обстоят дела с ИКТ в их фирме (эффективность, безопасность, доступность) и что можно/нужно сделать иначе (сэкономить денег, снизить риски, повысить конкурентноспособность). Письменно!

Что изучается при аудите?

- Всё – чем больше, тем лучше
- Аудит может быть точечным: по аспектам
 - Безопасность и доступность инфосистем
 - Защищённость данных (физическая среда)
 - Соответствие законодательству, стандартам
 - Полнота и достаточность документации и правил
 - Инвентаризация оборудования и лицензий
 - Code review (рефакторинг кода)
 - Сертификация персонала
 - Веб-сайт организации

Кто проводит аудит?

- Независимый специалист или компания
- Не должен быть одним из подрядчиков или поставщиков оборудования или услуг
- Сертификат CISA, CISM, CGEIT
- Входит в ассоциацию ISACA или её локальное подразделение (www.isaca.ee)
- Образование: обычно финансы/инфотехнология/юриспруденция и их комбинации (учёная степень, MBA)
- Опыт работы: от 5 лет (желательно)

Аудиторские организации

- "Большая четвёрка"
 - PriceWaterhouseCoopers
 - KPMG
 - Deloitte
 - Ernst & Young
- Государственные департаменты
 - Riigikontroll
 - Finantsinspektsioon
 - Andmekaitse inspektsioon
 - RIA

С чего начать?

- Аудит – это проект со всеми вытекающими
- Ознакомиться с организацией, её структурой, наличием и полномочиями ИТ-отдела
- Определить границы аудита (обзора) и его цели
- Договориться о единой контактной лице с каждой стороны, регулярных встречах, формате и сроке предоставления отчёта
- Проверить наличие доступа ко всем изучаемым объектам и достаточность прав

Первые шаги

- Получить документацию и тщательно её изучить
- Если мы имеем дело с "самоделкой" инфосистемой / ПО – начать им пользоваться с разными ролями и правами
- Делать заметки с самого начала
- Отчёт для заказчика писать на человеческом языке, рекомендации для ИТ-специалистов – на техническом

Шпаргалка аудитора

- Режим работы инфосистемы (5x8, 24x7x365) и как он обеспечен?
- Что случится, если режим нарушится? Кто, как быстро и какие действия должен предпринять (время реагирования, допустимое время простоя, "план пожаротушения")? Знают ли ответственные и исполнители о своих обязанностях? Доступны ли они? Есть ли у них всё необходимое оборудование и доступ?

Шпаргалка аудитора

- Проводился ли ранее аудит (обзор) инфосистемы? Кем, когда, каковы его результаты? Какие меры по ним приняты? Какие важные изменения в среде произошли после проведения аудита?
- Кто является разработчиком ИС, кто её обслуживает, поддерживает пользователей? Какова их репутация, опыт, история?\
- Из чего состоит ИС (железо, софт, версии) и нуждается ли в критическом обновлении?

Шпаргалка аудитора

- Какие бизнес-процессы будут нарушены из-за недоступности ИС? Как можно их дублировать с/без использования ИКТ? Как потом измененные/добавленные данные попадут в ИС после восстановления её работоспособности?
- Какие другие ИС зависят от "упавшей" ИС или от доступности каких других ИС зависит доступность исследуемой системы?
- Кого и как следует извещать о проблемах ИС разного уровня критичности?

Шпаргалка аудитора

- Насколько опытны пользователи ИС? Какие есть возможности для предотвращения проблем, вызванных их некомпетентностью?
- Существует ли в ИС возможность отката сделанных изменений или лог?
- Доступна ли пользователям самая свежая документация по ИС на понятном им языке?
- Ведётся ли FAQ по обращениям пользователей, лог типичных проблем и способах их устранения?

Шпаргалка аудитора

- Кто и как обслуживает аппаратную часть ИС? Заключен ли с ним договор со временем реагированием и ответственностью за простой?
- Какова лицензионная политика ИС, соблюдена ли она, как обеспечивается контроль за сроком действием лицензий, продление и отзыв лицензий?
- Установлены ли самые минимальные права для каждого из пользователей / группы?

Шпаргалка аудитора

- Есть ли в ИС противоречия здравому смыслу, несоответствие законодательству или бизнес-целям организации?
- Ведётся ли лог программных/аппаратных ошибок, как он хранится и защищается? Как часто и кем просматривается, принимаются ли какие-то действия?
- Требования к способу авторизации, паролям, частоте их смене, процедура получения, смены и отзыва доступа

Шпаргалка аудитора

- Импорт/экспорт данных
- Резервное копирование и восстановление данных, частота, период хранения копий
- Значения по умолчанию, границы настроек (персонализации)

Проблема аудита ИС с точки зрения безопасности

Три аспекта безопасности

- **Доступность** (*käideldavus, availability*) в часах или % от заявленного времени доступности
 - Если мы заявляем, что "наша инфосистема работает круглосуточно с доступностью 99%" то какой максимальный downtime в год мы можем себе позволить?
 - Достаточно ли будет его для переустановки ОС?
 - Если нет, то как обеспечить заявленную доступность?
 - Какова фактическая доступность нашей ИС, если мы вынуждены отключать её каждую ночь на 2 часа для создания бэкапа?

Три аспекта безопасности

- **Целостность** (*terviklus, integrity*) - бинарна: она либо есть, либо её нет, хотя можно проводить некоторые параллели с фрагментацией диска):
 - собственно сами данные
 - Метаданные
 - правила обработки данных
 - связи между всем вышеперечисленным
- Пример: RAID-контроллер (режим 0, 1, 5)

Три аспекта безопасности

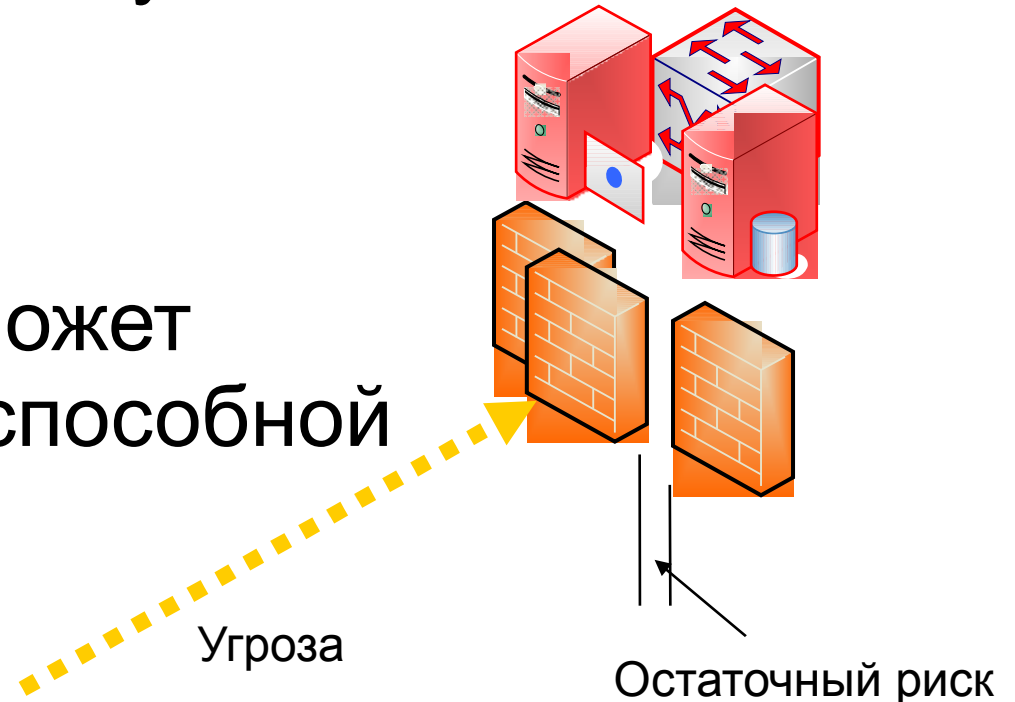
- Конфиденциальность (*konfidentsiaalsus, confidentiality*) – данные доступны только тем людям, которые имеют на это соответствующее право
 - И даже эти люди не могут своим правом злоупотребить!
 - Или хотя бы останется след злоупотребления!

Другие важные термины

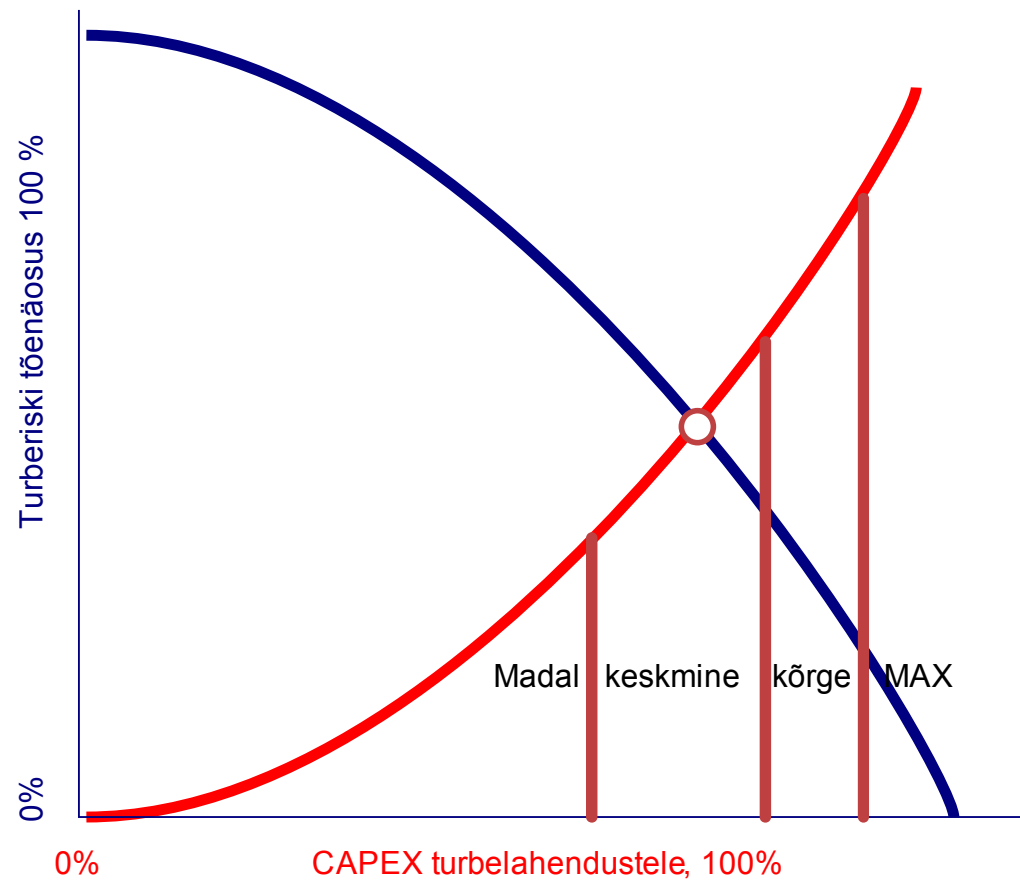
- Зависимость (*sõltumisväärsus, dependability*)
- Надёжность (*töökindlus, reliability*)
 - MTBF (Mean Time Before Failure – среднее время наработки на отказ)
- Безопасность (*ohutus, safety*)
- Защищённость (*turvalisus, security*)
- Угроза (*ohu, threat*)
- Уязвимость (*nõrkus, vulnerability*)
- Риск (*risk, risk*)
- Дыра в защите (*turbekadu, security loss*)
- Мера безопасности (*turbemeetmed, security measures*)

Остаточный риск

- Каждая мера безопасности стоит денег \$
- Меры безопасности уменьшают угрозу
- Но устранить её полностью слишком дорого
- Поэтому всегда существует некий остаточный риск
- *Это нормально*
- Иначе организация может стать неконкурентноспособной



Расходы на безопасность vs убыток в результате инцидента



Выводы

- Не существует "серебряной пули" – универсального способа устранить все угрозы
- Мы можем только снижать риски, используя комплексные меры безопасности
- При этом остаётся смириться с остаточным риском и признать вероятность возникновения определенных угроз
- Задача аудита – определить эти угрозы и оценить эффективность сделанных (планируемых) капиталовложений

Фреймворк ISKE

Что такое ISKE?

- Трёхуровневый каркас эталонных мер безопасности для инфосистем
- Разработан в Эстонии (RIA) на основе немецкого стандарта IT-Grundschutz (IT Baseline Protection Manual) в 2003 году
- Обязателен для использования в государственных структурах Эстонии, но подходит и для других организаций
- Обновляется (почти) каждый год, текущая версия – 5.01 (июнь 2010)
- Домашняя страница: <http://www.ria.ee/iske>

Задачи ISKE

- Обеспечить достаточную защиту обрабатываемых ИС данных
- Описывает эталонные меры для каждого из трёх уровней безопасности:
 - L (low)
 - M (medium)
 - *Оптимальный уровень защиты обычно тут*
 - H (high)
- Критерии: требования к конфиденциальности, целостности, доступности и скорости восстановления

Документы ISKE

- ISKE turbejuhend - основной документ, руководство по мерам безопасности
- ISKE kataloogid – приложение (более 2000 страниц), в котором подробно описаны все компоненты ИС, угрозы и возможные атаки
- ISKE audiidi juhend – руководство по аудиту
 - Класс H – обязательный аудит 1 раз в 2 года
 - Класс M – обязательный аудит 1 раз в 3 года
 - Класс L – обязательный аудит 1 раз в 4 года

Аспекты безопасности по ISKE

- Доступность – К
 - К1 – в днях (uptime 90%)
 - К2 – в часах (99%)
 - К3 – в секундах (99.9%)
- Целостность – Т
 - Т1 – запрещено несанкционированное изменение данных
 - Т2 – известен автор изменений
 - Т3 – подтверждение автора изменений третьим лицам
- Конфиденциальность – S
 - S1 – возможен материальный или моральный ущерб
 - S2 – угроза функционированию учреждения / приватность граждан
 - S3 – угроза функционированию гос-ва / угроза хаоса и анархии
- Уровень 0 (K0, T0, S0) – аспект не имеет значения

Примеры эталонных мер ISKE

- Оповещение о переполнении накопителя при заполнении его объёма на 75%
- 1 сервер = 1 услуга
- Регулярный поиск wifi honeypot
- Безопасные форматы файлов (txt, jpg, gif), потенциально опасные и запрещенные
- Название WiFi не должно ссылаться на владельца и не должно работать с DHCP
- Скринсерверы с паролем через 5 мин неактивности
- Изменения в топологии сети документируются в течение 2 часов
- При выносе сменных носителей из здания информация на них должна быть зашифрована

Стандартизация в ИТ

Стандарты в ИТ аудите

- Если аудируемая организация утверждает, что придерживается тех или иных стандартов – проверить
- Если не утверждает – обратить внимание на то, какие аспекты деятельности можно стандартизировать и как
- Стандарт – друг аудитора :)

Кто определяет стандарты?

- ISO – International Organization for Standardization
- IETF – Internet Engineering Task Force
 - *Технические стандарты и протоколы, RFC*
- W3C – World Wide Web Consortium
- OASIS - Organization for the Advancement of Structured Information Standards
- EVS – Eesti Standardikeskus
- И другие

Стандарты ISO

- ISO/IEC 19770 Software Asset Management
- ISO/IEC 20000 IT Service Management (ITSM)
- ISO/IEC 24762 Disaster Recovery Guidelines
- ISO/IEC 27000 Information Security
- ISO/IEC 31000 Risk Management
- ISO 9000 Quality Management
- ISO 14001 Environmental Management
(Green IT)
- EN 16001 Energy Management

Стандарты W3C

- Mobile Web (Geolocation, UI, widgets)
- Voice Browsing (VoiceXML)
- Internationalization (i18n, l10n)
- Security
- XML
- Meta Formats (RDF, OWL)
- Privacy (P3P)
- Accessibility (WAI, WCAG)

Стандарты OASIS

- BCM — Business Centric-Methodology
- CAP — Common Alerting Protocol
- CAM — Content Assembly Mechanism
- CIQ — Customer Information Quality
- DocBook — A markup language for technical documentation
- EML — Election Markup Language
- EDXL - Emergency Data Exchange Language,
- oBIX — open Building Information Exchange
- OpenDocument
- SAML — Security Assertion Markup Language,
- XACML — eXtensible Access Control Markup Language

Стандарты EVS

- EVS-ISO 2382 Infotehnoloogia sõnastik
- EVS 8:2008 Infotehnoloogia reeglid eesti keele ja kultuuri keskkonnas
 - Правила для информационных технологий в эстонской языковой и культурной среде
- EVS JUHEND - Standardi EVS 8:2000 rakendusjuhend

EVS 8:2008 - числа

- Разделитель дробной части – запятая (,).
 - Например: 543,21
- Разряды группируются с конца по 3 цифры и разделяются пробелом.
 - Например: 1 350 000
- Числа до 9999 не группируются
- В отрицательных числах знак минуса не отделяется от числа.
 - Например: -273
- Округляются [0;4] до предыдущего, [5;9] – до следующего.

EVS 8:2008 - деньги

- Разделитель дробной части – точка.
- Правила группировки такие же, как и у чисел.
- Международное обозначение валюты – ЕЕК и EUR, пишется перед суммой и отделяется от нее пробелом
- Внутреннее обозначение – kr, euro, € - пишется после суммы, отделяется пробелом, точка не ставится.
- Округление: [1;2] до 0, [3;7] до 5, [8;9] до следующего
 - Например: -543.21 € или 543.21 kr

EVS 8:2008 - календарь

- Первый день недели – понедельник
- День месяца всегда отделяется остальной части даты точкой
- Формат даты: *день.месяц.год*
- Ноль перед днем месяца может не ставиться
- Сокращения дней недели – однобуквенные (E, T, K, N, R, L, P)
- Сокращения месяцев: jaan, veebr, märts, aprill, mai, juuni, juuli, aug, sept, okt, dets
 - 21. veebruar 2004. a
 - 21. veebr 2004. a
 - laupäev, 21. veebruar 2004. a
 - L, 21. veebr. 2004. A
 - 21.02.2004

EVS 8:2008 - время

- 24-часовая система времени
- Формат времени: ч:мин:сек,мс
- Разделитель времени – двоеточие

Например:

- 22:45:36,12
- 07:30
- 21.02.2004 12:00

EVS 8:2008 - текст

- Кодовые страницы
 - ISO/IEC 8859-15, 8859-1, 8859-4, 8859-13;
 - MS Windows-1257 Baltic, Windows-1252 CE;
 - IBM CP 775, 850;
- Знак номера - слово “Nr” (№,# не используется)
- Знак деления – “:” или “/”
- Знак параграфа - §, а не ¶
- Знак препинания не отделяется пробелом от предыдущего слова, предложения отделяются одним пробелом, «красная строка» не используется (вместо неё «пустая строка»)
- Вложенность кавычек: “Text «Text»”
- Дефис, минус, тире – разные знаки (-, —, —)

EVS 8:2008 - имена

- Формат: Имя Фамилия
- Отчество не используется
- Допустим инициал имени
- Используются обороты “härра”, “proua”, “preili” и их сокращения – hr, pr
- Личный код формата GYYMMDDooooC

EVS 8:2008 – почтовый адрес

Standardiamet

Aia tn 5

10317 Tallinn

Eesti

Jaan Tamm

Tammi talu

Karu küla, Saue vald

12120 Haarju mk

EVS 8:2008 – телефоны

- Внутри – без кодов;
- международный формат +код, отделен пробелом
- Цифры группируются по 2,3 или по 4 с конца
- Можно выделять «логическую часть»

- Например
- +372 5555 5555
- 55 555 555
- 566 66 66
- 5 1234 36

EVS 8:2008 – код страны

- Двухбуквенный EE
- Трехбуквенный EST
- Телефонный 372
- Товарный 474
- Библиотечный 9985
- Локализация et

Выберите организацию

Вы устраиваетесь на работу в IT-helpdesk в

- сеть продуктовых магазинов
- сеть автозаправок
- сеть аптек
- сеть библиотек
- сеть страховых агентств

задача – задав 10 вопросов 3 контактными лицам организации выяснить максимум информации об использовании ИКТ

Контактные лица

- Генеральный директор
- Главный бухгалтер
- Руководитель ИТ
- Веб-мастер сайта
- Системный администратор
- Начальник IT helpdesk
- Сотрудник IT helpdesk
- Директор одного из отделений сети
- Работник одного из отделений сети

Фреймворк COBIT

Что такое COBIT?

- COBIT (Control Objectives for Information and related Technology) - методология управления, контроля и аудита информационных систем.
- Разработан в 1996 г Международной ассоциацией аудита и контроля за информационными системами (ISACA)
- Делит всю деятельность ИТ на 4 домена (сферы деятельности), 34 высокоуровневых процесса и 318 детальных задач управления
- Текущая версия – 4.1 (в разработке - 5.0)

Миссия SOBIT

- Исследование, разработка, реклама и продвижение международного набора авторитетных, отвечающих современным требованиям, общепризнанных задач управления ИТ.
- Связующее звено между бизнес-рисками, задачами управления и технической инфраструктурой.
- Ориентирован прежде всего на ИТ-менеджеров, руководителей предприятий и владельцев бизнес-процессов.

Цели и задачи COBIT

- Организовать мониторинг работы служб ИТ, привязанный к целям и задачам бизнеса
- Осуществлять сравнение уровня развития ИТ с другими предприятиями отрасли
- Представить виды деятельности ИТ в виде логичной управляемой структуры процессов
- Помочь сфокусироваться на контроле, а не на исполнении (оптимизация инвестиций в ИТ, обеспечить непрерывное предоставление услуг, предложить инструмент измерения эффективности и корректирующие меры).

Сферы влияния COBIT

- Финансы
 - доход/расход, ROI, активы, интрессы, риски
- Клиенты
 - Качество обслуживания, потребности в услугах
- Внутренние процессы
 - Соответствие законам, интеграция и автоматиз.
- Обучение и развитие
 - Инновации, мотивация персонал, база знаний

Домены COBIT

- планирование и организация (*ИТ-процессов и услуг отдела ИТ*)
- комплектование и внедрение
- предоставление и поддержка
- мониторинг и отчётность

Процессы COBIT (34)

- С одной стороны связан с доменом, с другой — с целью (ИТ-цель и бизнес-цель)
- Для каждого процесса определены:
 - Ключевые индикаторы достижения цели (KGI).
 - а были ли достигнуты ИТ-процессом бизнес-требования?
 - Ключевые показатели эффективности (KPI)
 - насколько хорошо работает ИТ-процесс для обеспечения достижения целей?
 - Степень зрелости процесса
 - по шкале от 0 (отсутствует) до 5 (внедрены лучшие практики)

Документы COBIT ("книги")

- «Резюме для руководства» - введение в остальные разделы стандарта. Содержит общие сведения о стандарте, определяет миссию COBIT и понятие системы управления ИТ.
- «Концептуальное ядро COBIT» - набор основополагающих принципов и понятий, модель управления ИТ
- «Руководство по менеджменту» - описывает разработку стратегии управления ИТ, контроль над использованием информационных ресурсов, их мониторинг и оценку

Документы COBIT ("книги")

- «Набор инструментов внедрения» - разъясняет ключевые концепции, предлагая пошаговое описание и примеры внедрения
- «Детальные задачи управления» - каждая задача управления (всего - 318) содержит формулировку ожидаемых результатов, которые необходимо достигнуть путем реализации конкретных процедур управления.
- «Руководство по аудиту» - облегчает использование концептуального ядра и основных принципов управления COBIT при проведении ИТ-аудита.

Пример COBIT: цели отдела ИТ

(справа – ссылки на связанные ИТ-процессы)

Goal	Name	Bus Prio	IT Processes						
2	Respond to governance requirements inline with board direction/ Удовлетворить требования руководства в соответствии с решениями Совета Директоров	3	PO1	PO4	PO10	ME1	ME3		
4	Optimise the use of information / Оптимизировать использование информации	3	PO2	DS11					
7	Acquire and maintain integrated and standardised application system/ Приобретать и поддерживать стандартизированные и интегрированные приложения	6	PO3	AI2	AI5				
8	Acquire and maintain an integrated and standardised IT infrastructure/ Приобретать и поддерживать стандартизированную и интегрированную ИТ инфраструктуру	6	AI3	AI5					
10	Ensure mutual satisfaction of third-party relationship / Установить взаимовыгодные отношения с производителями и поставщиками	3	DS2						
12	Ensure transparency and understanding of IT cost, benefits, strategy, policies and service levels. / Гарантировать прозрачность и понимание затрат на ИТ, выгод, стратегии, политики и уровней ИТ услуг	3	PO5	PO6	DS1	DS2	DS6	ME1	ME3
13	Ensure proper use and performance of the applications and technology solutions/ Гарантировать надлежащее использование и производительную работу технологических приложений и систем	3	PO6	AI4	AI7	DS7	DS8		
15	Optimise the IT infrastructure, resources and capabilities / Оптимизировать ИТ инфраструктуру, ресурсы и мощности	3	PO3	AI3	DS3	DS7	DS9		
20	Ensure automated business transactions and information exchanges can be trusted / Гарантировать правильность выполнения транзакции и информационного обмена	3	PO6	AI7	DS5				
24	Improve IT's cost-efficiency and its contribution to business profitability / Повышать эффективность ИТ затрат и их вклад в доходность Компании	6	PO5	AI5	DS6				
25	Deliver projects on time and on budget meeting quality standards / Выполнять проекты вовремя и в рамках бюджета, соблюдая стандарты качества	3	PO8	PO10					
26	Maintain the integrity of information and processing infrastructure / Поддерживать целостность информации, процедур и инфраструктуры ее обработки	3	AI6	DS5					
28	Ensure that IT demonstrates cost-efficient service quality, continuous improvement and readiness for future change / Гарантировать, что ИТ демонстрирует эффективное качество обслуживания и непрерывное усовершенствование	3	PO5	DS6	ME1	ME3			

Пример COBIT: приоритетные ИТ-процессы

№	Proc	Name	Cobit Prior	IT Goals Prior	Final Prior
12	AI2	Acquire and Maintain Application Software / Проектировать и разрабатывать приложения	2	6	12
15	AI5	Procure IT Resources / Обеспечение ИТ-ресурсов	2	6	12
1	PO1	Define a Strategic IT Plan / Определить стратегический план ИТ	1	3	9
10	PO10	Manage Projects / Управление проектами	1	3	9
16	AI6	Manage Changes / Управление изменениями	1	3	9
22	DS5	Ensure Systems Security / Обеспечить безопасность систем	1	3	9
31	ME1	Monitor and Evaluate IT Performance / Мониторинг и оценка производительности ИТ	1	3	9
33	ME3	Ensure Regulatory Compliance / Обеспечение соответствия нормативам	1	3	9
3	PO3	Determine Technological Direction / Определить технологическое направление	2	3	6
5	PO5	Manage the IT Investment / Управление инвестициями в ИТ	2	3	6
8	PO8	Manage Quality / Управление качеством	2	3	6
18	DS1	Define and Manage Service Levels / Определить и управлять уровнями сервиса	2	3	6
26	DS9	Manage the Configuration / Управление конфигурациями	2	3	6
13	AI3	Acquire and Maintain Technology Infrastructure / Проектирование и поддержка технической инфраструктуры	3	3	3
19	DS2	Manage Third-party Services / Управлять сервисами третьих сторон	3	3	3
23	DS6	Identify and Allocate Costs / Определить и распределить затраты	3	3	3
24	DS7	Educate and Train Users / Обучать пользователей	3	3	3
2	PO2	Define the Information Architecture / Определить архитектуру информационных систем	3	0	0
4	PO4	Define the IT Processes, Organisation and Relationships / Определить ИТ-процессы, организацию и отнош	3	0	0
6	PO6	Communicate Management Aims and Direction / Согласовывать цели и направления управления	2	0	0
7	PO7	Manage IT Human Resources / Управление человеческими ресурсами в ИТ	3	0	0
9	PO9	Assess and Manage IT Risks / Оценивать и управлять ИТ-рисками	1	0	0
11	AI1	Identify Automated Solutions / Определять автоматизированные решения	2	0	0
14	AI4	Enable Operation and Use / Обеспечение работы и использования	3	0	0
17	AI7	Install and Accredite Solutions and Changes / Установка, аккредитация решений и изменений	2	0	0
20	DS3	Manage Performance and Capacity / Управление производительностью и мощностью	3	0	0
21	DS4	Ensure Continuous Service / Обеспечить непрерывность сервисов	2	0	0
25	DS8	Manage Service Desk and Incidents / Управление службой поддержки и инцидентами	3	0	0
27	DS10	Manage Problems / Управление проблемами	2	0	0
28	DS11	Manage Data / Управление данными	1	0	0
29	DS12	Manage the Physical Environment / Управление физическим оборудованием	3	0	0
30	DS13	Manage Operations / Управление операциями	3	0	0
32	ME2	Monitor and Evaluate Internal Control / Мониторинг и оценка внутреннего контроля	2	0	0
34	ME4	Provide IT Governance / Обеспечить управление ИТ	1	0	0

Процесс AI2: проектирование и разработка приложений

Контроль за процессом

проектирования и разработки приложений

который удовлетворяет требованию бизнеса к ИТ по

обеспечению доступности приложений, соответствующих бизнес-требованиями в срок и по приемлемой цене

фокусируясь на

создании и поддержании регулярного и рентабельного процесса разработки

осуществляется с помощью

1) переноса бизнес-требований в Технические Задания

2) следования стандартам разработки для всех изменений

3) разделения мероприятий по разработке, тестированию и эксплуатации

и измеряется

а) количеством проблем на одно приложение, приводящих к наблюдаемым простоям системы

б) процентом пользователей, удовлетворенных предоставленной функциональностью

AI5: закупка ИТ-ресурсов

Контроль за процессом

закупки ИТ-ресурсов

который удовлетворяет требованию бизнеса к ИТ по
повышению рентабельности ИТ и их вкладу в доходность бизнеса

фокусируясь на

приобретении и поддержании компетенций в ИТ, отвечающих за реализацию стратегии по осуществлению закупок интегрированной и стандартизированной инфраструктуры и сокращению закупочных рисков

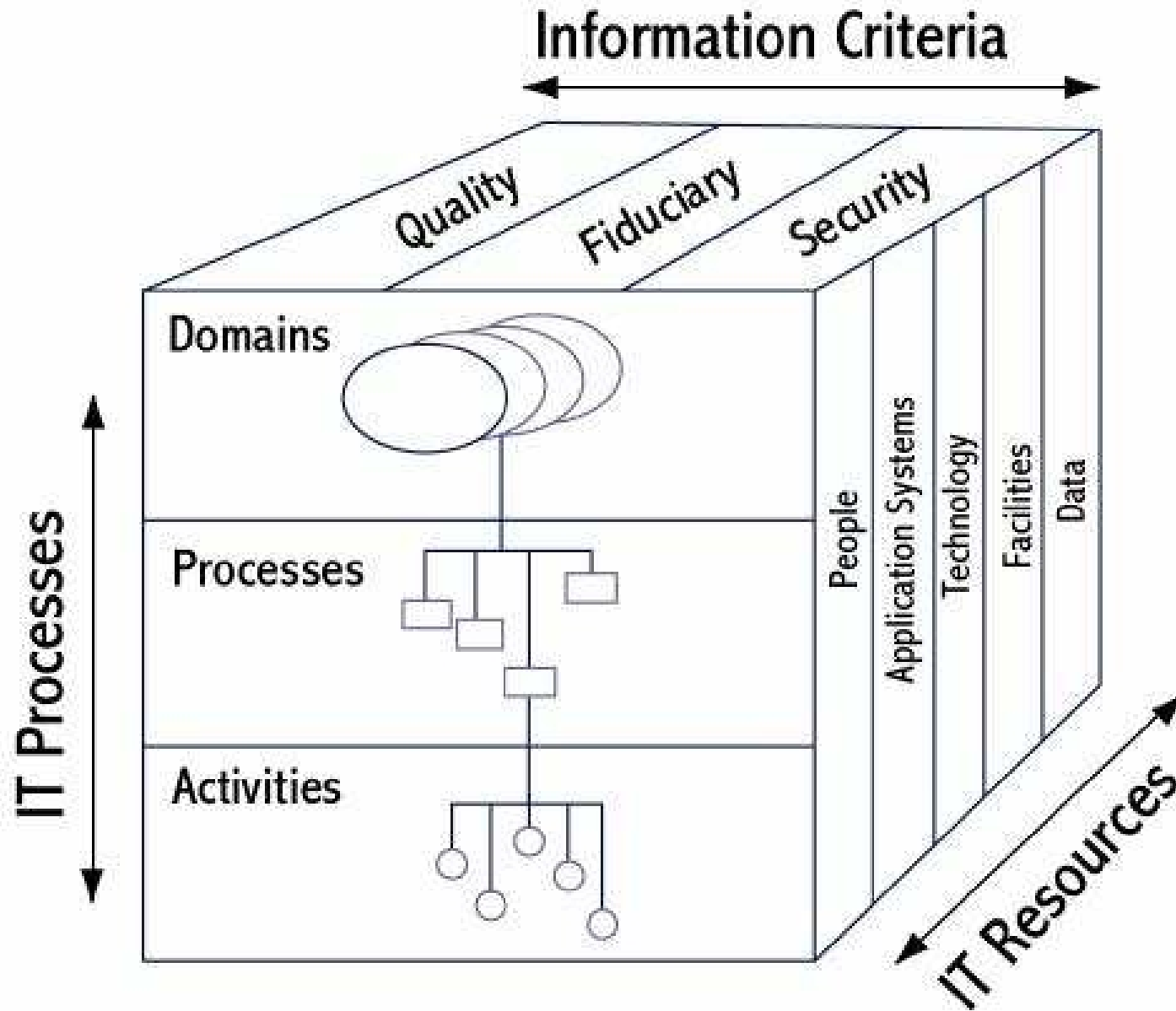
осуществляется с помощью

- 1) получения профессионального сопровождения по юридическим и контрактным вопросам**
- 2) определения процедур и стандартов закупок**
- 3) приобретения требуемого оборудования, ПО и услуг в соответствии с определенными процедурами**

и измеряется

- а) количеством споров по вопросам закупок**
- б) снижением закупочных цен**
- в) процентом заинтересованных лиц, удовлетворенных поставщиками**

Куб COBIT



Фреймворк ITIL

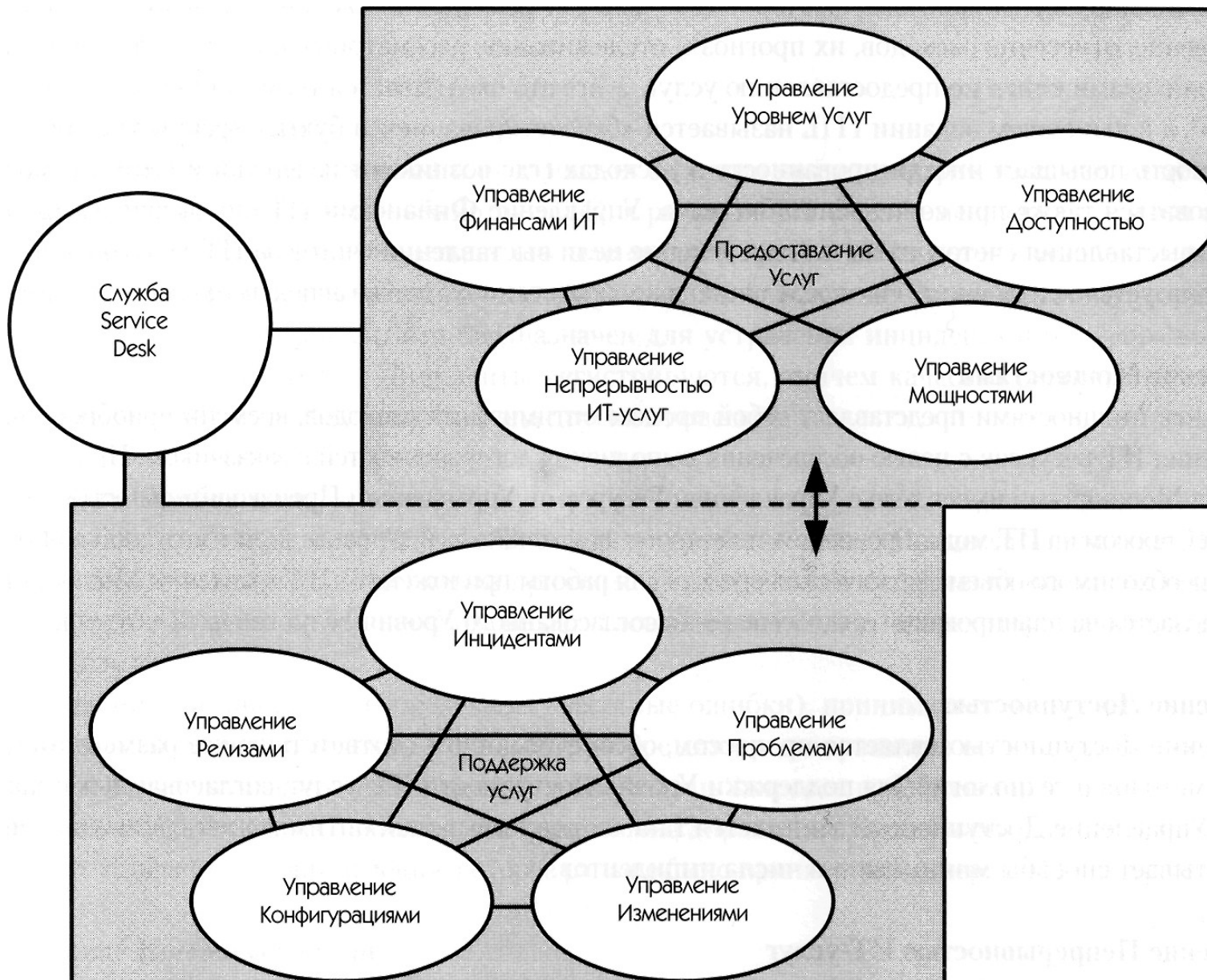
Что такое ITIL?

- ITIL (IT Infrastructure Library) - единый набор лучших практических методов по планированию и управлению ИТ, опробованных государственными и частными организациями всего мира
- Разработана в 1980-х годах в Англии, издаётся британским правительственным агентством Office of Government Commerce (принадлежит Королеве :) и является зарегистрированной торговой маркой
- Последняя версия – v3 (2007 г) соответствует ISO 9000

Цели и задачи ITIL

- предоставление услуг более высокого качества
- обоснование качества услуг с точки зрения затрат
- соответствие услуг требованиям бизнеса, заказчика и пользователя
- интеграция и централизация процессов
- знание всеми работниками своих ролей и обязанностей в ходе предоставления услуг
- извлечение уроков из прошлого опыта
- мониторинг показателей эффективности

Структура и состав ИТIL



"Книги" ITIL v3

- Стратегия услуг (Service Strategy)
- Проектирование услуг (Service Design)
- Преобразование услуг (Service Transition)
- Эксплуатация услуг (Service Operation)
- Постоянное улучшение услуг (Continual Service Improvement)

Базовые процесс ITIL

- Процесс управления инцидентами
- Процесс управления проблемами
- Процесс управления конфигурациями
- Процесс управления изменениями
- Процесс управления релизами
- Процесс управления доступностью
- Процесс управления непрерывностью
- Процесс управления финансами
- Процесс управления уровнем услуг
- Процесс управления мощностями

Служба Service Desk (HelpDesk, Call Center)

- единая точка контакта между пользователем и ИТ
- прием, регистрация обращений пользователей по вопросам ИТ;
- идентификация и обработка инцидентов и запросов на обслуживание;
- начальная поддержка пользователей;
- информирование пользователей о текущем статусе обращений;
- накопление базы знаний по решенным инцидентам;
- диспетчеризация инцидентов специалистам более высокой квалификации;
- контроль сроков решения инцидентов;
- эскалация инцидентов;
- управление жизненным циклом инцидента;
- участие в различных процессах поддержки и предоставления услуг
- информирование пользователей о проведении плановых работ