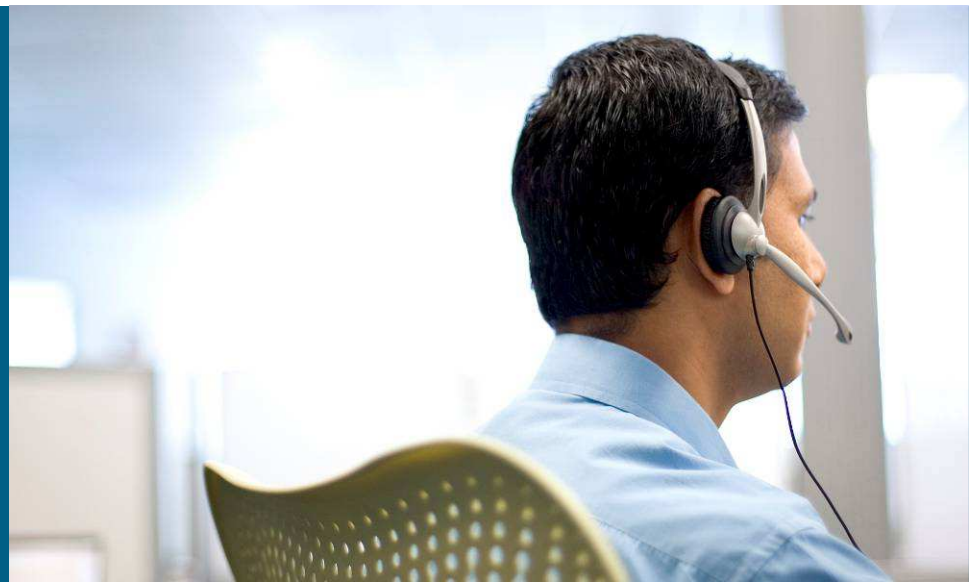
Управление ИБ с помощью ISO 27001, ISM3, ISF, ISO 13335 и др.



Алексей Лукацкий

Бизнес-консультант по безопасности

Содержание

- Какие бывают стандарты управления безопасностью?
- Стандарты управления ИБ
  - ISO 27001
  - ISO 13335
  - ISM3
  - ISF SoGP
- Какие другие стандарты существуют?
- Management vs. Governance
- Не увлекайтесь стандартами

Стандарты управления безопасностью

Типы стандартов УИБ

- Ориентированные на процессы
  - ISM3, CMMI, COBIT 4.0, ISO9001:2000, ITIL/ITSM
- Ориентированные на защитные меры (Controls)
  - BSI-ITBPM, ISO27001:2005, ISO13335-4
- Ориентированные на продукты
  - ISO15408
- Ориентированные на управление рисками
  - AS/NZS 4360, CRAMM, EBIOS, ISO 27005, MAGERIT, MARION, MEHARI, OCTAVE, SP800-3
- Ориентированные на лучшие практики
  - ISO/IEC 17799:2000, COBIT, ISF-SoGP

ISO 27001

Стандарт ISO 27001

- Название – «Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»
- В настоящем стандарте устанавливаются требования по созданию, внедрению, эксплуатации, мониторингу, анализу, поддержке и совершенствованию документально оформленной СМИБ в контексте общих бизнес-рисков организации
- Является стандартом в России (ГОСТ Р ИСО/МЭК 27001

СУИБ

- СУИБ (СМИБ) - та часть общей системы менеджмента, которая основана на подходе бизнес-рисков при создании, внедрении, функционировании, мониторинге, анализе, поддержке и совершенствовании информационной безопасности
- Целью построения СМИБ является обеспечение выбора адекватных и соответствующих мер (средств) контроля безопасности, с помощью которых обеспечивается адекватная защита информационных активов и создается доверие заинтересованных сторон

Ограничение ISO 27001

- Фокус на анализе рисков и построении СУИБ на основе проведенного анализа
- На сегодняшний день отсутствуют доказанные и воспроизводимые методы, позволяющие идентифицировать риски ИБ, оценить их вероятность и выбрать адекватные защитные меры (controls)
- Ориентация на внедрение защитной меры (control), а не достижении бизнес-цели

ISO 13335

Стандарт ISO TR 13335

- Состоит из 5 частей
  - Последние 3 части являются техническими отчетами (TR)
  - ISO 13335-5:2001 входит в состав ISO 18028-1
  - Первая часть разработана в 1996 году
- В начале 2008/09 года будет входить в серию ISO 2700x как ISO 27005
  - 4 из 5-ти частей
- Относится к техническому отчету 3-го типа
  - Технический комитет собирает данные разного сорта из материалов, обычно публикуемых как международный стандарт (например, состояние дел в данной области)
  - Не пересматривается до тех пор, пока не будет решено, что он не имеют больше ценности или полезности

Цели стандарта ISO TR 13335

- Главными целями стандарта являются:
  - определить и описать понятия, связанные с управлением безопасностью ИТ
  - определить отношения между управлением безопасностью ИТ и управлением ИТ вообще
  - представить несколько моделей, которые могут использоваться для объяснения безопасности ИТ
  - обеспечить общее руководство по управлению безопасностью ИТ

Разделы стандарта ISO TR 13335

- Часть 1 – Концепции и модели для управления безопасностью информационными и телекоммуникационными технологиями
- Часть 2 – Техники для управления рисками информационных и телекоммуникационных технологий
- Часть 3 – Техники для управления безопасностью ИТ
- Часть 4 – Выбор средств защиты
- Часть 5 – Руководящие принципы по сетевой безопасности – средства защиты для внешний коммуникаций

ISO TR 13335-1:1996

- Часть 1 дает общий обзор фундаментальных концепций и моделей, используемых для описания управления безопасностью информационных технологий
- Эти материалы предназначаются для менеджеров, ответственных за обеспечение безопасности информационных технологий, а также для лиц, ответственных за осуществление программы обеспечения общей безопасности в организации

ISO TR 13335-2:1997

- Часть 2 посвящена описанию аспектов управления и планирования
- Она предназначаются для менеджеров, ответственных за системы информационных технологий организации. К ним могут относиться:

  менеджеры по информационным технологиям, которые должны наблюдать за проектированием, внедрением, тестированием, закупкой или эксплуатацией систем информационных технологий, или

  менеджеры, ответственные за те виды деятельности, которые в значительной степени основаны на использовании систем информационных технологий

ISO TR 13335-3:1997

- Часть 3 дает описание способов обеспечения безопасности и предназначается для лиц, участвующих в управлении проектом на протяжении всего срока его действия
  - в части планирования, проектирования, внедрения, тестирования, приобретения или эксплуатации

ISO TR 13335-4:2000

- Часть 4 содержит указания по выбору средств защиты и их поддержке в виде базовых моделей и мер контроля
- В ней также описывается, как эти средства защиты дополняют способы обеспечения безопасности, о которых идет речь в Части 3
- Кроме того, в Части 4 говорится о том, как можно использовать методы дополнительной оценки для выбора средств защиты

ISO TR 13335-5:2001

- Часть 5 содержит руководящие указания для организаций, системы информационных технологий которых подключаются к внешним сетям
- Эти указания относятся к выбору и использованию средств защиты, обеспечивающих безопасность внешних соединений и услуг, поддерживаемых этими соединениями, а также дополнительных средств защиты, необходимых для систем информационных технологий в связи с указанными соединениями

Особенности стандарта ISO TR 13335

- Не догма, а руководство к действию, которое может и должно адаптироваться
- Показывает место ИБ в иерархии целей, стратегий и политик в организации
- Помимо триады CIA учитываются

  Подотчетность (accountability), подлинность (authenticity) и адекватность (reliability)
- Имеет стыковку с другими стандартами

  ITIL/COBIT - Управление конфигурацией, управление изменениями, управление инцидентами и т.д.

  ISO 27001 – Процессный подход

Особенности стандарта ISO TR 13335

- Учитывает наличие Комитета управления ИТ и Совета безопасности ИТ
- Учитывает не только технологические аспекты. Например,

  Рекомендации привлекать финансовой департамент, аудиторские подразделения и т.д. к разработке политике безопасности

  Учет социологических и даже экологических аспектов при выборе защитных мер
- Содержит методологию выбора средств защиты

ISM3

Стандарт ISM3

- Название – «Модель зрелости управления информационной безопасностью» (ISM3, ISM-cubed)
- Разработан ISM3 Consortium
  - Текущая версия – 2-я
- Расширяет принципы контроля качества ISO 9001 применительно к системам управления информационной безопасности
  - Процессно-ориентированный стандарт
- Опирается на ISO 9000, ITIL, CMMI и ISO 27001
- Совместим со стандартами COBIT, ISO, NIST, OCTAVE, OWASP и другими

Цель ISM3

- Цель СУИБ –предотвращать и отражать атаки, ошибки и аварии, которые могут подвергнуть опасности безопасность информационных систем и поддерживаемых ими организационных процессов

Разные цели безопасности

- Общие

  Пример: Оптимизация использования информации, денег, людей, времени и инфраструктуры

- Стратегические

  Пример: Координировать ИБ, ФБ и безопасность рабочего пространства

- Тактические

  Пример: Определить метрики, ориентированные на результат и оптимальность его достижения

- Операционные

  Идентифицировать и защитить активы

  Управлять жизненным циклом измерения ИБ

Уровни зрелости ISM3

- 5 уровней зрелости
  - Undefined
  - Defined
  - Managed (соответствует сертификации по ISO 9001)
  - Controlled
  - Optimized
- Каждому уровню соответствует набор мер, процедур, процессов, рекомендаций и т.д.
- Имеются определенные стыковки с моделями зрелости COBIT и CMMI
- Пользователь может выбрать нужный ему уровень зрелости

Ключевые отличия ISM3

- Измеримые цели ИБ и использование метрик для измерения их достижения
  - Позволяет создавать KPI, SLA безопасности для аутсорсинга
- Ориентирован на компании разного масштаба, включая SMB
- Смотрит на безопасность, как на процесс, который с течением времени улучшается, но никогда не достигает 100%-ой безопасности
- Описывает различные варианты последствий инцидентов
  - Прямой и непрямой, финансовый и нефинансовый ущерб

Ключевые отличия ISM3

- Различные методы выбора защищаемых процессов
  - Уровень зрелости
  - Оценка угроз
  - Оценка рисков
  - Оценка защищенности
  - Business Impact Analysis
  - И т.д.
- Описывает различные бизнес-цели и связывает их с целями безопасности
- Учет различных ролей в компании
  - Заказчик, стратегический, тактический и оперативный менеджмент, владелец процесса, владелец актива и др.

Отличия ISM3 от ISO 27001

- Связь с бизнес-целями
- Учитывает уровни зрелости организации
  - Отсутствует бинарная логика «соответствует / не соответствует»
- Ориентация на пользователя (включая топ-менеджмент), а не на аудитора
- Не так зависит от интерпретации со стороны аудитора
- Не ограничивается триадой CIA
- Позволяет измерять эффективность СУИБ
- Не требует анализа риска
  - Но допускает
- Различные варианты описания процессов
- Не так известен

Пример: ISM3 и ISO 27001

- Цель: «Число человеко-часов в результате простоя в результате вирусной атаки должно быть менее 10 за год»
- Достижение цели измеримо
- Возможно изменение метрики для перехода на более высокий уровень зрелости
- Прост для понимания

- Цель: внедрение мер по предотвращению вредоносного кода
- Цель измерима только бинарной логикой (Реализовано / Нет)
- Не связана с бизнесом
- Непонятна руководству
- Отсутствует «движение» (прогресс)

ISF SoGP

Стандарт ISF SoGP

- Название – «Standard of Good Practice for Information Security» (ISF SoGP)
- Разработан Information Security Forum

  Текущая версия – от 2007-го года
- Опирается на ISO 27002, COBIT v4.1, SOX, PCI DSS, Basel II и др.
- 372 страницы (!)

Область применения ISF SoGP

- ISF SoGP покрывает 6 аспектов ИБ:
  - Управление безопасностью
  - Окружение конечного пользователя
  - Критичные бизнес-приложения
  - Разработка систем
  - Сети
  - Инсталляция компьютеров

Особенности ISF SoGP

- Широкий охват различных аспектов ИБ

  Приложения, КПК, Instant Messaging, аутсорсинг, управление патчами, флешки, удаленная поддержка систем, VoIP, беспроводной доступ и т.д.

- Отличная систематизация материала

  Принцип

  Цель

  Защитные меры

  Лучшие практики и рекомендации

  Дополнительная информации

- Ориентация на анализ рисков

- Измерение эффективности проводится на соответствие ISF SoGP

Другие стандарты

Другие стандарты по УИБ

- SPE20003

  Нидерланды

- AS/NZS 4444

  Австралия и Новая Зеландия

- SS627799

  Дания и Швеция

- Canadian Handbook on Information Technology Security

- СТО БР ИББС-1.0-2006

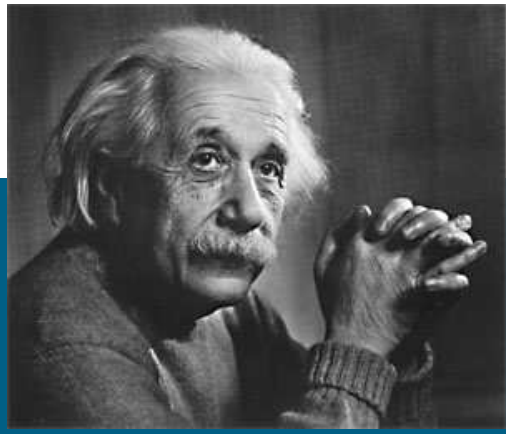
  Россия

- ITU-T X.1051

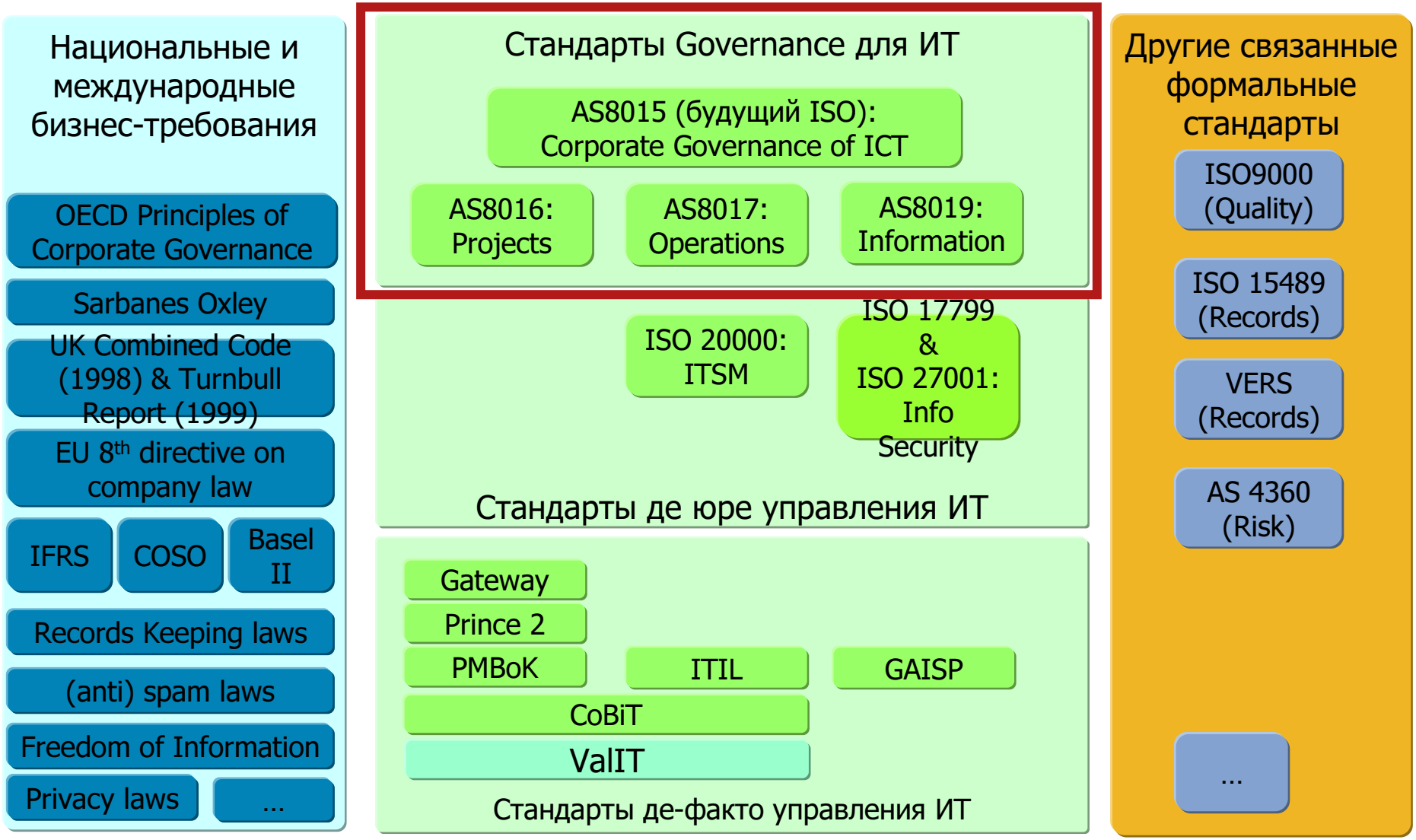
- Специальные публикации NIST 800 (12, 14, 18)

“Невозможно решить проблему на том же уровне, на котором она возникла. Нужно стать выше этой проблемы, поднявшись на следующий уровень.”

Альберт Эйнштейн



Не только безопасность



Management vs. Governance

“Концепция "governance" не нова. Она также стара, как и человеческая цивилизация. Просто "governance" означает: **процесс принятия решения и процесс, при котором решения внедряются (или не внедряются).**”

Комиссия по социальным и экономическим вопросам ООН

Другие определения Governance

- Governance (в бизнесе) – действие по разработке и последовательному управлению связанных в единое целое политиками, процессами и правильными решениями в данной области ответственности
- . . . связь между бизнесом и управлением ИТ
- . . . стратегические ИТ-решения, за которые отвечает корпоративный менеджмент, а не CIO или другие ИТ-менеджеры
- . . . ИТ Governance – это подмножество Corporate Governance, фокусирующееся на информационных системах
- …подтверждение того, что ИТ-проекты легко управляются и глубоко влияют на достижение бизнес-целей организации

Другие определения Governance

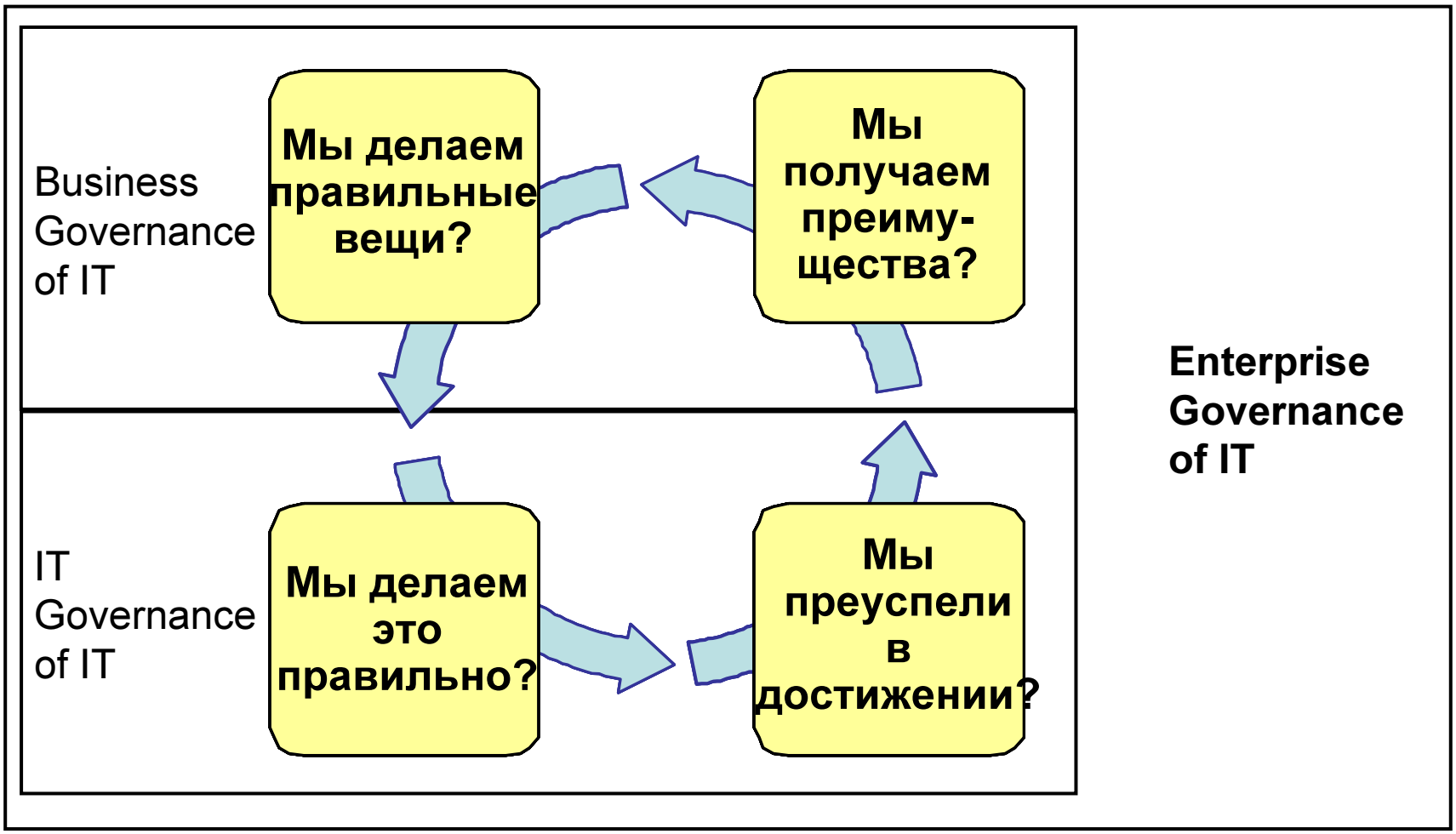
- ИТ Governance подразумевает систему, в которой все ключевые роли, включая совет директоров и внутренних клиентов, а также связанные области, такие как, например, финансы, делают необходимый вклад в процесс принятия ИТ-решений
- …взаимосвязь между ИТ, инициативами соответствия (compliance), управлением рисками и корпоративной бизнес-стратегией

Связь с другими ИТ-дисциплинами

- IT governance поддерживает следующие дисциплины:
  - Управление ИТ-активами
  - Управление ИТ-портфолио
  - Архитектура предприятия
  - Управление проектами
  - Управление программами
  - Управление ИТ-сервисами
  - Оптимизация бизнес-технологий

Ключевые вопросы Governance

Непрерывный процесс…



Источник: *The Information Paradox*

4 вопроса в деталях

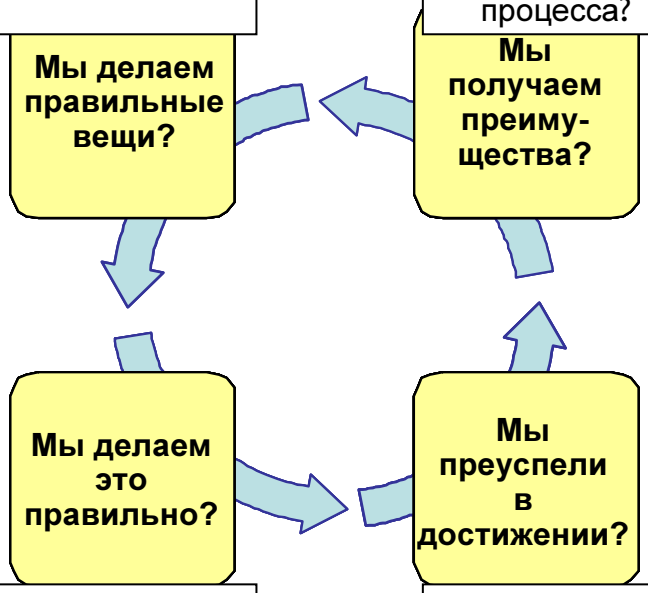
Источник: Fujitsu Consulting

Стратегический вопрос. Инвестиции:

- В соответствие с нашим видением?
- Соответствуют нашим бизнес-принципам?
- Содействуют нашим стратегическим целям?
- Обеспечивают оптимальное значение, затраты и уровень рисков?

Вопрос **ценности**. Мы имеем:

- Очевидное понимание ожидаемых преимуществ?
- Релевантные метрики?
- Эффективные преимущества реализации процесса?



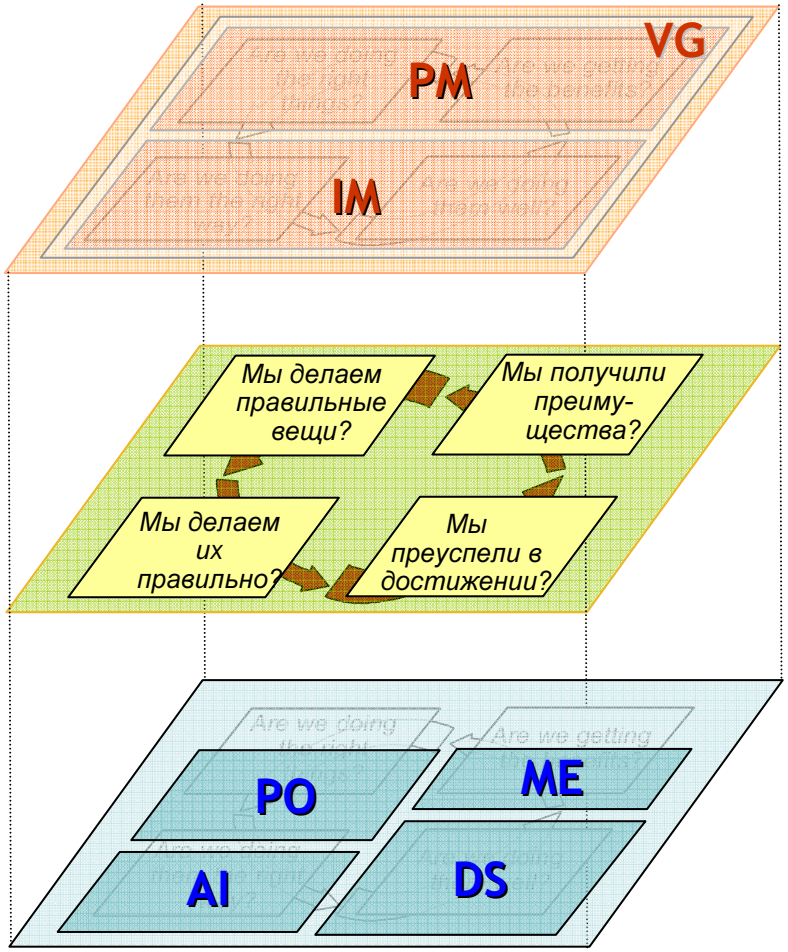
Архитектурный вопрос. Инвестиции:

- В соответствие с нашей архитектурой?
- Соответствуют нашим архитектурным принципам?
- Содействуют созданию архитектуры?
- В соответствие с другими инициативами?

Вопрос **реализации**. Мы имеем:

- Эффективный процесс управления изменениями и реализации?
- Компетентные и доступные технические и бизнес-ресурсы для реализации:
  - Требуемых возможностей; и
  - Организационных изменений, требуемых для достижения возможностей.

Val IT как решение задачи



Val IT

Governance & управление портфолио программой изменения бизнеса

"..достучаться до CXO и других старших менеджеров с посланием, как ценность ИТ для бизнеса может быть прозрачным и увеличивать..."

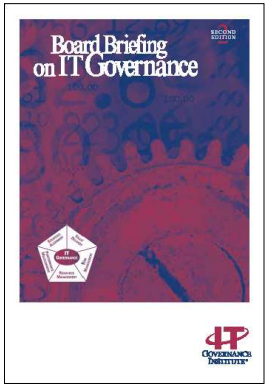
CobiT

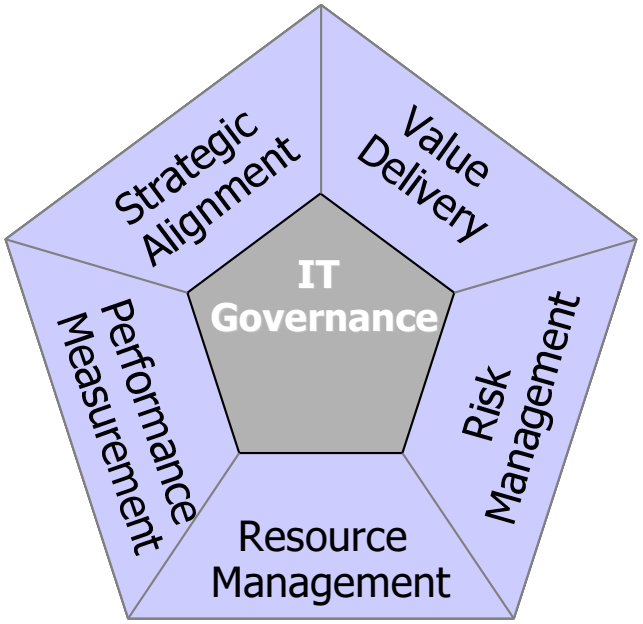
Governance & управление портфолие технологических проектов, сервисов, систем & поддерживающей инфраструктуры

IT Governance согласно Val IT

Руководство, процесс и структура гарантирующие, что ИТ на предприятии разрешают и поддерживают стратегию и цели предприятия, а также определяющие:

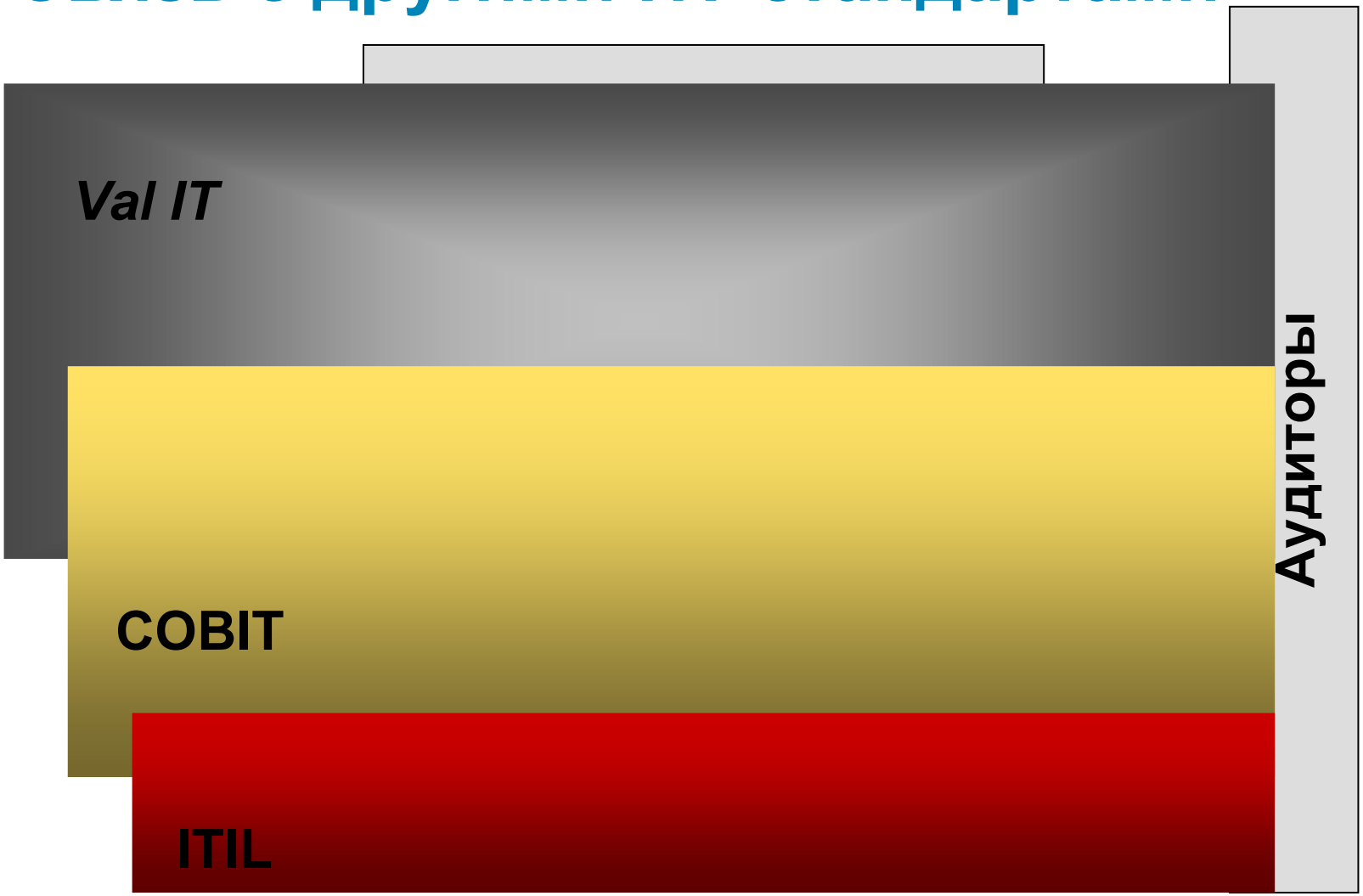
1. какие ключевые решения должны быть приняты;
2. кто отвечает за их принятие;
3. как они должны быть приняты; и
4. процессы и and поддерживающие их структуры для принятия решений, включающие мониторинг строгого соблюдения процессов и эффективности принятия решений





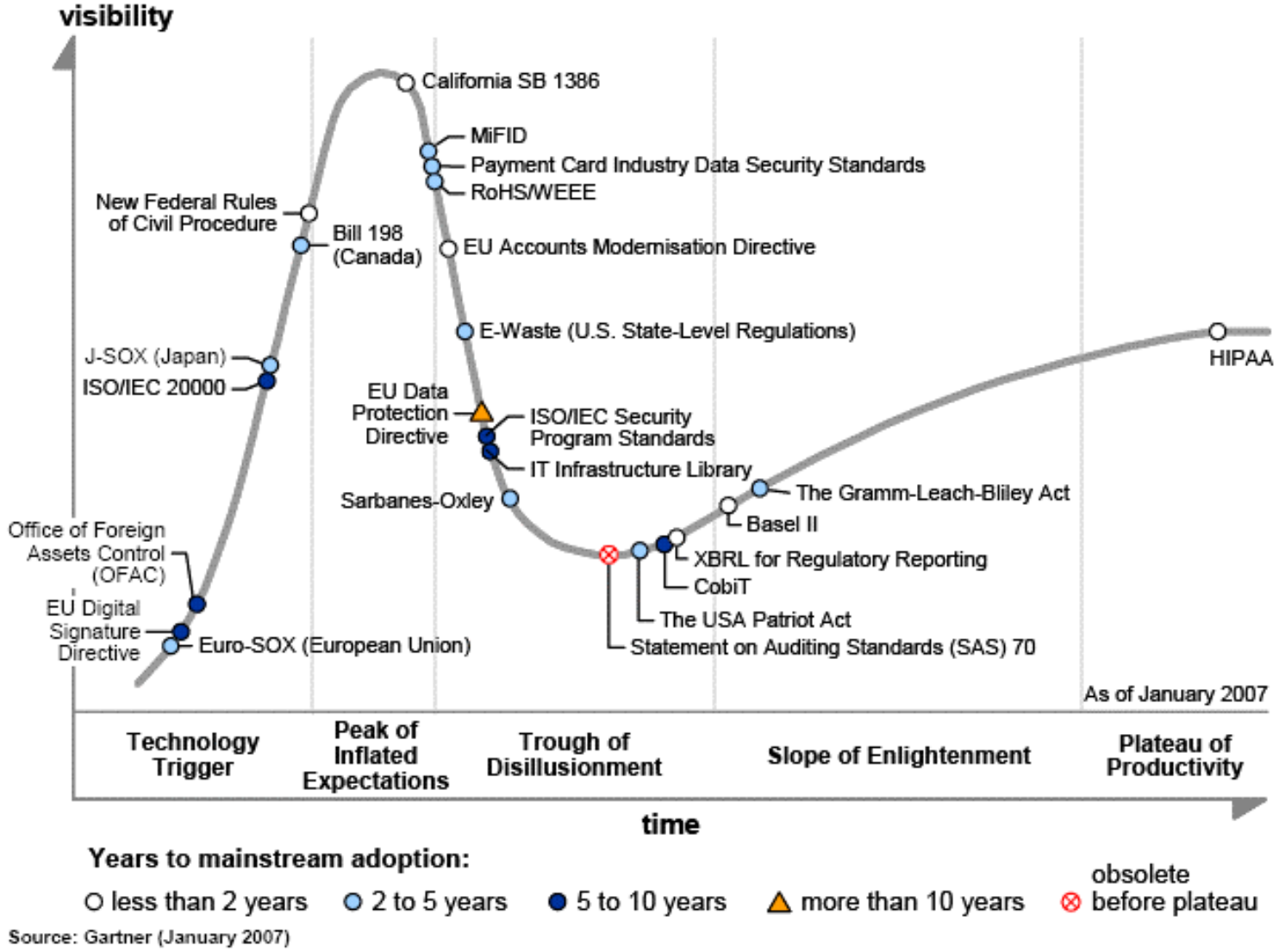
Источник : ITGI

Связь с другими ИТ-стандартами



Заключение

Внедрение произойдет не завтра

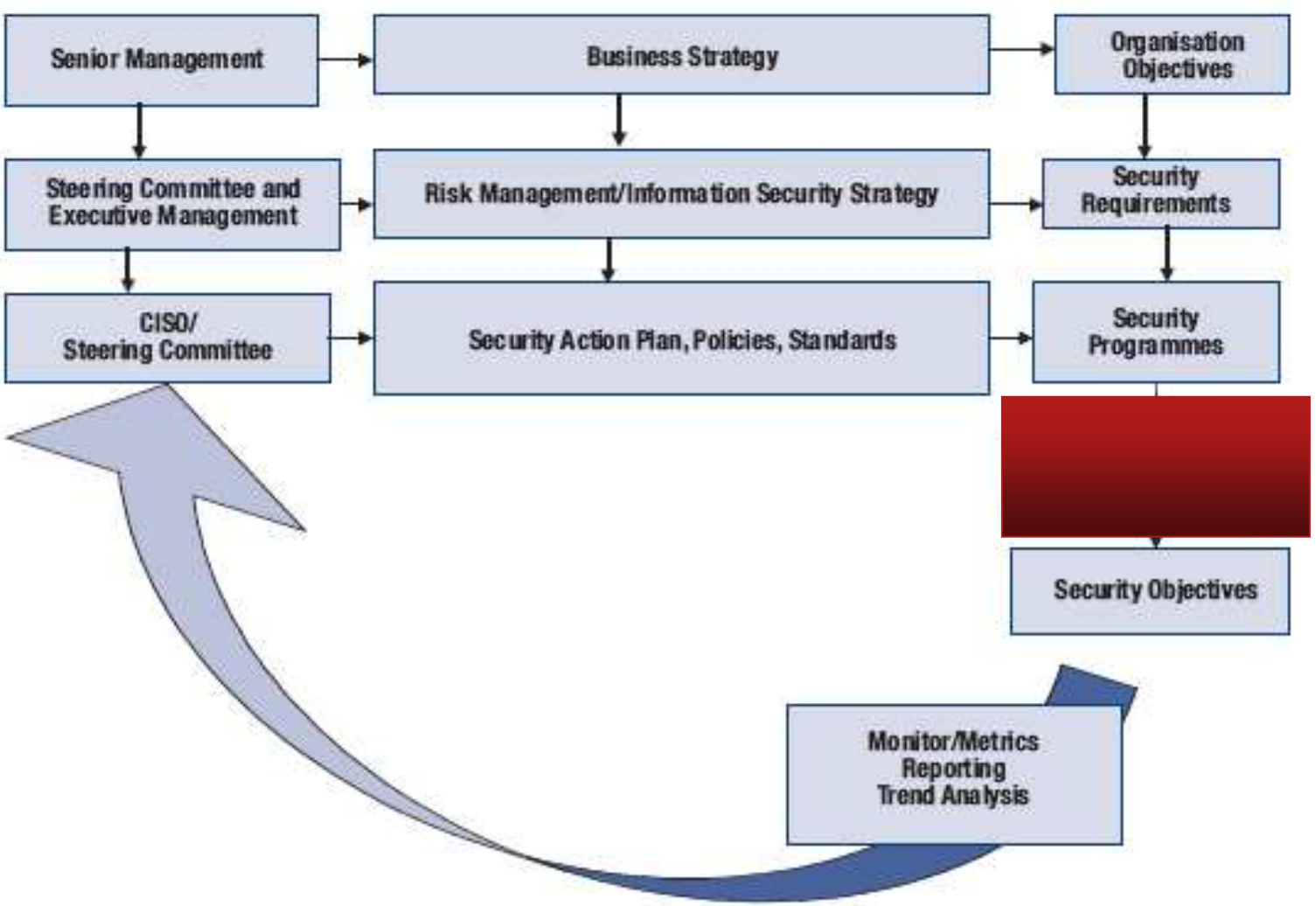


Source: Gartner (January 2007)

Резюме: ИБ Governance

- Способность показать, как ИБ связана с бизнес-стратегией
- Способность показать, как ИБ несет ценность бизнесу
- Способность показать, как ИБ управляет рисками
- Способность показать, как ИБ управляет ресурсами
- Способность показать, как ИБ управляет достижением целей

Структура ИБ Governance



Вопросы?

Дополнительные вопросы Вы можете задать по электронной почте security-request@cisco.com
или по телефону: +7 495 961-1410