- Среда внутреннего контроля
- Риски в сфере ИТ и их оценка
- Вселенная аудита в сфере ИТ: что подлежит аудиту?
- Годовой план
- Примеры

Более чем 60% организаций испытывают серьёзную проблему в части контроля безопасности и целостности своих компьютерных систем

- Информация доступна беспрецедентному числу работников.
- Информацию в распределённых компьютерных сетях сложно контролировать.
- Клиенты и поставщики имеют доступ к системам и базам данных друг друга.
- Некоторые компании рассматривают потерю важной информации как отдалённую и маловероятную угрозу.
- Отсутствует полное понимание последствий с точки зрения контроля при переходе от централизованных систем к системам, использующим интернет.
- Многие компании не осознают, что информация – это стратегический ресурс, и её защита должна быть стратегическим требованием.
- Необходимость повышать производительность и снижать издержки заставляет руководство отказываться от применения мер контроля, которые требуют значительного времени.

Обзор концепций внутреннего контроля

Внутренний контроль – процесс, призванный обеспечить разумную уверенность в достижении следующих целей контроля

Защита активов	Ведение учёта	Предоставление информации	Повышение эффективности	Содействие политикам	Соблюдение нормативных положений
Предупреждение или выявление несанкционированного приобретения, использования или отчуждения	Достаточная степень детализации для точного и справедливого отражения активов компании	Точная и достоверная	Содействовать операционной эффективности и повышать её	Поощрять следование предписанным политикам	Соблюдение применимых законов и нормативных положений

Внутренний контроль – неотъемлемая часть управленческой деятельности

Типы средств внутреннего контроля *(важные функции)*

Средства предотвращения

Предупреждают возникновение проблем

Пример:

- ✓ наём квалифицированного персонала, разделение обязанностей сотрудников,
- ✓ контроль физического доступа к активам и информации

Средства выявления

Выявляют проблемы, которые не удалось предотвратить

Пример:

повторная проверка расчётов, банковская сверка и ежемесячная подготовка пробного баланса

Средства исправления

Позволяют исправлять проблемы а также исправлять возникающие ошибки и восстанавливаться от их последствий.

Пример:

хранение резервных копий файлов, исправление ошибок, допущенных при вводе данных

Общие средства контроля

Обеспечить стабильность контрольной среды организации и эффективное управление ею

Пример: инфраструктура ИТ; приобретение, разработка и обслуживание ПО

Средства контроля в отношении прикладного использования

Предупреждают, выявляют и исправляют транзакционные ошибки и мошенничество при использовании прикладных программ

Средства контроля в отношении **вводимых ресурсов – обработки - результата**

Пример: процедуры санкционирования ввода, подтверждения и редактирования данных

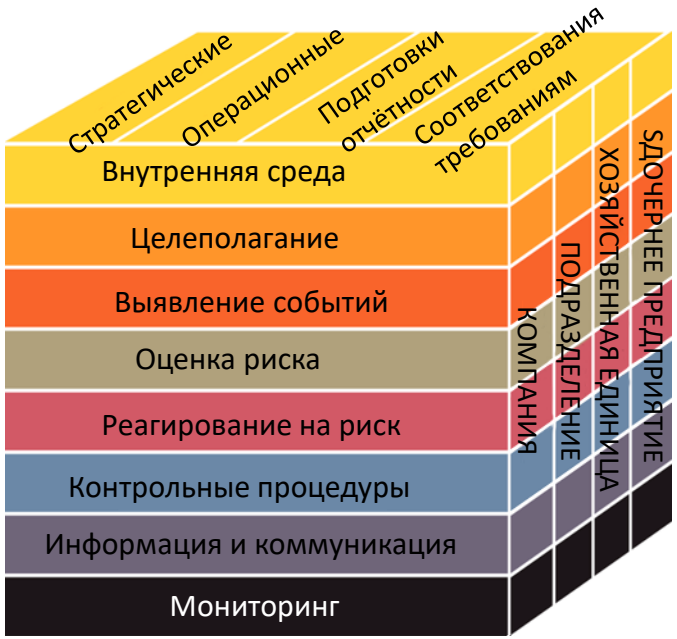
Что такое риск?

Согласно определению COSO, это – **событие, происшествие** или случай, обусловленные **внутренними или внешними источниками**, которые **сказываются на реализации стратегии или достижении целей**.

Их воздействие может быть **положительным** или **отрицательным**, или сочетать эти эффекты».

Возможность

РИСК



Руководству необходимо стремиться предвидеть все возможные позитивные или негативные события, определять, какие из них наиболее/наименее вероятны, и понимать взаимосвязь между событиями.

Пример - внедрение системы электронного обмена данными (ЭОД), в которой электронные документы формируются передаются клиентам и поставщикам, и куда поступают ответы в электронном виде.

Вот некоторые события, которые могут произойти в компании: выбор неподходящей технологии; несанкционированный доступ; утрата целостности данных; незавершённые операции; отказ системы; несовместимость систем.

Оценка риска и реагирование на риск

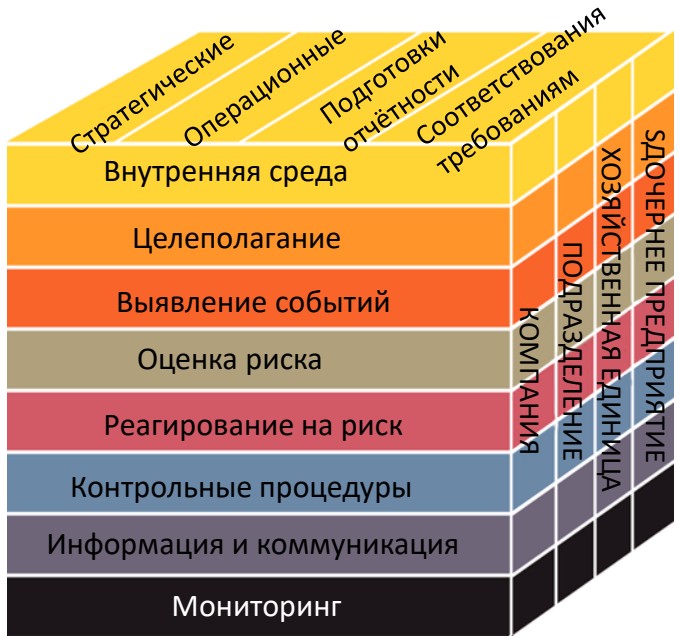
Присущий риск

Согласно определению COSO, присущий риск – это риск, связанный с функционированием организации в условиях отсутствия **каких-либо управленческих действий** (реагирования на риск), призванных изменить **вероятность** реализации риска или **воздействие** в случае его реализации**.**

Остаточный риск

Остаточный риск – это риск, который сохраняется после реагирования менеджмента на существование риска

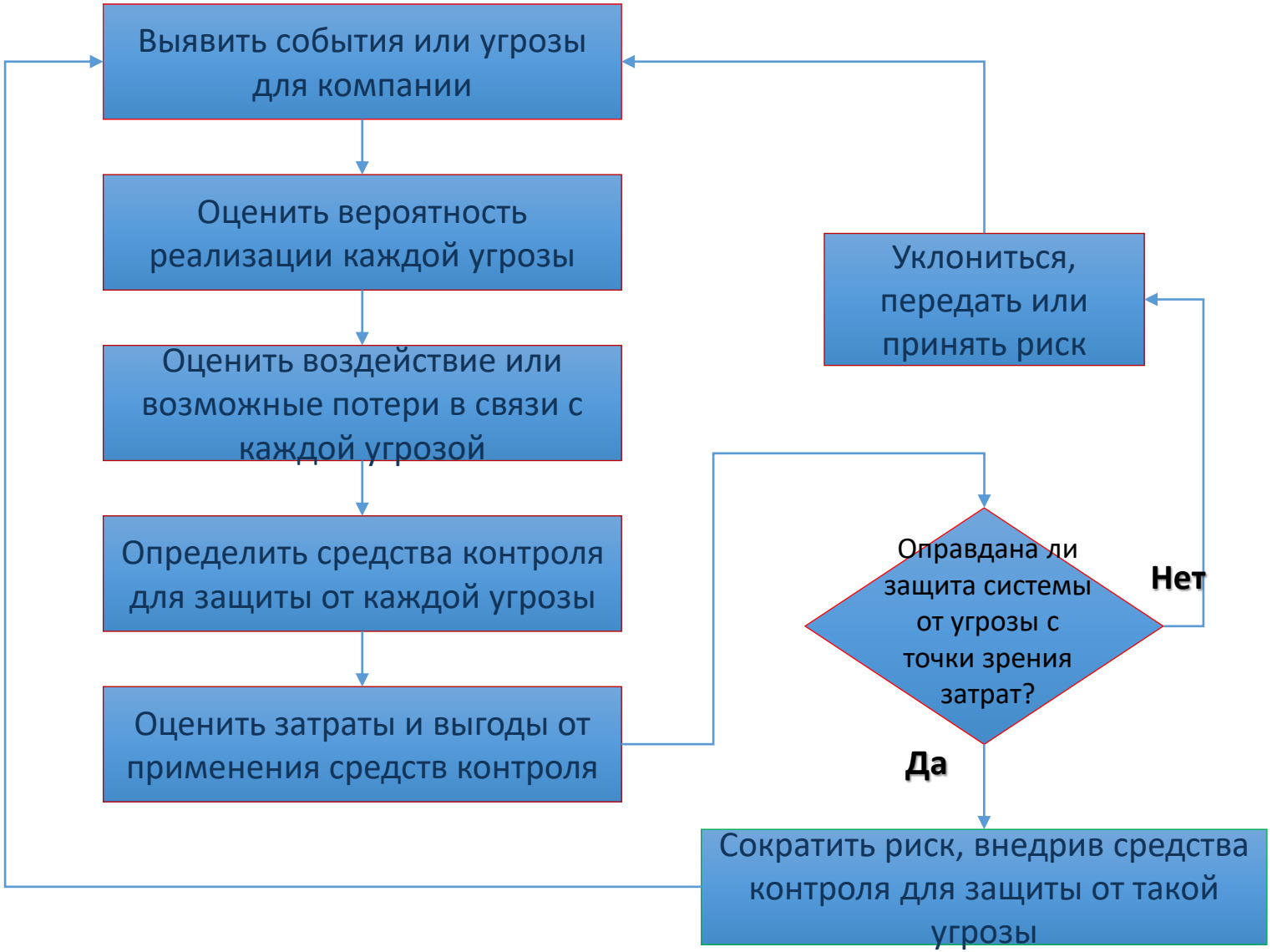
Для того, чтобы согласовать выявленные риски с готовностью компании идти на риск, руководству необходимо рассматривать риски применительно ко всей организации. Оно должно оценивать вероятность и воздействие риска, а также затраты и выгоды, связанные с разными **вариантами реагирования** на него.



Сократить | **Принять** | **Передать** | **Уклониться**

Оценка риска и разработка средств внутреннего контроля

Руководству следует разрабатывать действенные системы внутреннего контроля (ВК), чтобы снижать присущий риск.
В ходе ВА *(аудита ИТ)* следует оценивать системы ВК, чтобы обеспечить их действенное функционирование.



Определение контроля и анализ затрат и выгод

Руководству следует определить средства контроля, которые защищают компанию от каждого события

- **Предотвращение**
- **Выявление**
- **Исправление**

Цель создания системы ВК – обеспечить разумную уверенность в том, что события не происходят

Средства внутреннего контроля

Избыток средств контроля стоит дорого и негативно сказывается на эффективности операционной деятельности

Если средств контроля слишком мало, то они не обеспечат необходимую разумную уверенностьТ

Выгоды от процедуры ВК должны превышать связанные с ней затраты!

- **Как измерить выгоды?**
- **Как измерить затраты?**

Ожидаемый ущерб = **Вероятность** X **Воздействие**

Риск = **Вероятность** X **Воздействие**

Риск = Угроза x Уязвимость

Следует помнить о двух особых случаях:

Если какой-либо из факторов равен нулю, то даже если все остальные очень важны или существенны, то и риск будет равен нулю.

Риск предполагает неопределённость. Если что-то обязательно произойдёт то это – не риск.

Пример

В ОС Windows существует уязвимость повышения привилегий, т.е. компонент Win32k не может должным образом работать с объектами в своей памяти («уязвимость повышения привилегии Win32k»).
Эта уязвимость затрагивает:

- Windows 7,
- **Windows Server 2012 R2**,
- Windows RT 8.1,
- **Windows Server 2008**,
- **Windows Server 2019**,
- **Windows Server 2012**,
- Windows 8.1,
- Windows Server 2016,
- **Windows Server 2008 R2**,
- Windows 10

This CVE ID is unique from CVE-2018-8641.

Ежегодная оценка риска

Оценка риска на основании шести Критериев

- Стратегический
- Репутационный
- Финансовый
- Сложности процесса
- Управление ИТ и информацией
- Персонал

#	Процесс	Risks												
		Strategic	Reputation	Financial	Process Complexity	IT and information	Governance	Human Resource	IA Total 2018	IA Total 2017	IA Total 2016	Management average 2018	Management Average 2017	Management Average 2016	Difference
Основной процесс		a										b			c = a - b
A.1 – Управление финансами	Бюджетирование Контроль и учёт	4	4	2	4	3	3	20	20	20		22	20.5	15.3	(2)
A.2 – Микроэкономическая политика	Развитие	4	4	4	4	4	4	24	24	24		23	23.5	17.3	1
A.3 – Политика бухучёта и аудита	Внедрение Разработка и внедрение	4	4	4	3	2	2	19	19	17		19	16.4	17.3	0
A.4 – Информационная безопасность	Управление в сфере информационной безопасности	4	4	2	4	4	4	22	22	22		22	23.0	16.3	(0.5)

Рейтинг риска		Итого	Периодичность аудита
Высокий	4	21-24	Каждый календарный год
Выше среднего	3	17-20	Каждые 2 года
Средний	2	13-16	Каждые 3 года
Низкий	1	6-12	По усмотрению ГА, АК или Совета директоров

Ежегодная оценка риска в области ИТ (на базе Cobit)

	B	C	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1																	
2					Ответить на каждый вопрос, оценивая по шкалеот 1 до 4 *(1-не важный, 4-очень важный)*												
3				**Присущий риск**						**Внутренний контроль**							
4	Процесс №		Остаточный риск (B, C, H)	Суммарное значение присущего риска	Является ли упомянутая операция критической для ЦБ	Влияют ли ошибки и потери на авторитет ЦБ	Ведут ли к нарушению законодательства допущение ошибок и понесении потерь?	Имеет ли финансовое воздействие допущении ошибок и понесении потерь	Насколько реализация операции зависит от внешних факторов?	Суммарное значение мер внутреннего контроля	Присущий внутреннему контролю уровень механизма по отношению к операции	Были ли прежде выявлены ошибки и пробелы	Насколько состоящийся этот аспект?	Насколько урегулировано этого процесса	Зависит ли ралиазация процесса от одного специалиста?	Суммарное значение остаточного риска	**Периодичность проверок**
5		Процессы			25	25	15	25	10		25	25	20	15	15		
6	**Планирование и организация (ПО)**																
7	ПО 1	Разработка стратегического плана в области IT.	H	400	4	4	4	4	4	400	4	4	4	4	4	16.0	1 год
8	ПО 2	Разработка информационной архитектуры.	L	185	2	1	1	3	2	210	1	2	3	3	2	1.9	5 лет
9	ПО 3	Определение вектора технологического развития.	L	0						0						0.0	5 лет
10	ПО 4	Определение ИТ-процессов, организации и взаимодействия.	L	0						0						0.0	5 лет
11	ПО 5	Управление инвестициями в сфере ИТ.	L	0						0						0.0	5 лет
12	ПО 6	Информирование о целях и задачах управления.	L	0						0						0.0	5 лет
13	ПО 7	Управление кадрами в сфере ИТ.	L	0						0						0.0	5 лет
14	ПО 8	Управление качеством.	L	0						0						0.0	5 лет
15	ПО 9	Доступ и управление рисками в сфере ИТ.	L	0						0						0.0	5 лет

Вселенная аудита в области ИТ

- Риск-ориентированный подход

- Систематичный и комплексный подход *(не должно иметься ни одной сферы, связанной с работой, административными функциями или ИТ, в отношении которой никогда не проводится аудит)*

Вселенная аудита в сфере ИТ

Единицы аудита в сфере ИТ

- Планирование и управление ИТ
- Сети, ОС, СУБД
- Приобретение и разработка ИТ
- Управление риском и ОНБ
- Физическая и техническая безопасность

Процессы CobIT

- Планирование и организация
- Приобретение и внедрение
- Предоставление и поддержка
- Мониторинг и оценка

Единица аудита	Ед. аудита по COBIT	В плане на 2018	В плане на 2019	В плане на 2020
Планирование и управление ИТ	PO1		X	
	PO2		X	
	PO3		X	
	PO4		X	
	DS3		X	
Планирование и управление ИТ – мониторинг	PO8			X
	M1			X
	M2			X
	M3			X
	M4			X
Сети	DS9	X		X
	DS10	X		X
	DS13	X		X
	AI6	X		X
База данных	DS9	X		X
	DS10	X		X
	DS11	X		X
	DS13	X		X
	AI6	X		X
	AI7	X		X
ОС	DS9		X	
	DS10		X	
	DS13		X	
	AI6		X	
	AI7		X	
Приобретение и разработка ИТ-приложений	AI1	X		X
	AI2	X		X
	AI3	X		X
	PO10	X		X
План непрерывности деятельности	DS1		X	
	DS2		X	
	DS4		X	
	DS8		X	
Информ. безоп-ть согласно ISO27001:2013	DS5	X	X	X
Физическая и техническая безопасность	DS12	X		X

Департамент ИТ

- **Инфраструктура ИТ**
  - ЦОД
  - Сетевое оборудование
  - Серверы *(Linux u Windows)*
  - ОС
  - Приложения
- **Персонал**
  - сотрудники

Объекты аудита в сфере ИТ

- Приложения:
  наборы взаимосвязанных компьютерных программ и соответствующих данных, обеспечивающие один (*или более*) бизнес-процесс.

- Часто аудит распространяется и на поддерживаемый бизнес-процесс (*комплексный аудит*)

Объекты аудита в сфере ИТ

Инфраструктура ИТ:

- Аппаратные средства и/или ПО, которые поддерживают одну или несколько систем приложений
- Могут рассматриваться как отдельные объекты аудита, либо проходить аудит вместе с поддерживаемой системой приложений

Примеры:

- ✓ Сетевая безопасность
- ✓ Электронная почта
- ✓ Интранет
- ✓ ОС
- ✓ СУБД

Объекты аудита в сфере ИТ

- Процессы управления ИТ:

  Деятельность персонала в Департаменте ИТ согласно описанию в CobiT и ITIL

- Общие средства контроля *(применимы к нескольким инфраструктурам и приложениям)*

Объекты аудита в сфере ИТ

- Процессы управления в сфере ИТ - примеры:
  - Управление инцидентами
  - Управление изменениями
  - Управление конфигурацией
  - Управление уровнем обслуживания
  - Управление безопасностью
  - Управление производительностью

Объекты аудита в сфере ИТ

День 1, Презентация 3

Подходы к аудиту в сфере ИТ

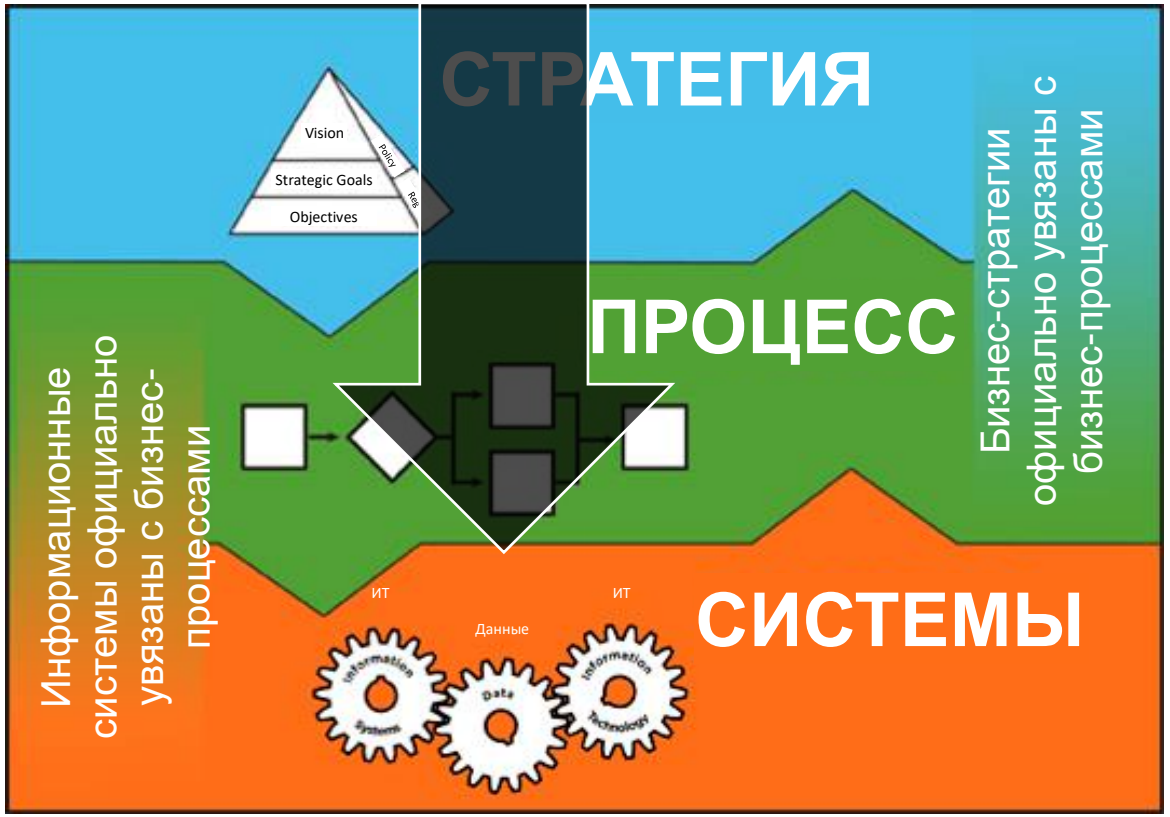
Как проводить аудит систем ИТ?

Подходы к аудиту в сфере ИТ

Подходы к аудиту в сфере ИТ

1 Вертикальный

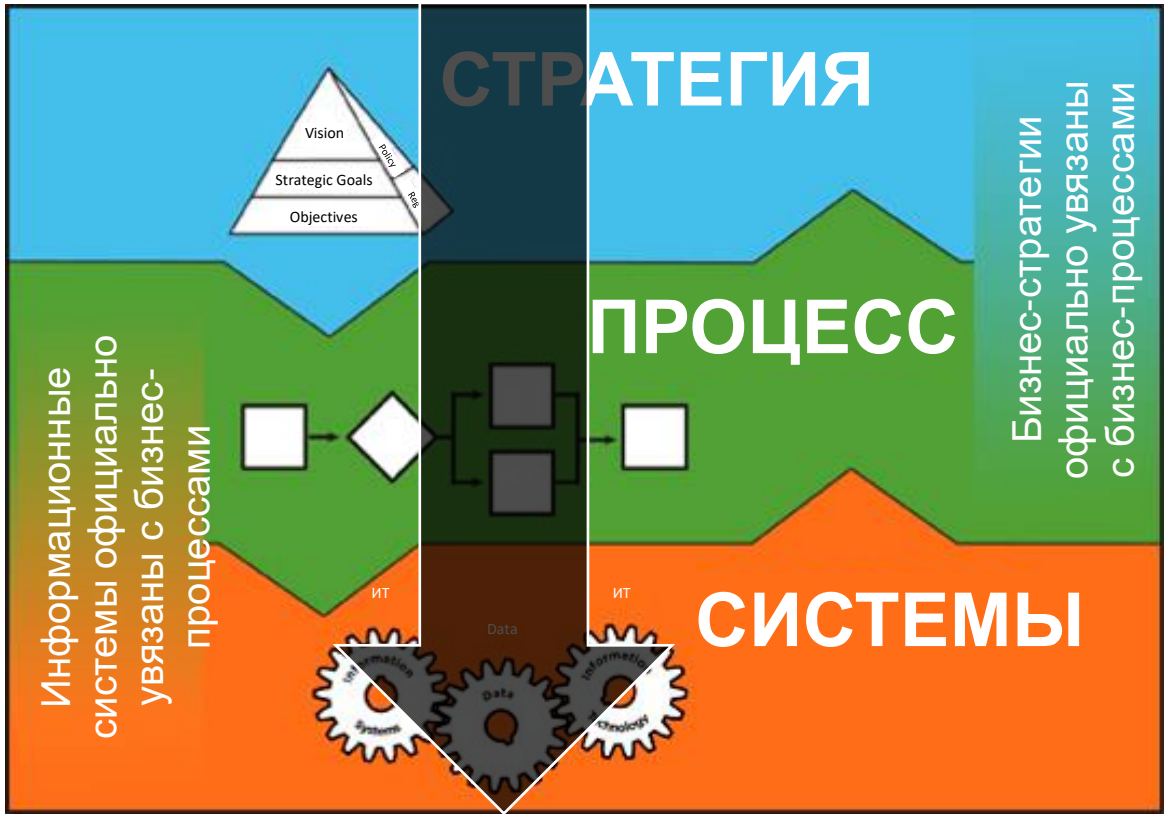
Общие средства контроля применительно к ИТ в бизнес-процессе



Подходы к аудиту в сфере ИТ

2 Глубокий вертикальный

- ✓ Общие средства контроля в ИТ
- ✓ Средства контроля в отношении прикладного использования



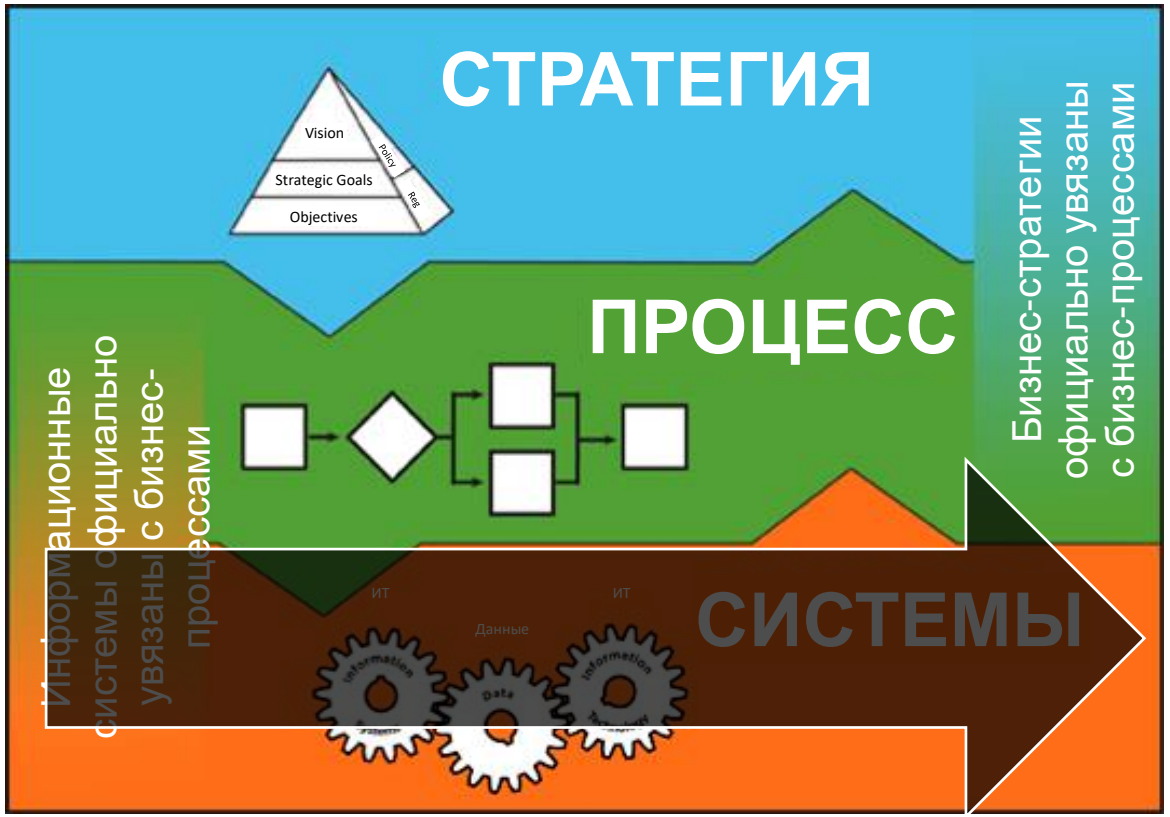
Подходы к аудиту в сфере ИТ

3 Горизонтальный

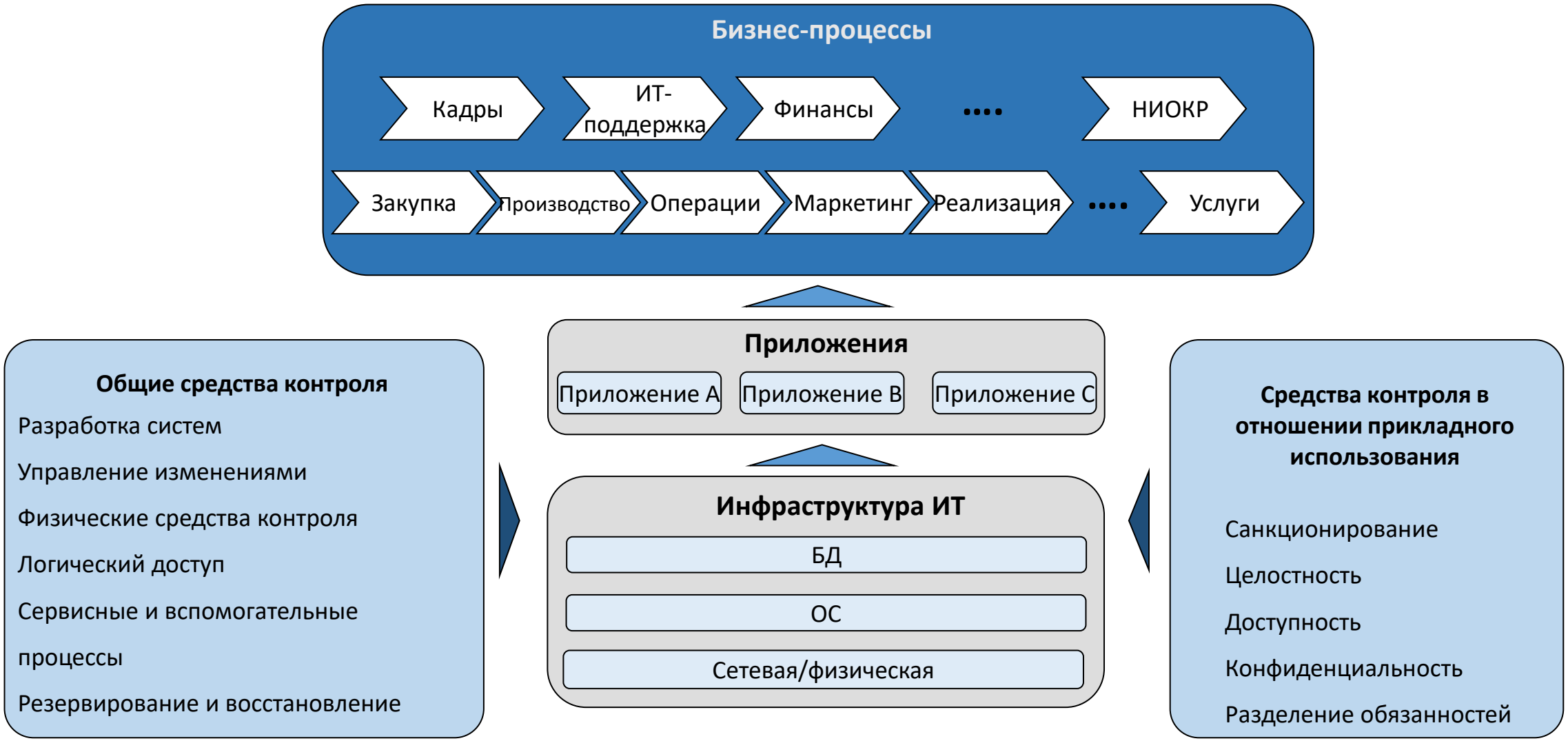
Все актуальные средства контроля в сфере ИТ

Примеры:

- ✓ Информационная безопасность
- ✓ Управление базами данных
- ✓ Техническая поддержка



Подходы к аудиту в сфере ИТ, ОСК ИТ



Подходы к аудиту в сфере ИТ

Что ещё???

- **Аудит до внедрения**
  - На этапе разработки и внедрения новых приложений, инфраструктуры или ИТ-процессов либо при любых существенных изменениях в уже имеющихся
- **Аудит после внедрения**
  - Когда приложения, инфраструктура или ИТ-процессы уже функционируют

Обеспечивая независимость

Старайтесь не участвовать непосредственно в разработке

Обозначьте необходимость в «ключевых средствах контроля», но не конкретизируйте их формы

Заранее обговорите основные правила участия

Аудит до и после внедрения проводится разными группами

Предпосылки для успеха

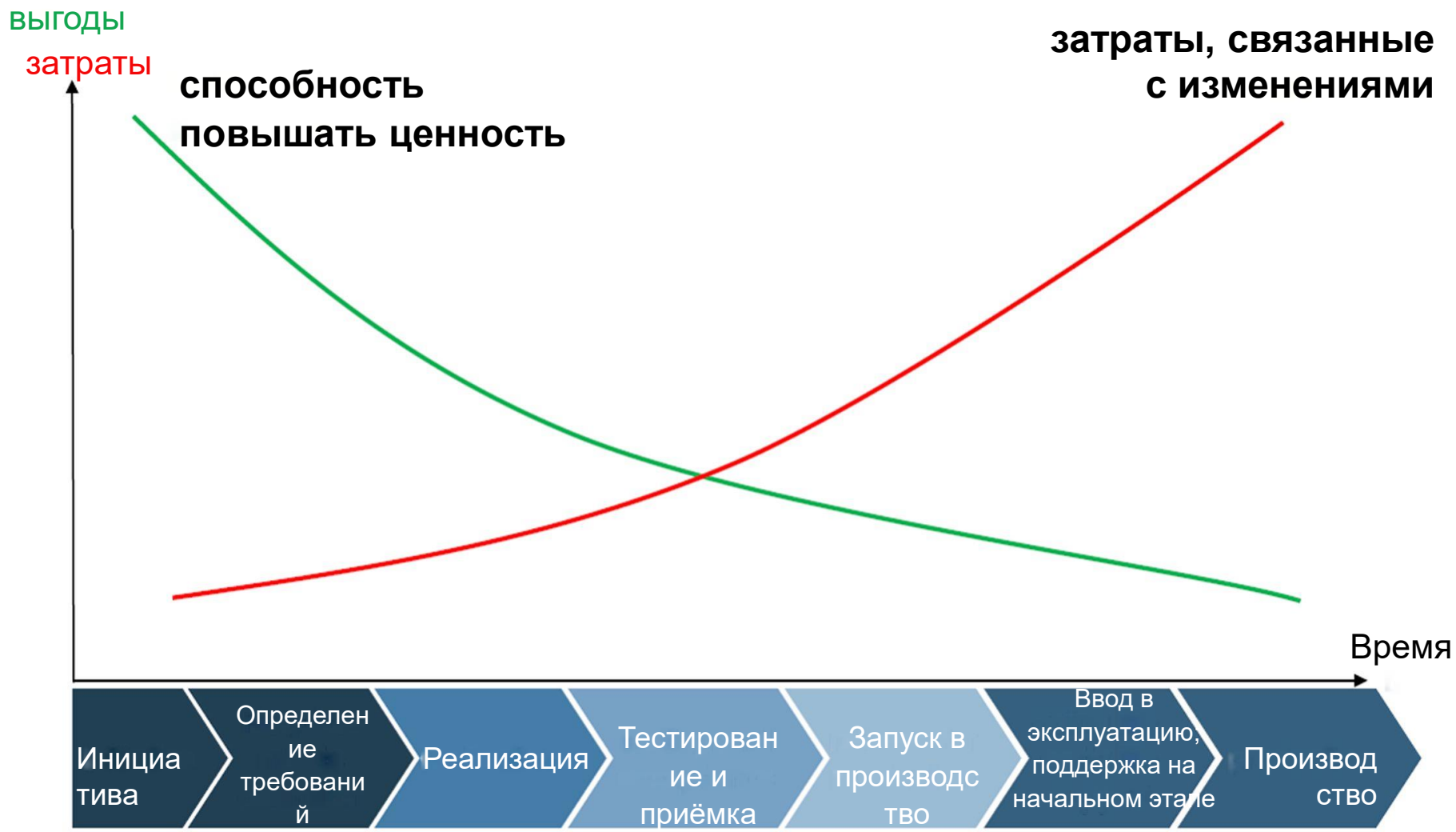
Предпосылки для успеха

- Следует начинать на этапе запуска проекта
- Между руководителем проекта и аудитором необходимо обеспечить эффективную координацию
- Должен выполняться параллельно проекту
- Результаты необходимо представлять своевременно

Проблемы

- Аудиторов могут воспринимать как членов проектной команды
- Участие в аудите до внедрения может скомпрометировать независимость аудитора
- При аудите до внедрения аудитор обычно получает для ознакомления только предварительные варианты документов

Польза благодаря аудиту до внедрения



Необходимые навыки

Общие навыки и опыт в сфере аудита

Общее представление о процессах, которые будет поддерживать создаваемое приложение

Навыки проектного управления

Знания и опыт в качестве аудитора в сфере ИТ

Прочие соображения

О чём стоит подумать...

Поручать старшим аудиторам в группе, которые обладают самым значительным опытом в этой области.

Участие аудитора должно начинаться одновременно с началом формирования группы разработчиков, и не позднее оглашения требований пользователей.

Вряд ли будет осуществляться на постоянной основе, - скорее, на ключевых этапах процесса разработки.

Первый аудит новой системы после внедрения – не ранее, чем черед полгода после её передачи пользователю/оператору.

Стандарты, методы и инструменты

Стандарты, методы и инструменты

- ✓ **GTAG 11** –Практическое(ие) руководство(а) для Главного аудитора и внутренних аудиторов по разработке риск-ориентированного плана аудита в сфере ИТ.
- ✓ **GAIT** – риск-ориентированная методология оценки объёма общих средств контроля в сфере ИТ

- ✓ **Рамочная основа COBIT,** цели контроля, модели зрелости и руководство по обеспечению уверенности применительно к процессам в сфере ИТ

- ✓ ISO 27002 *(нормы и правила в сфере управления информационной безопасностью)*
  - ✓ Руководства, средства контроля и методики для управления информационной безопасностью
- ✓ Руководство по аудиту систем управления информационной безопасностью

- ✓ **PMBOK** (при совмещении COBIT и PMBOK) можно использовать для разработки вселенной аудита и ОСК ИТ для процесса управления проектами.

Этапы обеспечения уверенности относительно процесса

По каждому процессу необходимо пройти следующие этапы обеспечения уверенности. Проверьте:

Этап 1 Определены цели и задачи процесса?

Этап 2 Определён ответственный за процесс?

Этап 3 Определены функции и обязанности?

Этап 4 Определена политика, планы и процедуры?

Этап 5 Имеется программа повышения эффективности процесса?

Как использовать Cobit при планировании и проведении аудита в сфере ИТ

По каждому процессу используется следующая структура

Задача управления

Требования высокого уровня, которые необходимо учитывать в интересах эффективного контроля каждого ИТ-процесса. Формулируются как краткие, ориентированные на действия управленческие практики.

Определяющие факторы ценности

Примеры выгод для бизнеса, которые можно получить благодаря эффективному контролю

Определяющие факторы риска

Примеры рисков, которые может потребоваться избегать или снижать

Проверка структуры управления

Обеспечивает руководство на уровне задачи управления для специалистов по обеспечению уверенности, которые выполняют этот процесс в отношении ИТ. Этапы выведены из практики контроля, которая, в свою очередь, формулируется исходя из каждой задачи управления. Этапы проверки уверенности:

– оценить структуру средств контроля
– подтвердить, что средства контроля введены в действие
– оценить операционную эффективность контроля

Пример - DS5 Обеспечить безопасность систем

Задача управления	Определяющие факторы ценности	Определяющие факторы риска
DS5.1 Управление безопасностью в сфере ИТ Управлять безопасностью в сфере ИТ на самом высоком надлежащем уровне в организации, так чтобы управление действиями в части безопасности соответствовало требованиям бизнеса.	• Критические ИТ-активы защищены • Стратегия безопасности в сфере ИТ поддерживает потребности бизнеса • Стратегия в безопасности в сфере ИТ согласована с общим планом бизнеса • Практика обеспечения безопасности надлежащим образом реализована, поддерживается и соответствует применимым законам и нормативным актам	• Управление безопасностью в сфере ИТ отсутствует • Цели в области ИТ и цели бизнеса не согласованы • Данные и информационные активы не защищены

Проверка структуры управления

• Определить, имеется ли координационный комитет по вопросам безопасности, в котором представлены ключевые функциональные области, включая ВА, безопасность в сфере ИТ и правовой отдел.
• Определить, существует ли процесс для определения приоритетности предлагаемых инициатив в сфере безопасности, в т.ч. требуемые уровни политик, стандартов и процедур.
• Выяснить и подтвердить наличие хартии по безопасности в сфере ИТ.
• Рассмотреть и проанализировать хартию, чтобы убедиться, что информационная безопасность в ней соотносится с приемлемым для организации уровнем риска, и что в неё в явном виде включены:
  - Объём ответственности и цели подразделения, отвечающего за управление безопасностью
  - Обязанности подразделения, отвечающего за управление безопасностью
  - Факторы, способствующие соблюдению положений и риску
• Выяснить и подтвердить, что политика в сфере информационной безопасности охватывает обязанности совета директоров, высшего и среднего звена управления, сотрудников и всех пользователей ИТ-инфраструктуры предприятия, и что в ней есть ссылки на подробные стандарты и процедуры безопасности.
• Выяснить и подтвердить наличие детальной политики информационной безопасности, стандартов и процедур. Примеры политики, стандартов и процедур:
  - Политика обеспечения соблюдения требований безопасности
  - Степень допустимого риска для руководства (признание невыполнения требований безопасности)
  - Политика обеспечения безопасности при использовании средств внешней связи
  - Политика в отношении использования межсетевых экранов
  - Политика обеспечения безопасности при использовании электронной почты
  - Согласие следовать положениям политики в сфере ИБ
  - Политика обеспечения безопасности при пользовании ПК/ноутбуком
  - Политика в отношении пользования Интернетом

Заключительные соображения …

Единого «рецепта» не существует. **Однако есть ряд важных факторов**:

Эффективная вселенная аудита в сфере ИТ **предусматривает риск-ориентированный подход, который соотносит каждый элемент ИТ с бизнес-процессом**, который, в свою очередь, коррелирует со стратегическими целями.

ГА следует **продемонстрировать руководству,** как вселенная аудита в сфере ИТ повысит ценность каждого рассматриваемого процесса, а также как каждый процесс может повлиять на стратегические цели и задачи организации.

При определении и подтверждении вселенной аудита в сфере ИТ ГА необходимо добиться **вовлечённости и, по возможности, реакции** руководства.

Благодаря заинтересованности и поддержке со стороны руководства ГА и внутренние аудиторы в сфере ИТ могут эффективнее доносить свои рекомендации.


Thank You