Авторское изложение COBIT для ИТ аудиторов

Александр Астахов, CISA
Рабочая группа ISACA.RU

Оглавление

Введение

Как родилась эта статья? Занятый подготовкой учебного курса по аудиту безопасности информационных систем, автор не смог обойти вниманием COBIT – стандарт ориентированный, прежде всего, на руководство организации и на ИТ аудиторов и регламентирующий вопросы управления ИТ. COBIT является синтезом четырех десятков международных стандартов (де-юре и де-факто) в области управления ИТ, аудита, контроля и информационной безопасности. Его основной стратегической задачей является ликвидация разрыва между руководством организации с их видением бизнес целей и ИТ департаментом, осуществляющим поддержку важнейшей для любой современной организации информационной инфраструктуры, которая должна работать на достижение этих целей. Задача эта очевидно является сильно нетривиальной, что подтверждается бросающейся в глаза неоднозначностью явления под названием COBIT. Многократное повторение одних и тех же, в сущности весьма немудренных, мыслей в одной и той же, либо слегка модифицированной форме, сделало возможным при подготовке курса опустить большинство параграфов без потери смысла. Стремление сделать этот стандарт как можно более универсальным и независящим не от технических платформ, не от отраслевых особенностей функционирования организации возводит авторов на такой высокий уровень абстракции, с которого порой перестает видиться предмет изучения. Впрочем стиль изложения и используемая терминалогия также оставляют желать много лучшего. Другими словами, несмотря на уникальность, всеобъемлемость, универсальность COBIT и важность затрагиваемых вопросов, он производит весьма неоднозначное впечатление.

Получившаяся статья является изложением основных положений COBIT с точки зрения ИТ аудитора. Автор даже смеет надеятся на то, что она может заменить чтение самого стандарта, т.к. он старался не упустить не одной ключевой мысли, а также схемы, модели, понятия и т.п., являющихся полезными для практики. «Руководство по аудиту» (Audit Guideline) здесь изложено в полном объеме, также как и «Концептуальное ядро COBIT» (COBIT Framework), являющее основой для понимания всех основных положений стандарта. Однако данная работа не является переводом COBIT, за исключением Приложений для которых был сделан практически дословный перевод соответствующих разделов стандарта, чтобы читатель смог получить более точное представление об этом документе и стиле изложения материала в нем.

Используемая терминология

Дадим определение нескольким ключевым для COBIT понятиям, на которых строится все изложение и которые, скорее всего, могут вызвать неоднозначность толкования у читателей.

Control	Механизм управления	Политики, процедуры, практики и организационные

		структуры, предназначенные для предоставления обоснованных гарантий достижения бизнес целей, а также предостващения, детектирования и корректировки нежелательных событий.
Control Objective	Задача управления	Формулировка желаемого результата или цели, которые должны быть достигнуты путем реализации механизмов управления в рамках конкретного ИТ процесса.
COBIT	Задачи управления для информационных и смежных технологий	Control Objectives for Information and related Technology - Международный стандарт, определяющий набор универсальных задач управления ИТ, ориентированных, прежде всего, на руководство организации и на ИТ аудиторов.
COBIT Framework	Концептуальное ядро COBIT	Набор основополагающих принципов и понятий, высокоуровневых задач управления, а также модель управления ИТ, на базе которых строятся все положения COBIT. Основная концепция COBIT предполагает построение механизмов управления в ИТ исходя из того, какая информация необходима для поддержания бизнес целей и удовлетворения требованиям бизнеса. При этом информация рассматривается как результат использования ИТ ресурсов, управление которыми осуществляется в рамках ИТ процессов.
IT Governance	Система управления информационными технологиями	Структура взаимосвязей и процессов, определяющих направление и осуществляющих управление предприятием с целью достижения бизнес целей путем получения добавленной стоимости при наличие баланса между величиной рисков и возвратом инвестиций, сделанных в ИТ.

Остальные важные для COBIT понятия определяются по ходу изложения.

История создания COBIT

COBIT является результатом обобщения мирового опыта, международных и национальных стандартов и руководств в области управления ИТ, аудита и информационной безопасности. В состав интернациональной команды разработчиков COBIT входят специалисты государственных и коммерческих предприятий, учебных заведений и фирм, специализирующихся на вопросах безопасности и управления ИТ.

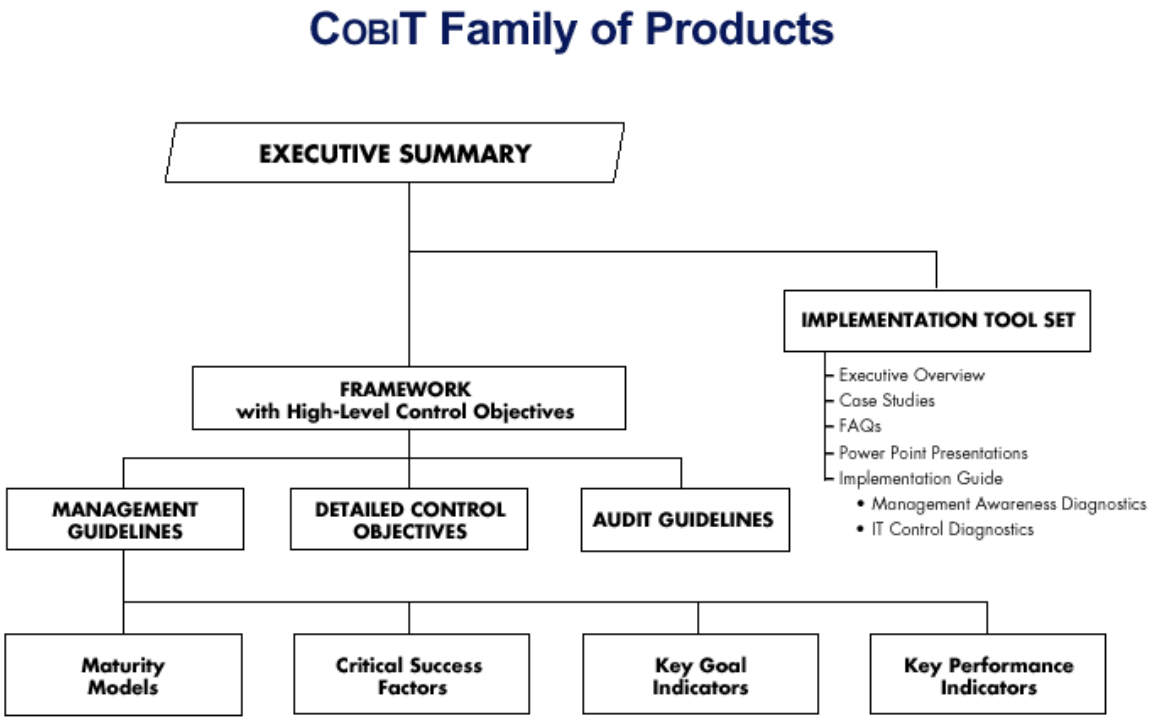
Первая версия стандарта была выпущена в 1996 году Организацией Аудита и Контроля Информационных Систем (Information Systems Audit and Control Foundation (ISACF)). Она включала в себя Концептуальное ядро (COBIT Framework), определяющее набор основополагающих принципов и понятий в области управления ИТ, описание Задач управления (Control Objectives) и «Руководство по аудиту» (Audit Guideline). Вторая версия COBIT была опубликована в 1998 году. Она содержала переработанную версию высокоуровневых и детальных Задач управления, дополненных «Набором

Инструментов Внедрения» (Implementation Tool Set). Третья редакция стандарта была выпущена уже Институтом управления ИТ (IT Governance Institute), учрежденным Ассоциацией Аудита и Контроля ИС (Information Systems Audit and Control Association (ISACA)) совместно с ISACF с целью дальнейшего развития и популяризации принципов управления ИТ. Институт управления ИТ в настоящее время является основным разработчиком COBIT. В третьей версии стандарта появилось «Руководство для менеджеров» (Management Guidelines) в основе которого лежит понятие «Система управление ИТ» (IT Governance).

Структура и состав документов

В состав третьей редакции COBIT входит несколько книг, включая Резюме для руководства (Executive Summary), Концептуальное ядро (Framework), Руководство по менеджменту (Management Guideline), Руководство по аудиту (Audit Guideline) и Детальные задачи управления (Detailed Control Objectives), а также Набор инструментов внедрения (Implementation Tool Set).

Описанная структура COBIT показана на рисунке.



Резюме для руководства

Резюме для руководства (Executive Overview) служит введением в остальные разделы стандарта. Оно содержит общие сведения о стандарте, определяет Миссию COBIT (COBIT Mission) и понятие Системы управления ИТ (IT Governance).

Эффективное управление ИТ является чрезвычайно важным фактором для выживания и успеха организации. Многие организации осознают потенциальные выгоды, связанные с использованием высоких технологий. Однако только успешные организации способны адекватно оценивать и управлять рисками, связанными с внедрением этих технологий. **Система управления ИТ** (IT Governance) в настоящее время признается ключевой частью **Системы управления предприятием** (Enterprise Governance). Это понятие является одним из основных в COBIT. Система управления ИТ определяется в COBIT как *структура взаимоотношений и процессов, задающих направление и осуществляющих управление предприятием с целью достижения бизнес целей путем получения добавленной стоимости при наличие баланса между величиной рисков и возвратом инвестиций, сделанных в ИТ.*

COBIT является инструментом, позволяющим руководству предприятия обеспечить переход от постановки бизнес задач к вопросам управления ИТ, помогая установить должный уровень понимания рисков и преимуществ, связанных с использованием ИТ и реализовать эффективную систему управления ИТ, направленную на достижение бизнес целей предприятия.

Миссия COBIT *состоит в исследовании, разработке, рекламе и продвижении международного набора авторитетных, отвечающих современным требованиям, общепризнанных Задач управления (Control Objectives) ИТ для повседневного использования бизнес менеджерами и аудиторами.*

Таким образом, COBIT является связующим звеном между бизнес рисками, задачами управления и технической инфраструктурой. Он представляет лучшие практики, объединенные в структуру доменов и процессов, которые позволяют оптимизировать инвестиции в ИТ и предоставляют критерии для оценки эффективности управления ИТ.

COBIT ориентирован прежде всего на ИТ менеджеров, руководителей предприятий и владельцев бизнес процессов, которые должны убедиться в наличие системы внутреннего контроля, поддерживающей бизнес процессы и устанавливающей роль каждого механизма управления в работе по удовлетворению требований к информационному обеспечению бизнеса. Эффективность управления ИТ ресурсами выражается в COBIT посредством критериев *эффективности, продуктивности, конфиденциальности, целостности, доступности, соответствия и надежности* информации, определяемых ниже. Механизмы управления включают в себя политики, организационные структуры, процедуры и

регламенты. **Задачей управления ИТ (IT Control Objective)** является *формулировка желаемого результата или цели, которые должны быть достигнуты путем реализации механизмов управления в рамках конкретного ИТ процесса.*

Концептуальное ядро

Концептуальное ядро COBIT (COBIT Framework) представляет собой *набор основополагающих принципов и понятий, а также модель управления ИТ, на базе которых строятся все положения COBIT.* Основная концепция COBIT предполагает построение механизмов управления в ИТ исходя из того, какая информация необходима для поддержания бизнес целей и удовлетворения требованиям бизнеса. При этом информация рассматривается как результат использования ИТ ресурсов, управление которыми осуществляется в рамках ИТ процессов.

Концептуальное ядро COBIT предоставляет владельцу бизнес процесса инструмент для реализации стратегии управления ИТ. Отправным пунктом является следующее утверждение:

ДЛЯ СВОЕВРЕМЕННОГО И ПОЛНОГО ПОЛУЧЕНИЯ ИНФОРМАЦИИ, НЕОБХОДИМОЙ ОРГАНИЗАЦИИ ДЛЯ ДОСТИЖЕНИЯ БИЗНЕС ЦЕЛЕЙ, УПРАВЛЕНИЕ ИТ РЕСУРСАМИ ДОЛЖНО ОСУЩЕСТВЛЯТЬСЯ ПРИ ПОМОЩИ НАБОРА ЕСТЕСТВЕННЫМ ОБРАЗОМ СГРУППИРОВАННЫХ ПРОЦЕССОВ.

Концептуальное ядро COBIT сформировано из набора 34 высокоуровневых задач управления (одна задача для каждого ИТ процесса), сгруппированных в четыре домена: **планирование и организация**, **комплектование и внедрение**, **предоставление и поддержка**, и **мониторинг**. Такая структура охватывает все аспекты управления и использования ИТ. Выполнение всех 34 задач управления, позволяет гарантировать владельцу бизнес процесса, что система управления ИТ является адекватной задачам бизнеса.

В настоящее время существует два различных класса моделей управления: Модели управления бизнесом (такие как COSO) и специализированные модели управления ИТ (такие как DTI). Целью COBIT является обеспечение перехода от первых ко вторым. COBIT ориентирован в первую очередь на менеджеров и владельцев бизнес процессов, поэтому он оперирует на более высоком уровне абстракции нежели технологические стандарты в области управления ИТ.

Для достижения целей бизнеса информация должна удовлетворять определенным критериям, которые в COBIT называются бизнес требования к информации. Выделяют следующие классы бизнес требований:

Требования качества:

- Качество
- Стоимость
- Доставка

Требования доверия:

- Эффективность и производительность операций
- Надежность информации
- Соответствие нормативным документам

Требования безопасности:

- Конфиденциальность
- Целостность
- Доступность

На основе перечисленных классов требований в COBIT определяются следующие, в некоторой степени пересекающиеся, категории бизнес требований к информации (*информационные критерии*):

Эффективность	effectiveness	актуальность и уместность информации для бизнес процесса, а также ее своевременность, корректность, непротиворечивость и практичность
Продуктивности	efficiency	предоставление информации путем наиболее оптимального (продуктивного и экономичного) использования ресурсов
Конфиденциальность	confidentiality	защищенность информации от несанкционированного раскрытия
Целостность	integrity	точность и полнота информации, а также ее обоснованность с точки зрения ценностей и ожиданий бизнеса
Доступность	availability	возможность получения необходимой информации в течение времени, определяемого требованиями бизнеса. Также включает защиту информации и ее носителей от похищения или

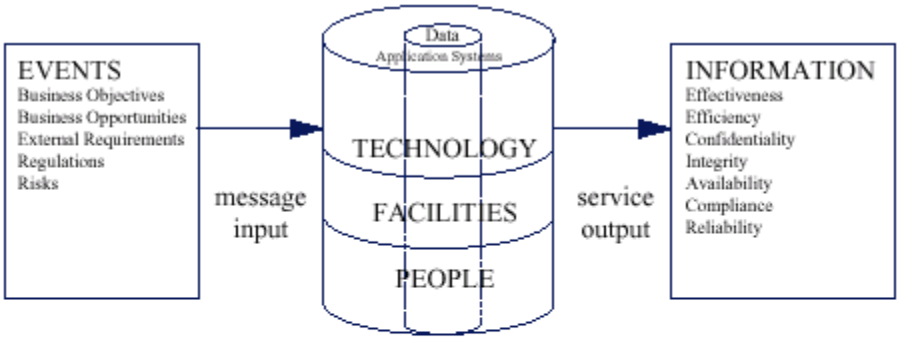
		уничтожения
Соответствие	compliance	соответствие информации законам, распоряжениям и соглашениям, регулирующим бизнес процесс
Надежность	reliability	предоставление руководству информации, пригодной для использования в управлении, для подготовки финансовой и других видов отчетности

В COBIT определяются следующие классы *ИТ ресурсов*:

Данные	data	информационные объекты в самом широком смысле слова (внешние и внутренние), структурированные и не структурированные, графические и звуковые и т.п.
Прикладные системы	application systems	включают в себя не только автоматизированные (программные), но и ручные процедуры
Технологии	technology	Технические средства, операционные системы, системы управления данными, сетевое оборудование и программное обеспечение, мультимедиа и т.д.
Средства поддержки	facilities	вспомогательные ресурсы, оборудование, помещения, необходимые для поддержки функционирования ИС
Люди	people	сотрудники предприятия со своими навыками и опытом, необходимыми для планирования, организации, комплектования, сопровождения, поддержки и мониторинга информационных систем и сервисов

Денежные средства и капитал не рассматриваются в качестве ИТ ресурсов, т.к. они являются средствами инвестирования в любой из перечисленных классов ресурсов.

Структура управления ИТ, оражающая взаимосвязь между бизнес целями, ИТ ресурсами и информационными критериями, показана на рисунке.



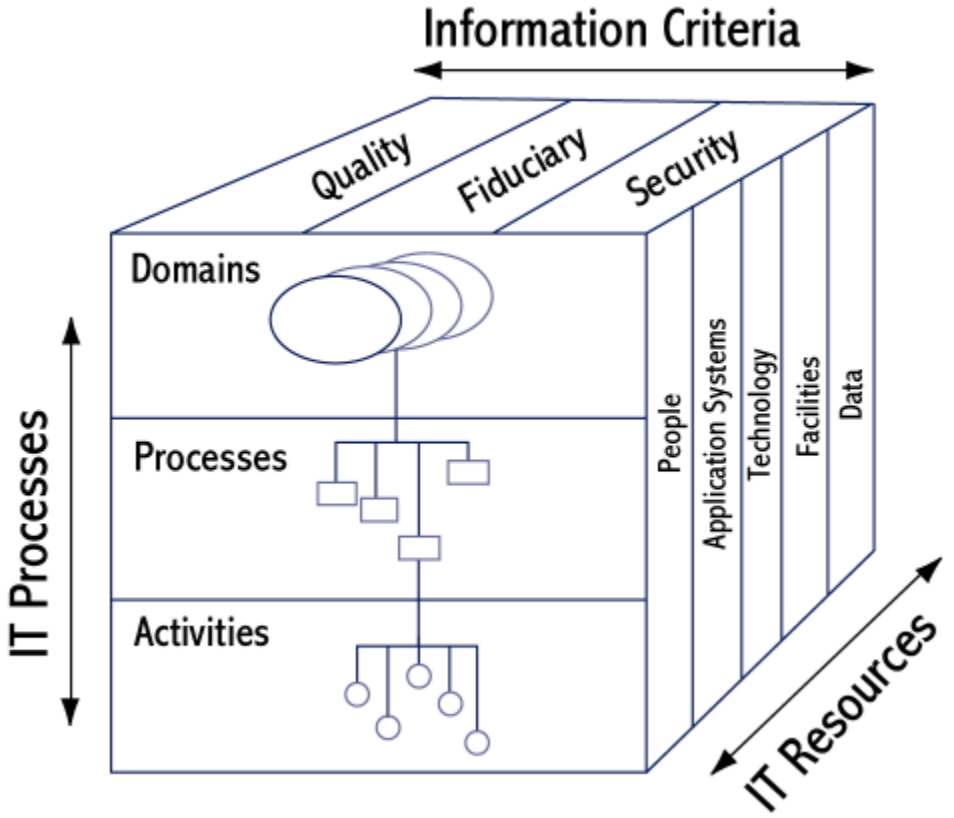
Для удовлетворения *бизнес требований к информации* адекватные *механизмы управления ИТ ресурсами* должны быть определены и внедрены. С этой целью и определяется набор *задач управления* для *ИТ процессов*.

Концептуальное ядро COBIT состоит из высокоуровневых задач управления и общей структуры, определяющей их классификацию, в которой выделяются три уровня управления ИТ ресурсами. На самом нижнем уровне находятся конкретные действия и задачи позволяющие получать измеримый результат. На более высоком уровне находятся ИТ процессы, включающие в себя набор действий и задач, нацеленных на достижение бизнес целей. На самом высоком уровне абстракции ИТ процессы естественным образом объединяются в домены, соответствующие распределению областей ответственности в организационной структуре предприятия.

Концептуальное ядро COBIT может рассматриваться с трех точек зрения:

(1) информационные критерии
(2) ИТ ресурсы
(3) ИТ процессы

Эти три элемента управления ИТ могут быть представлены в виде «Модели куба» (COBIT Cube), изображенной на рисунке.



Четыре высокоуровневых домена управления определяются следующим образом:

Планирование и организация	planning and organization	Этот домен включает стратегию и тактику, а также определение способов наиболее эффективного использования ИТ для достижения бизнес целей. Реализация стратегических замыслов должна быть спланирована и согласована. Должна быть создана соответствующая организационная и ИТ инфраструктура.
Комплектование и внедрение	acquisition and implementation	Для реализации ИТ стратегии должны быть идентифицированы, разработаны и/или приобретены соответствующие ИТ решения, которые также должны быть внедрены и интегрированы в бизнес процессы. Этот домен также включает в себя внесение изменений в ИТ системы.
Предоставление и поддержка	delivery and support	Этот домен включает предоставление требуемых информационных сервисов,

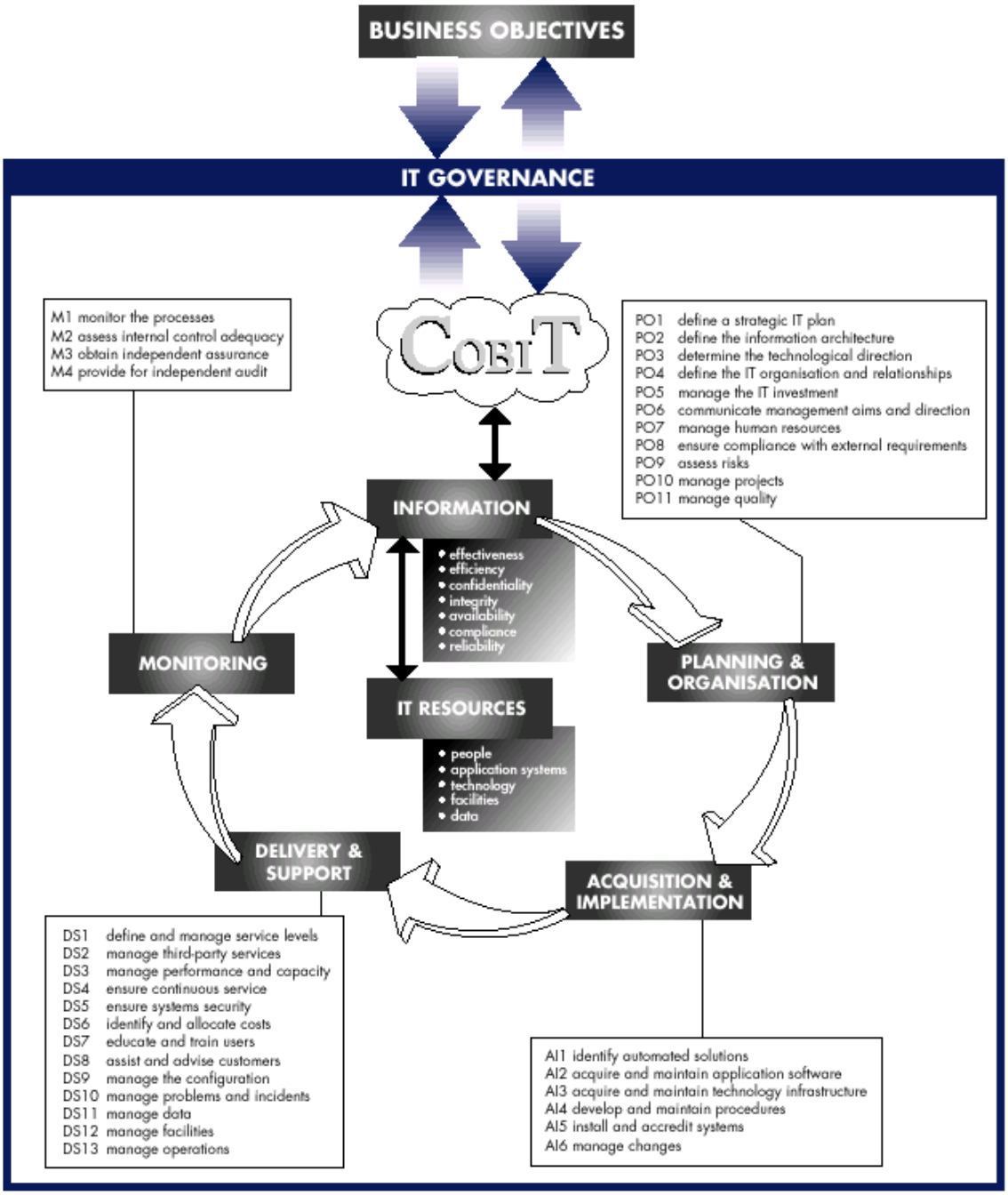
		включая обеспечение безопасности и непрерывности бизнеса, а также обучение. Для предоставления сервисов должны существовать соответствующие поддерживающие процессы. Этот домен включает в себя обработку данных прикладными системами.
Мониторинг	monitoring	Качество и соответствие ИТ процессов требованиям контроля должны оцениваться на регулярной основе. Таким образом, этот домен включает в себя надзор со стороны руководства за процессами управления в организации, а также независимый контроль со стороны внутренних и внешних аудиторов.

Механизмы управления (и соответствующие задачи управления) не обязательно способствуют реализации всех бизнес требований к информации в равной степени. С этой точки зрения, по отношению к информационным критериям, они делятся на следующие категории:

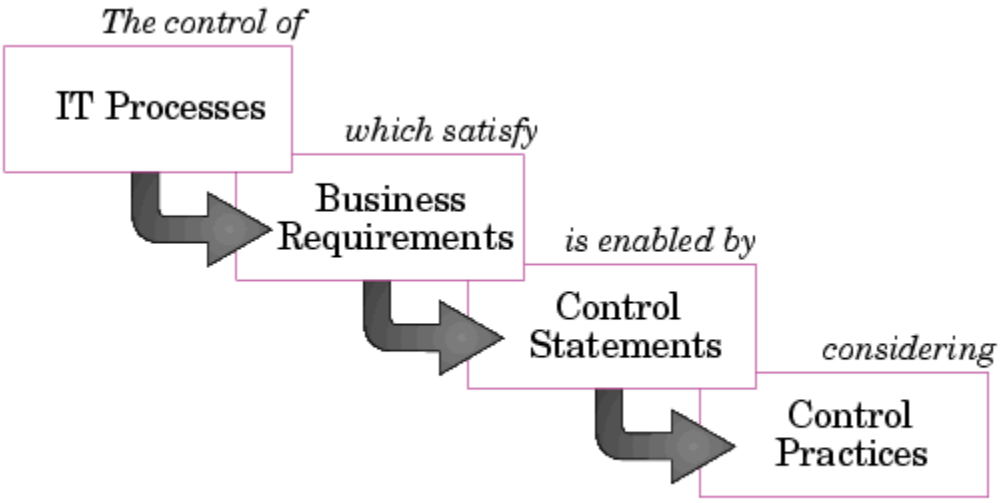
Первичные	Primary	Задача управления оказывает прямое влияние на соответствующий информационный критерий
Вторичные	Secondary	Задача управления оказывает косвенное влияние на соответствующий информационный критерий
Пустые	Blank	Задача управления хотя и может оказывать какое-то влияние на соответствующий информационный критерий, однако это влияние не является определяющим

Точно так же, механизмы управления задействуют ИТ ресурсы не в равной степени, поэтому концептуальное ядро COBIT для каждой цели контроля определяет ИТ ресурсы, управление которыми осуществляется в рамках рассматриваемого ИТ процесса.

В COBIT все 34 высокоуровневых ИТ процесса группируются по четырем доменам, как показано на рисунке.

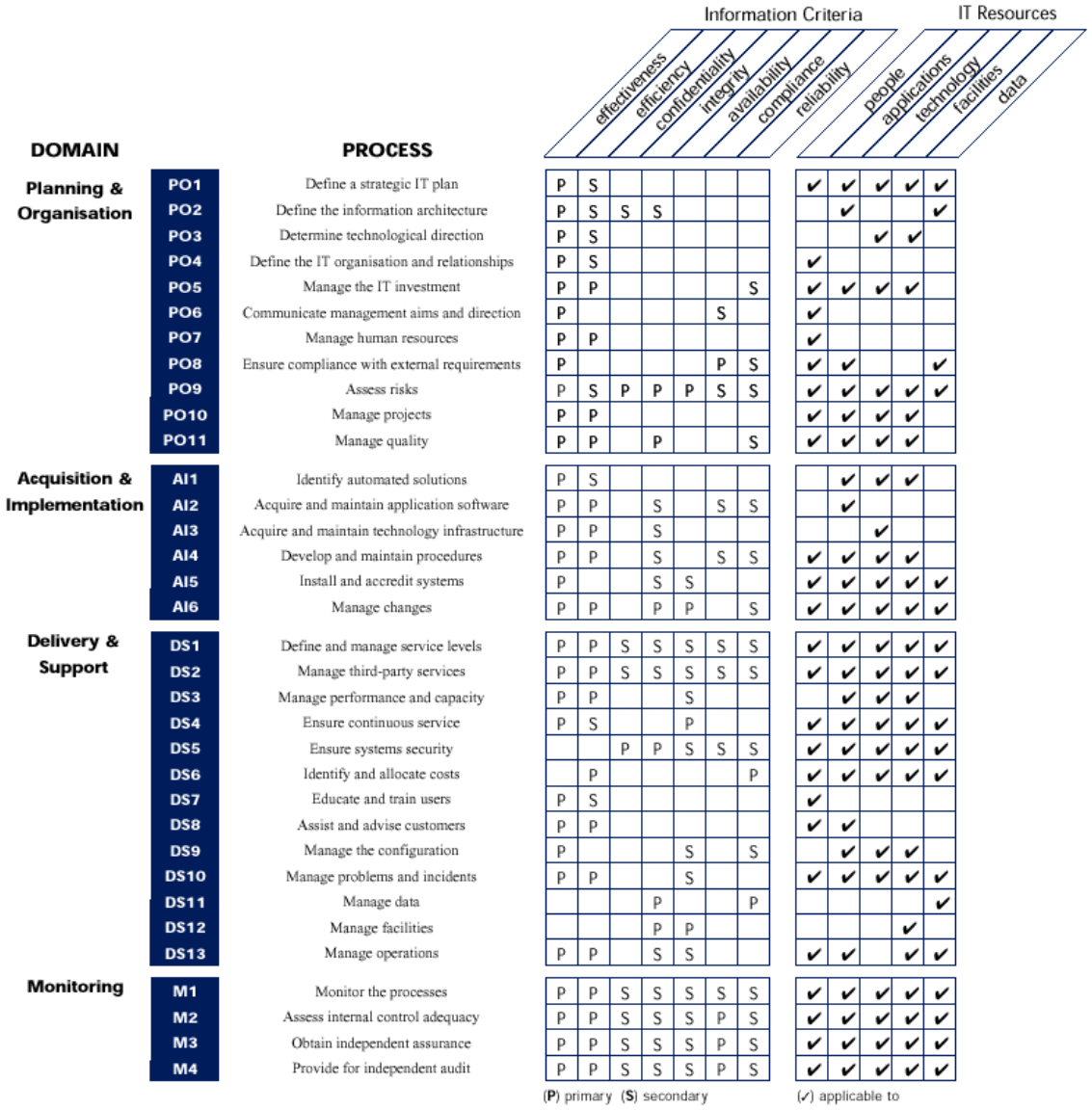


Концептуальное ядро COBIT ограничивается описанием высокоуровневых целей контроля для каждого из 34 ИТ процессов в форме, представленной на следующей схеме.



Управление *ИТ процессом*, удовлетворяющее *Бизнес требованию* (Business Requirements), обеспечивается *формулировкой задачи управления* (Control Statement), для которой должны быть рассмотрены потенциально применимые *практики управления* (Control Practices).

В следующей таблице представлены сгруппированные по доменам ИТ процессы с указанием информационных критериев, на которые оказывает влияние задача управления, и ИТ ресурсов, задействованных в ИТ процессе.



			Information Criteria							IT Resources				
DOMAIN		PROCESS	effectiveness	efficiency	confidentiality	integrity	availability	compliance	reliability	people	applications	technology	facilities	data
Planning & Organisation	PO1	Define a strategic IT plan	P	S						✔	✔	✔	✔	✔
	PO2	Define the information architecture	P	S	S	S					✔			✔
	PO3	Determine technological direction	P	S								✔	✔	
	PO4	Define the IT organisation and relationships	P	S						✔				
	PO5	Manage the IT investment	P	P					S	✔	✔	✔	✔	
	PO6	Communicate management aims and direction	P					S		✔				
	PO7	Manage human resources	P	P						✔				
	PO8	Ensure compliance with external requirements	P					P	S	✔	✔			✔
	PO9	Assess risks	P	S	P	P	P	S	S	✔	✔	✔	✔	✔
	PO10	Manage projects	P	P						✔	✔	✔	✔	
	PO11	Manage quality	P	P		P			S	✔	✔	✔	✔	
Acquisition & Implementation	AI1	Identify automated solutions	P	S							✔	✔	✔	
	AI2	Acquire and maintain application software	P	P		S		S	S		✔			
	AI3	Acquire and maintain technology infrastructure	P	P		S						✔		
	AI4	Develop and maintain procedures	P	P		S		S	S	✔	✔	✔	✔	
	AI5	Install and accredit systems	P			S	S			✔	✔	✔	✔	✔
	AI6	Manage changes	P	P		P	P		S	✔	✔	✔	✔	✔
Delivery & Support	DS1	Define and manage service levels	P	P	S	S	S	S	S	✔	✔	✔	✔	✔
	DS2	Manage third-party services	P	P	S	S	S	S	S	✔	✔	✔	✔	✔
	DS3	Manage performance and capacity	P	P			S				✔	✔	✔	
	DS4	Ensure continuous service	P	S			P			✔	✔	✔	✔	✔
	DS5	Ensure systems security			P	P	S	S	S	✔	✔	✔	✔	✔
	DS6	Identify and allocate costs		P					P	✔	✔	✔	✔	✔
	DS7	Educate and train users	P	S						✔				
	DS8	Assist and advise customers	P	P						✔	✔			
	DS9	Manage the configuration	P				S		S		✔	✔	✔	
	DS10	Manage problems and incidents	P	P			S			✔	✔	✔	✔	✔
	DS11	Manage data				P			P					✔
	DS12	Manage facilities				P	P						✔	
	DS13	Manage operations	P	P		S	S			✔	✔		✔	✔
Monitoring	M1	Monitor the processes	P	P	S	S	S	S	S	✔	✔	✔	✔	✔
	M2	Assess internal control adequacy	P	P	S	S	S	P	S	✔	✔	✔	✔	✔
	M3	Obtain independent assurance	P	P	S	S	S	P	S	✔	✔	✔	✔	✔
	M4	Provide for independent audit	P	P	S	S	S	P	S	✔	✔	✔	✔	✔

(**P**) primary (**S**) secondary (✓) applicable to

Детальные задачи управления

Для каждого из 34 ИТ процессов, описанных в Концептуальном ядре COBIT, определяется набор (от 3 до 30) **Детальных задач управления** (Detailed Control Objectives) (всего их насчитывается 318).

По утверждению разработчиков COBIT, источников для определения детальных целей контроля послужили 41 международный стандарт (де юре и де факто). Каждая задача управления содержит формулировку ожидаемых результатов или целей, которые необходимо достигнуть путем реализации конкретных процедур управления в рамках ИТ процесса.

Формулировки задач управления в COBIT носят в максимальной степени абстрактный характер, что делает их независимыми от конкретных программно-аппаратных платформ и характера деятельности организации.

Задачи управления ориентированы на руководство организации, персонал ИТ департамента, подразделения внутреннего контроля и аудита, а также, что более важно, на владельцев бизнес процессов. Они предоставляют рабочий справочник для всех субъектов управления и дают четкое определение минимального набора механизмов управления, необходимых для обеспечения эффективности, продуктивности, и экономии ресурсов.

Пример описания детальных целей контроля для ИТ процесса «Оценка рисков» представлен в Приложении 2 вместе с «Руководством по аудиту», используемым для оценки их обоснованности, приемлемости, полноты, эффективности и экономичности.

Руководство по менеджменту

Руководство по менеджменту (Management Guidelines) позволяет руководству предприятия реализовать более эффективные стратегии управления ИТ, установить контроль над использованием информационных ресурсов и соответствующими процессами, осуществлять мониторинг и давать сравнительную оценку достижения бизнес целей и оценивать производительность в рамках каждого ИТ процесса.

Определяемые в COBIT **Модели зрелости** организации (Maturity Models), позволяют руководству организации оценить текущее состояние ИТ процессов в сравнении с лучшими примерами в данной отрасли, и определить возможности для их совершенствования. **Критические Факторы Успеха** (Critical Success Factors) определяют наиболее важные ориентированные на руководство методы внедрения системы управления ИТ процессами. **Ключевые Индикаторы Целей** (Key Goal Indicators) определяют критерии для оценки достижения бизнес целей при помощи ИТ процессов. **Ключевые Индикаторы Производительности** (Key Performance Indicators) определяют критерии для оценки производительности ИТ процессов в достижении ими бизнес целей организации.

Руководство по менеджменту позволяет находить ответы на следующие вопросы: Как далеко следует заходить и компенсируются ли затраты получаемой прибылью? Что является индикатором хорошей производительности? Что является критическими факторами для достижения успеха? Каковы риски, в случае, если поставленные цели не будут достигнуты? Что делают другие?

Набор инструментов внедрения

Набор инструментов внедрения (Implementation Tool Set) дает разъяснения ключевых концепций, пошаговое описание и примеры внедрения. Он включает в себя следующие компоненты:

- Обзорная часть
- Руководство по внедрению, включая примеры меморандумов и презентаций
- Два полезных инструмента: **Диагностика осведомленности руководства** (Management Awareness Diagnostic) и **Диагностика ИТ управления** (IT Control Diagnostic), помогают анализировать структуру управления ИТ организации
- Часто задаваемые вопросы и ответы на них

Процесс внедрения COBIT в деятельность организации выглядит следующим образом:

- Определение бизнес целей при помощи Концептуального ядра COBIT,
- Выбор ИТ процессов и механизмов управления с использованием высокоуровневых и детальных задач управления,
- Согласование программы действий с бизнес планом,
- Оценка существующих процедур и результатов внедрения механизмов управления при помощи «Руководства по аудиту» и
- Оценка текущего статуса организации, идентификация критичных действий ведущих к успеху и измерение производительности в достижении целей организации при помощи «Руководства по менеджменту».

Уроки внедрения COBIT на предприятиях по всему миру указывают на необходимость вовлечения высшего руководства организации в дискуссии на эту тему уже на ранней стадии проекта внедрения. Следует быть готовым дать разъяснения основных концепций COBIT (в форме обзора и на более детальном уровне), а также привести примеры успешных внедрений в других организациях.

Руководство по аудиту

Общее описание

Руководство по аудиту (Audit Guideline) позволяет производить проверку реализации каждого из 34 высокоуровневых ИТ процессов на предмет достижения каждой из 318 детальных задач управления, что дает возможность аудитору гарантировать руководству предприятия адекватность реализованной системы управления ИТ и формировать рекомендации по ее улучшению.

«Руководство по аудиту» является дополнительным инструментом, облегчающим использование концептуального ядра и основных принципов управления COBIT при проведении ИТ аудита.

Существуют различные формы проведения ИТ аудита, включая внешний и внутренний ИТ аудит, различные виды обследований, обзоры безопасности, сертификацию продуктов ИТ и аттестацию ИС, экспертные оценки и технические экспертизы, а также различные формы контроля качества. При этом используемые методы и программы проведения аудита могут существенно различаться. «Руководство по аудиту» определяет основные принципы и общую структуру для проведения ИТ аудита, применимую к широкому классу организаций и ИТ систем.

Модели проведения аудита

Наиболее распространенной моделью оценки механизмов управления является *классическая модель аудита*, на которой и построена содержащееся в COBIT «Руководство по аудиту». Другим общепризнанным подходом является *модель анализа рисков*. Любая из этих моделей может с успехом применяться на практике при проведении аудита ИТ в организациях на базе COBIT.

Более подробно об этом можно прочитать в публикации автора, посвященной аудиту безопасности информационных систем (2).

Основные задачи аудита

Основными задачами ИТ аудита являются:

- Предоставление руководству организации обоснованных гарантий достижения целей контроля,
- При наличии существенных уязвимостей механизмов управления ИТ, оценка и обоснование результирующих рисков и
- Выдача рекомендаций руководству по поводу корректирующих действий.

Уровни описания процедуры аудита по COBIT

На верхнем уровне абстракции общий подход к аудиту опирается на следующие основные элементы:

- Концептуальное ядро COBIT, включая классификацию ИТ процессов, информационные критерии и ИТ ресурсы (см. Выше Суммарную таблицу целей контроля)
- Общие требования к процедуре аудита (см. ниже Раздел «Планирование и выработка стратегии аудита»)
- Общие требования к аудиту ИТ процесса (см. Раздел «Обобщенная схема руководства по аудиту»)

- Общие принципы управления (см. ниже Раздел «Общие замечания относительно оценки процессов управления»)

На втором уровне абстракции используются детальные инструкции по аудиту ИТ процессов, описанные в «Руководстве по аудиту».

Эти инструкции представлены в стандартизованном виде, предусматривающем описание четырех стадий процедуры аудита: **Сбор информации**, **Оценка механизмов управления**, **Тест соответствия**, **Детальный тест**. Этот шаблон используется как при описании общей процедуры ИТ аудита, так и при описании детальных инструкций по проведению аудита. Описание процедуры аудита конкретной задачи управления «Оценка рисков» приведено в Приложении 1.

На третьем, самым нижнем уровне абстракции, аудитор дополняет и конкретизирует «Детальные инструкции по аудиту» с целью приведения их в соответствие с конкретными условиями. При этом в ходе планирования процедуры аудита, учитываются следующие факторы:

- Критерии и требования, специфичные для данной отрасли
- Отраслевые и промышленные стандарты
- Особенности программно-аппаратных платформ
- Конкретные методы управления, используемые в организации

Важно принимать во внимание то обстоятельство, что не все задачи управления, являются применимыми в конкретной ситуации. Для определения актуальных задач управления должна производиться оценка рисков.

Все элементы, содержащиеся в «Руководстве по аудиту» предназначены для использования лишь в качестве вспомогательных средств и методологической основы при разработке конкретных программ проведения ИТ аудита.

Общее руководство по проведению аудита

В настоящем разделе рассказывается о том, как следует проводить аудит Системы управления ИТ в соответствии с принципами COBIT.

Общие замечания относительно оценки процессов управления

Общие принципы управления сосредоточены главным образом на распределении ответственности, стандартах управления и управлении информационными потоками.

С точки зрения руководителя механизм управления определяется как контроль выполнения поставленных задач, оценка производительности и, в случае необходимости, корректировка действий персонала.

Процесс управления состоит из четырех этапов. Сначала определяется стандарт производительности. Затем определяется состояние ИТ процесса, путем получения субъектом управления информации от объекта управления (ИТ процесса). После этого, информация о состоянии ИТ процесса сравнивается с требованиями стандарта. В случае выявления несоответствия требованиям стандарта субъект управления предпринимает корректирующие действия, путем передачи соответствующей управляющей информации ИТ процессу.

Исходя из этой модели, можно сделать следующие замечания, которые следует принимать во внимание при оценке механизмов управления:

1. Для того чтобы модель управления работала, ответственность за бизнес процессы должна быть четко распределена, также должна быть установлена строгая подотчетность каждого должностного лица. В противном случае, не будет происходить обмен управляющей информацией, и корректирующие действия не будут предприниматься.
2. Стандарты управления могут быть самыми разными, начиная с высокоуровневых планов и стратегий и заканчивая *ключевыми индикаторами производительности и критичными факторами успеха*. Четко документированные, сопровождаемые и доступные для всех сотрудников организации стандарты являются необходимым условием для реализации хорошего процесса управления.
3. Такие же требования предъявляются и к ИТ процессу: хорошая документированность и четкое распределение ответственности. Важным аспектом является четкое определение допустимых отклонений от требований стандарта.
4. Своевременность, целостность и пригодность информации контроля служит основой хорошего функционирования системы управления. Аудитор должен уделять этому внимание.

Планирование и выработка стратегии аудита

Прежде всего, необходимо правильно определить границы проведения аудита. Для этого следует исследовать, проанализировать и определить следующее:

- Структуру бизнес процессов
- Платформы и информационные системы, поддерживающие бизнес процессы и их взаимодействие с другими платформами и системами
- ИТ роли и распределение ответственности, включая аутсорсинговые функции
- Бизнес риски и стратегические направления

На следующем шаге определяются информационные критерии, имеющие особенную важность для бизнес процессов. Затем определяются ИТ риски и общий уровень контроля, связанный с рассматриваемыми бизнес процессами. Для этого необходимо определить:

- Последние изменения в бизнес окружении, повлиявшие на ИТ
- Последние изменения в ИТ окружении, новые разработки и т.п.
- Последние инциденты, связанные с механизмами управления или бизнес окружением
- Механизмы мониторинга ИТ инфраструктуры, используемые руководством
- Последние аудиторские отчеты
- Последние результаты самооценок

На основе полученной информации осуществляется выбор соответствующих ИТ процессов и связанных с ними ИТ ресурсов.

Далее определяется стратегия проведения аудита и на ее основе разрабатывается детальный план аудита, включающий этапы, задачи и вопросы, требующие принятия решений. Пример общей процедуры аудита приведен ниже.

Схема проведения аудита

В COBIT используется следующая схема проведения аудита:

- Идентификация и документирование (включает в себя сбор и превичный анализ информации)
- Оценка механизмов управления
- Тест соответствия
- Детальное тестирование

*На самом деле, приведенная схема отличается от общепринятой, в частности в ней отсутствуют этапы **Инициирования и планирования, Выработки рекомендаций и Подготовки отчетных документов**. Видимо эти задачи в COBIT включаются в приведенную схему неявным образом. Более четкая схема проведения аудита приведена в публикации (2).*

Сбор и первичный анализ информации аудита

На данном этапе осуществляется документирование процедур достижения задач управления и идентификация существующих механизмов управления. С этой целью производится интервьюирование руководства и сотрудников организации для уяснения следующих вопросов:

- Требования бизнеса и ассоциированные с ними риски
- Организационная структура
- Распределение ролей и ответственности
- Политики и процедуры
- Законы и другие нормативные акты
- Существующие механизмы управления
- Существующая отчетность

Оценка механизмов управления

На данном этапе производится оценка эффективности существующих механизмов управления или степени выполнения задач управления. Определение того Что, Зачем и Как должно быть протестировано. Также оценивается целесообразность и пригодность механизмов управления, используемых в исследуемом ИТ процессе, путем сравнения с установленными критериями и промышленными стандартами, критическими факторами успеха, а также применения аудиторской экспертной оценки.

Аудитору необходимо убедиться в том, что:

- Существующие ИТ процессы документированы
- Ответственность и подотчетность четко определены
- Там, где необходимо, существуют компенсирующие механизмы управления

Тест соответствия

Тестом соответствия называется этап аудита, задачей которого является получение гарантий пригодности существующих механизмов управления для решения задач управления. Проверка осуществляется путем получение прямых и косвенных свидетельств надлежащего выполнения установленных процедур управления за оцениваемый период.

На этом этапе выполняется также ограниченное исследование адекватности результатов процесса управления, определяется уровень детального тестирования и объем дополнительной работы, необходимой для получения гарантий адекватности ИТ процесса.

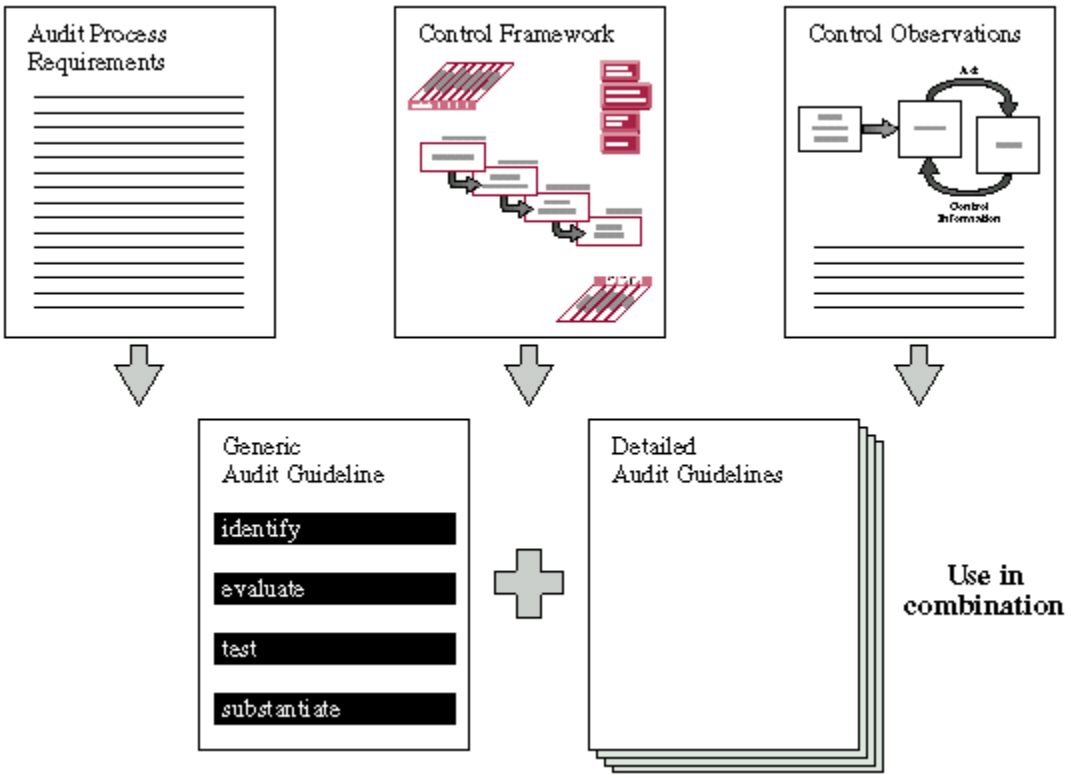
Детальное тестирование

Детальным тестом называется заключительный этап аудита, целью которого является оценка и обоснование рисков недостижения задач управления путем использования аналитических методов и экспертных оценок. Целью является побуждение руководства к действию. Аудиторы должны творчески подходить к поиску и представлению этой зачастую конфиденциальной информации.

На данном этапе аудитор производит документирование недостатков механизмов управления, а также угроз и уязвимостей, являющихся следствием этих недостатков. Также осуществляется идентификация и документирование реальных и потенциальных последствий реализации угроз путем причинно-следственного анализа, и проводится сравнительное тестирование.

Обобщенная схема руководства по аудиту

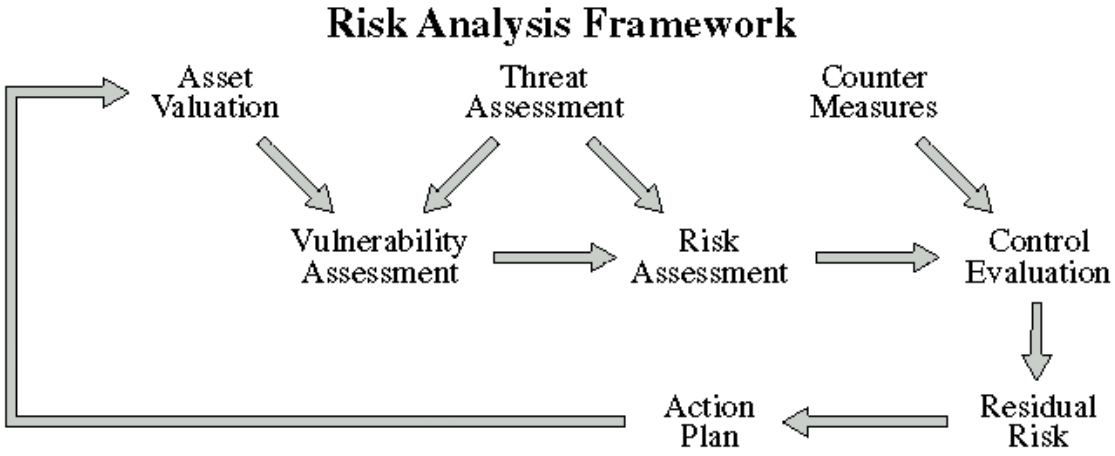
Представленная на рисунке схема иллюстрирует общий подход к проведению ИТ аудита в соответствии с COBIT. Согласно этому подходу, процедура аудита строится в соответствии с описанием, приведенным в разделе «Структура проведения аудита» (на рисунке – «General Audit Guideline») и включает в себя четыре этапа. Схема каждого из этих этапов, применительно к аудиту конкретной задачи управления изложена в Приложении 1 («Audit Process» по COBIT). В рамках этой схемы, для оценки достижения каждой из 34 задач управления используется «Детальное руководство по аудиту» (на рисунке – «Detailed Audit Guideline»), пример которого для задачи управления «Оценка рисков» приведен в Приложении 2. Выработка стратегии и планирование процедуры аудита осуществляется в соответствии с общими требованиями (на рисунке – «Audit Process Requirements»). При проведении аудита также должны учитываться «Общие замечания относительно оценки процессов управления» (на рисунке – «Control Observations»). Кроме того, во всех вышеперечисленных документах используется понятийный аппарат и модель взаимосвязей между бизнес целями, ИТ процессами, ИТ ресурсами, информационными критериями и целями контроля, определенные в Концептуальном ядре COBIT (на рисунке – «Control Framework»).



Анализ рисков как альтернативный подход к оценке ИС

При принятии решения по поводу внедрения тех или иных механизмов управления ключевым является вопрос о соотношении стоимости этих механизмов и величины рисков, на уменьшение которых они направлены.

Методы и походы к анализу и управлению рисками остаются за рамками COBIT, который ограничивается лишь определением общего понятия и указанием на важность использования анализа рисков при проведении ИТ аудита. Пожалуй, вся содержательная часть соответствующего параграфа COBIT, посвященного этой теме, заключается в приведенной ниже диаграмме и кратком пояснении к ней.



Анализ рисков (Risk Assessment) начинается с оценки *ИТ ресурсов* (Asset Valuation), необходимых для достижения бизнес целей. ИТ ресурсы включают в себя информацию, технические, программные и прочие средства, необходимые для ее получения, обработки, хранения и т.п. На следующем шаге осуществляется *анализ уязвимостей* (Vulnerability Assessment) и *угроз* (Threat Assessment), использующих эти уязвимости и препятствующих достижению бизнес целей. Вероятность угрозы, величина уязвимости и размер возможного ущерба определяют степень риска, ассоциированного с возможностью осуществления данной угрозы. Далее осуществляется *выбор контрмер* (Counter Measures) и *оценка их эффективности* (Control Evaluation), а также определяется *величина остаточных рисков* (Residual Risk). Результатом анализа рисков является *план действий по внедрению механизмов управления* (Action Plan), после чего весь цикл повторяется заново.

Более полное изложение современных методов анализа и управления рисками приводится в публикации (2).

Выводы

COBIT является международным стандартом, определяющим набор универсальных задач управления ИТ, ориентированных, прежде всего, на руководство организации и на ИТ аудиторов. Уникальность и основная ценность COBIT заключается в том, что он предлагает модель, обеспечивающую взаимосвязь между бизнес целями и ИТ процессами.

В состав третьей редакции COBIT входит несколько книг, включая Резюме для руководства, Концептуальное ядро, Руководство по менеджменту, Руководство по аудиту, Детальные задачи управления и Набор инструментов внедрения.

«Резюме для руководства» служит введением в остальные разделы стандарта. Оно содержит общие сведения о стандарте, определяет Миссию COBIT и понятие Системы управления ИТ. «Концептуальное ядро COBIT» представляет собой *набор основополагающих принципов и понятий, а также модель управления ИТ, на базе которых строятся все положения COBIT.* «Руководство по менеджменту» позволяет руководству предприятия реализовать более эффективные стратегии управления ИТ, установить контроль над использованием информационных ресурсов и соответствующими процессами, осуществлять мониторинг, давать сравнительную оценку достижения бизнес целей и оценивать производительность в рамках каждого ИТ процесса. «Набор инструментов внедрения» дает разъяснения ключевых концепций, пошаговое описание и примеры успешного внедрения COBIT в организациях по всему миру. «Руководство по аудиту» позволяет производить проверку реализации каждого из 34 высокоуровневых ИТ процессов на предмет достижения каждой из 318 детальных задач управления, что дает возможность аудитору гарантировать руководству предприятия адекватность реализованной системы управления ИТ и формировать рекомендации по ее улучшению.

COBIT определяет общих подход, общую схему и детальные инструкции по проведению аудита системы управления ИТ на базе описанных в нем задач управления, которые могут быть спользованы при разработке детальных планов и программ аудита.

Процедура аудита по COBIT разбивается на четыре этапа: **Сбор информации**, **Оценка механизмов управления**, **Тест соответствия**, **Детальный тест**. Эта схема используется как при описании общей процедуры, так и при описании детальных инструкций по проведению аудита.

Несмотря на все присущие COBIT недостатки, которые не позволяют считать этот документ эталоном выражения передового опыта в области управления и аудита ИТ, он остается достаточно важным и полезным для практики стандартом, знакомство с которым будет весьма полезным для ИТ аудиторов, ИТ менеджеров и руководителей организаций.

Ссылки

1) COBIT 3rd Edition, Released by the COBIT Steering Committee and the IT Governance Institute, July 2000
2) Астахов А.М., Аудит безопасности информационных систем, ISACA.RU, 2002

Приложение 1. Процедура аудита конкретной задачи управления

Последовательность шагов по проведению ИТ аудита проиллюстрирована на диаграммах, приведенных ниже. На диаграммах показаны цели каждого этапа, что аудитор должен получить для перехода к следующему этапу, а также процесс сбора информации и процесс принятия решений для каждого этапа.

Идентификация и документирование

Цель этапа – познакомиться с существующими в организации задачами управления, и почему руководство организации считает, что оно контролирует эти задачи. Производится идентификация ответственных лиц, ИТ процессов и процедур.

Ожидаемые результаты – аудитор должен идентифицировать, задокументировать и проверить следующее:

- Кто выполняет задачи для реализации цели контроля,
- Где выполняется задача,
- Когда выполняется задача,
- На каких входных данных выполняется задача,
- Каковы ожидаемые выходные данные и
- Каковы установленные процедуры для выполнения задачи.

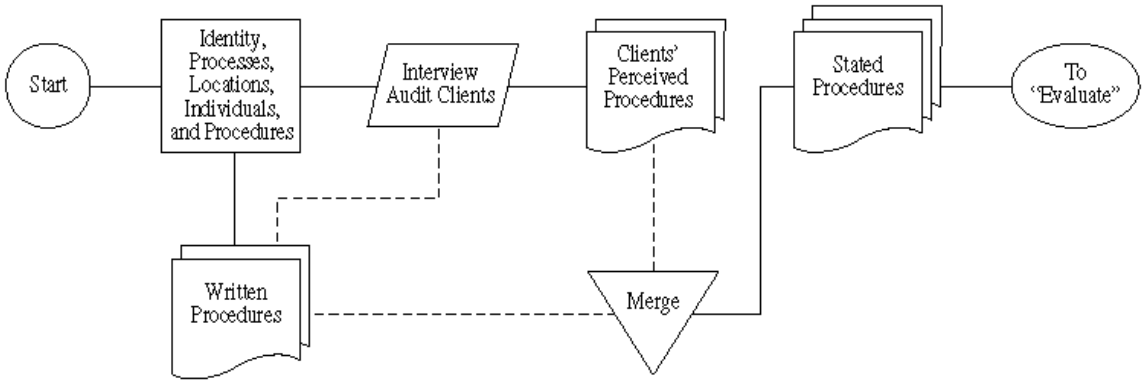


Рисунок 1. Диаграмма этапа идентификации и документирования

Оценка

Цель этапа – оценка установленных процедур и определение того, предоставляют ли данные процедуры эффективную структуру управления. Процедуры должны быть оценены на соответствие установленным критериям, промышленным стандартам и взглядам аудитора. Эффективная структура управления должна быть экономически оправдана и предоставлять обоснованные гарантии выполнения задач управления.

Ожидаемые результаты – По окончанию этого этапа аудитор должен иметь:

- Оцененные на применимость к процедурам законы, распоряжения и организационные критерии
- Оценка существующих процедур с точки зрения их экономической оправданности и предоставления обоснованных гарантий выполнения задач управления
- Оценка любых компенсирующих механизмов управления, используемых для укрепления слабых процедур
- Выводы относительно обеспечения эффективной структуры управления установленными процедурами и компенсирующими механизмами
- Выводы относительно уместности проведения тестов соответствия

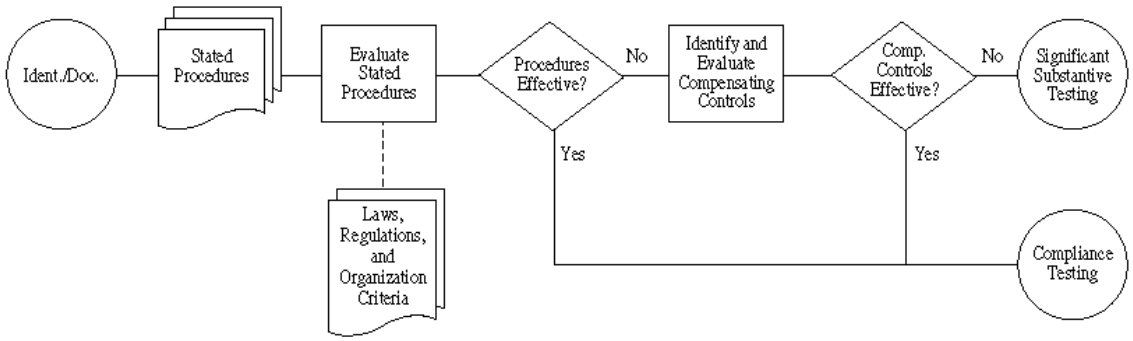


Рисунок 2. Диаграмма этапа оценки

Тест соответствия

Цель этапа – Анализ соблюдения сотрудниками организации предписанных механизмов управления. Существующие процедуры и компенсирующие механизмы управления сравниваются с установленными. С этой целью проводятся интервью и анализ документации, позволяющие установить правильность и последовательность применения механизмов управления. Тест соответствия применяется только к процедурам, которые были оценены как эффективные на предыдущем этапе.

Ожидаемые результаты – По завершению тестов соответствия аудитор должен получить документальные данные относительно соблюдения установленных процедур сотрудниками организации, а также выводы относительно правильности и последовательности применения этих процедур и компенсирующих механизмов управления. На базе оценки уровня соответствия аудитор определяет уровень детального тестирования, необходимого для получения гарантий адекватности процесса управления.

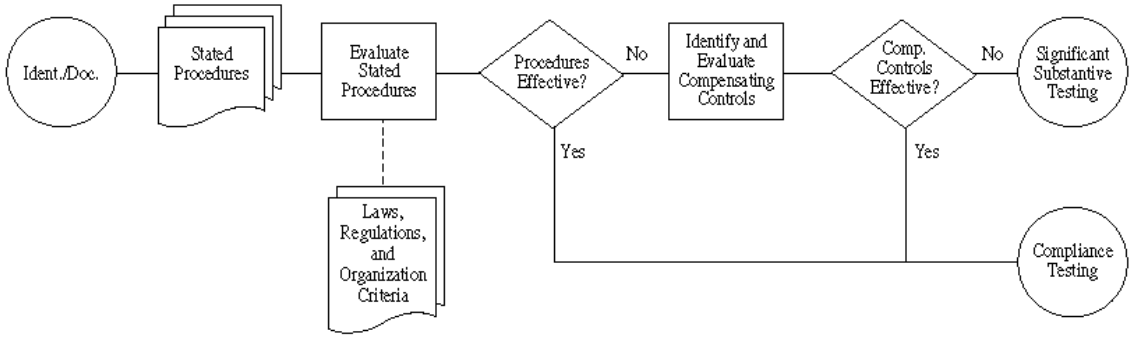


Рисунок 3. Диаграмма этапа теста соответствия

Детальное тестирование

Цель этапа – Проведение необходимых тестов данных для предоставления руководству организации окончательных гарантий достижения бизнес целей.

Ожидаемые результаты – Аудитор должен в достаточном объеме протестировать результаты ИТ процессов, для того чтобы сделать выводы относительно выполнения задачи управления. Детальное тестирование проводится в значительном объеме в следующих случаях:

- Отсутствуют механизмы управления
- Оценка механизмов управления указывает на их несостоятельность или

- Тест соответствия показывает, что механизмы управления не были правильно и последовательно применены.

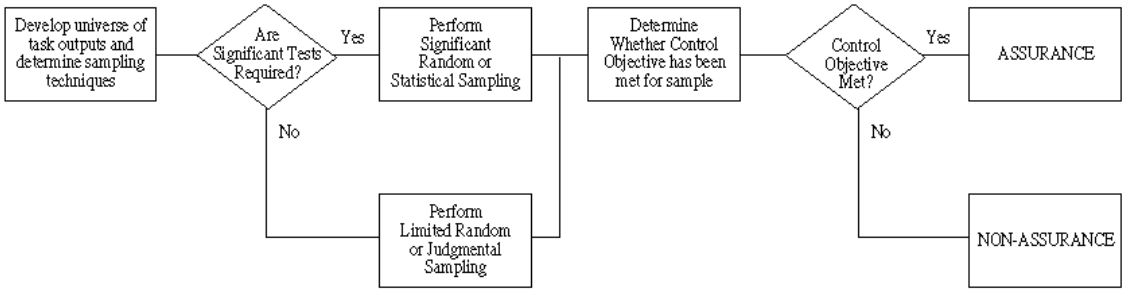


Рисунок 4. Диаграмма этапа детального тестирования

Приложение 2. Пример руководства по аудиту задачи управления – «Оценка рисков»

PO9 Оценка рисков

Высокоуровневая задача управления

P	Эффективность
S	Продуктивность
P	конфиденциальность
P	Целостность
P	Доступность
S	Соответствие
S	Надежность

Контроля над ИТ процессом

Оценка рисков

Который удовлетворяет бизнес требованию

Поддержки решений руководства путем выполнения ИТ задач управления и реагирования на угрозы путем уменьшения сложности, увеличения объективности и идентификации важных факторов, влияющих на принятие решений

Достигается путем

Идентификации ИТ рисков и анализа возможных последствий осуществления угроз с привлечением экспертов из разных функциональных подразделений, а также путем принятия экономически оправданных мер по уменьшению рисков

И принимается во внимание

- ответственность за управление рисками
- различные виды ИТ рисков (технологические, безопасности, непрерывности функционирования, несоответствия нормативным требованиям и т.п.)
- определение и обсуждение допустимых остаточных рисков (risk tolerance profile)
- анализ причин и использование методов мозгового штурма при анализе рисков
- количественная и/или качественная оценка рисков
- методика оценки рисков
- план уменьшения рисков
- своевременная переоценка

X	Люди
X	приложения
X	Технологии
X	оборудование
X	Данные

Детальные задачи управления

9.1 Оценка бизнес рисков

Руководство должно создать структуру для проведения систематической оценки рисков. Эта структура должна предусматривать регулярную оценку информационных рисков, препятствующих достижению бизнес целей, и определение методов управления рисками, позволяющих снизить их до приемлемой величины. Оценка рисков должна производиться на глобальном уровне и на системном уровне, для новых и существующих проектов, с участием представителей разных функциональных подразделений. Руководство должно обеспечить регулярную переоценку рисков и обновление исходных данных по результатам проведения аудита, проверок и идентифицированных инцидентов.

9.2 Подход к оценке рисков

Руководство должно установить общий подход к оценке рисков, который определяет масштаб и границы, методику оценки рисков, ответственность и требуемые навыки. Руководство должно возглавлять идентификацию решений по уменьшению рисков и быть вовлечено в идентификацию уязвимостей. Специалисты по безопасности должны возглавлять идентификацию угроз и ИТ специалисты должны выбрать механизмы управления. Качество оценки рисков должно гарантироваться хорошо структурированной методикой и высокой квалификацией специалистов.

9.3 Идентификация рисков

Подход к анализу рисков должен фокусироваться на обследовании существенных элементов риска и причинно-следственных взаимосвязях между ними. Существенные элементы риска включают в себя материальные и нематериальные ресурсы, ценность ресурсов, угрозы, уязвимости, контрмеры, последствия и вероятности угроз. Процесс идентификации рисков должен включать качественное и, где это уместно, количественное ранжирование рисков. Исходные данные должны предоставляться руководством. Также должны использоваться результаты стратегического планирования, предыдущих аудитов и другие источники. Оценка рисков должна охватывать бизнес риски, риски, связанные с законодательством, технологиями, торговыми партнерами и людскими ресурсами.

9.4 Измерение величины риска

Подход к оценке рисков должен обеспечивать анализ результатов идентификации рисков путем качественных оценок и/или количественных измерений. Также должна быть оценена способность организации к принятию остаточных рисков.

9.5 План уменьшения рисков

Подход к анализу рисков должен предусматривать наличие плана управления рисками, гарантирующего использование экономически оправданных механизмов управления и мер безопасности для уменьшение величины рисков на постоянной основе. План управления рисками должен определять стратегию управления в терминах предотвращения, уменьшения и принятия рисков.

9.6 Принятие остаточных рисков

Подход к анализу рисков должен обеспечивать формализацию принятия остаточных рисков, в зависимости от идентификации и измерения рисков, политики организации, неопределенности, присущей используемому подходу к оценке рисков, и экономической эффективности реализации контрмер и механизмов управления. Остаточные риски должны компенсироваться адекватным страховым покрытием, контрактными обязательствами и самострахованием.

9.7 Выбор контрмер

При нацеленности на обоснованную, пригодную и пропорциональную систему контрмер и механизмов управления, более высокий приоритет должен присваиваться механизмам управления с наивысшим возвратом инвестиций, а также тем, которые позволяют получить быстрые результаты. Система управления должна обеспечить баланс мер превентивного, детектирующего, корректирующего и восстанавливающего характера. Более того, руководство должно довести до сведения всех ответственных лиц цели мер контроля, согласовать взаимно конфликтующие меры и осуществлять непрерывный мониторинг эффективности всех мер контроля.

9.8 Обязательство по оценке рисков

Руководству следует поощрять использование анализа рисков в качестве важного инструмента предоставления информации для проектирования и внедрения внутренних механизмов управления, определения стратегического плана развития ИТ, а также для реализации механизмов мониторинга и оценки.

Руководство по аудиту

Высокоуровневые и детальные задачи управления проверяются путем:

Достижением понимания путем:

Интервьюирования:

1. Высшее руководство ИТ
2. Отдельных ИТ специалистов
3. Отдельных специалистов по управлению рисками
4. Ключевых пользователей ИТ сервисов

Получения:

1. Политики и процедуры, имеющие отношение к оценке рисков
2. Документы с оценкой бизнес рисков
3. Документы с оценкой операционных рисков
4. Документы с оценкой ИТ рисков
5. Детали базиса, по которому измеряется величина риска и потери
6. Файлы персонала, для которого производится оценка рисков
7. Политики страхования остаточных рисков
8. Мнения экспертов
9. Результаты обследований
10. База данных управления рисками

Оценка механизмов управления путем:

Проверки того, что:

1. Существует структура для систематической оценки рисков, включая риски недостижения целей организации, а также существует система управления рисками
2. Подход к анализу рисков предусматривает регулярное обновление оценок на глобальном и системном уровне
3. Процедура оценки рисков позволяет учитывать как внешние, так и внутренние факторы и принимает во внимание результаты аудитов, ожидания и идентифицированные инциденты
4. Цели всей организации включены в процесс идентификации рисков
5. Процедуры мониторинга изменений в работе систем предусматривают своевременное уточнение данных о системных рисках и уязвимостях
6. Существуют процедуры непрерывного мониторинга и улучшения оценки рисков, облегчающие процессы создания механизмов управления
7. Документация по оценки рисков включает в себя следующее:

    - Описание методологии оценки рисков
    - Идентификацию существенных уязвимостей и соответствующих рисков
    - Риски и соответствующие уязвимости, для противодействия которым существуют механизмы управления

8. Вероятность, частота и методы анализа рисков включены в процедуру идентификации рисков
9. Квалификация персонала, выполняющего оценку рисков, является адекватной
10. Существует формальный количественный и/или качественный (или комбинированный) подход к идентификации и измерению величины рисков, угроз и уязвимостей
11. Вычислительные и другие методы используются для измерения рисков, угроз и уязвимостей
12. Для реализации необходимых контрмер, направленных против рисков, угроз и уязвимостей, используется план управления рисками
13. Решение о допустимости тех или иных остаточных рисков, принимает во внимание:

    - Политику организации
    - Идентификацию и измерение рисков
    - Неопределенность, присущую самому подходу к оценке рисков
    - Стоимость и эффективность реализации контрмер и механизмов управления

14. Страховка покрывает остаточные риски
15. Существуют формальные количественные и/или качественные подходы к выбору механизмов управления и максимизации возврата
16. Имеется баланс между используемыми детектирующими, превентивными, корректирующими и восстанавливающими контрмерами
17. Существуют формальные процедуры для обнародования целей механизмов управления

Оценка соответствия путем:

Тестирования:

1. Структура оценки рисков предусматривает регулярное обновление оценки рисков с целью уменьшения рисков до приемлемой величины
2. Документация по оценке рисков согласована со структурой оценки рисков, должным образом подготовлена и сопровождается
3. ИТ менеджеры и ИТ персонал вовлечены в процесс оценки рисков
4. Руководство организации осведомлено о факторах, обуславливающих риски, и вероятности угроз
5. Соответствующий персонал понимает и формально принимает остаточные риски
6. Отчеты по оценке рисков предоставляются высшему руководству на согласование своевременно
7. Подход, используемый для анализа рисков, имеет результатом количественное и/или качественное измерение величины уязвимости к риску
8. Риски, угрозы и уязвимости, идентифицированные руководством, и их атрибуты используются для выявления каждой разновидности угрозы
9. План управления рисками является актуальным и включает в себя экономически оправданные механизмы управления и контрмеры, направленные на уменьшение рисков
10. Существует система приоритетов и для каждого риска существует соответствующая контрмера:

    - Спланированная превентивная мера
    - Вторичный детектирующий механизм управления
    - Третичный корректирующий механизм управления

11. Сценарии осуществления угроз документированы, актуальны и доведены до сведения ответственных лиц
12. Для остаточных рисков существует достаточное страховое обеспечение, учитывающее различные сценарии угроз, включая:

    - Пожар, затопление, землетрясение, ураганы, терроризм, непредвиденные природные бедствия
    - Недостаточная ответственность сотрудников организации
    - Потеря прибылей и клиентов в результате прерывания бизнес процессов
    - Другие риски, которые обычно не охватываются рассмотренными выше ИТ и бизнес планами обеспечения непрерывности бизнеса

Обоснование риска невыполнения задач управления путем:

Выполнения:

1. Сравнение структуры оценки рисков с другими организациями той же отрасли или с соответствующими международными стандартами, либо общепризнанными «лучшими практиками»
2. Детальное исследование подхода к оценке рисков, используемого для идентификации, измерения и уменьшения величины рисков до приемлемого уровня

Идентификации:

1. Не идентифицированные риски
2. Не измеренные риски
3. Риски, которые не были уменьшены до приемлемого уровня
4. Устаревшие оценки рисков
5. Ошибочные количественные либо качественные оценки рисков, угроз и уязвимостей
6. Планы управления рисками, не предусматривающие экономически оправданных механизмов управления и мер безопасности
7. Отсутствие формального признания остаточных рисков
8. Неадекватное страховое обеспечение