Комплаенс-контроль

Как выстроить процесс, обеспечивающий соответствие требованиям законодательства и различным нормативным актам, а также контроль за выполнением внутренних процедур? В чем преимущества сервисного подхода, направленного на снижение профильных рисков? Как в этом процессе обеспечить прозрачное взаимодействие между службой внутреннего контроля, IT-подразделением, подразделениями безопасности, бизнеса и менеджментом?

Управление соответствием: комплаенс как сервис с автоматической пролонгацией статуса

Как показывает консалтинговая практика, организации испытывают сложности при построении процесса, обеспечивающего соответствие требованиям законодательства и нормативным актам, а также контроль за выполнением внутренних процедур. Это особенно актуально для менеджмента крупных компаний с обширной филиальной сетью. Рассмотрим аспекты поддержания соответствия в организации на примере обеспечения информационной безопасности в банке.

Л.В. ПЛЕТНЕВ,
ЗАО НИП «Информзащита», отдел безопасности банковских систем, руководитель направления

Проблемы при осуществлении контроля соответствия (Compliance Control)

1. Зачастую бывает сложно управлять большим количеством требований, регулирующих деятельность организации. В частности, в области защиты информации на банки распространяется более 1000 требований федеральных законов о лицензировании видов деятельности, национальной платежной системе, персональных данных, коммерческой тайне, электронной подписи, а также требований нормативных документов Банка России и международных платежных систем.

Организации сталкиваются с рядом сложностей при анализе применимых к ним требований, в частности, когда:

Комплаенс-контроль

— требование одного стандарта усложняет требование другого или требования часто меняются регулятором. В этом случае банк вынужден перестраивать процессы и осуществлять дополнительную настройку своих систем. Например, в Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее — Закон № 152-ФЗ) со времени его принятия четырнадцать раз вносились изменения, которые в свою очередь влекли изменения подзаконных нормативных документов;

— требования имеют формулировки, сложные для восприятия, или формулировки с неоднозначной трактовкой. Например, формулировки некоторых требований Положения Банка России от 09.06.2012 № 382-П[1] (далее — Положение № 382-П) не соответствуют описанному методу проверки, а некоторые пункты комплекса стандартов СТО БР ИББС могут вызывать вопросы о способах их выполнения;

На банки распространяется более 1000 требований федеральных законов о лицензировании видов деятельности, национальной платежной системе, персональных данных, коммерческой тайне, электронной подписи, а также требований нормативных документов Банка России и международных платежных систем.

— требования негативно влияют на непрерывность бизнес-процессов. Например, шифрование промышленных баз данных может напрямую влиять на их производительность. А что важнее — обеспечить соответствие или гарантировать своевременное выполнение бизнес-процесса?

2. Другая проблема управления соответствием — непонимание целей нормативно-правовых актов проверяемыми подразделениями. Внутренние проверки и внешние аудиты их сотрудники часто считают неэффективными, отвлекающими от основной деятельности и могут даже саботировать контрольные процедуры. Причина такой ситуации заключается в том, что влияние связанных мер на риски организации не оценивается, а участники контрольного процесса недостаточно информированы.

3. Не налажено взаимодействие подразделений, выполняющих надзорные функции, с сервисными подразделениями и бизнесом. Это также приводит к снижению уровня соответствия, несвоевременному получению информации о нарушениях в процессах компании. Проведение аудита в соответствии с планом проверок один раз в год или реже не обеспечивает уверенность в необходимом уровне соответствия, «слабое звено» может не проверяться в течение длительного времени. Например, может не проверяться периферийная инфраструктура значимых для бизнеса автоматизированных банковских систем, притом что именно в таких системах могут быть

[1] Положение Банка России от 09.06.2012 № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств».

уязвимости, представляющие опасность компрометации основных систем.

4. Требует внимания и вопрос неравномерности проведения контрольных мероприятий. В проверяемых подразделениях может случиться аврал, связанный с необходимостью выполнять проектную и повседневную работу одновременно с проведением внутреннего и внешнего аудита. Классический пример: четвертый квартал в IT-департаменте, когда на сотрудников одновременно ложится высокая нагрузка по выполнению IT-стратегии и участию в проверках службы внутреннего контроля.

5. Еще один проблемный пункт — это отсутствие механизмов оперативного мониторинга выполнения контрольных процедур и отсутствие средств автоматизации, позволяющих оперативно обрабатывать информацию о состоянии контролируемых процессов.

Как управлять большим количеством требований?

Решение этой проблемы заключается в постоянном учете и контроле всех требований, которые распространяются на организацию. Для этого оформляются карты требований. Compliance Mapping осуществляется по направлениям деятельности и поддерживается в актуальном состоянии профильным подразделением при поддержке СВК. Требования в каждой карте правильнее классифицировать по процессам или процедурам, присущим областям деятельности. Например, требования по защите от компьютерных вирусов необходимо сгруппировать в класс «антивирусная защита».

На практике часто формируют гибридную классификацию на основе применимой нормативно-правовой документации. В табл. 1 приведена классификация требований по информационной безопасности на основе стандартов СТО БР ИББС-1.2-2014[1] и PCI DSS[2]. В соответствии с классами требований формируется карта. В карту полезно включать требования, которые могут стать применимыми к компании в будущем или по требованию регулятора, или в случае наступления вероятного события, например открытия какого-либо бизнес-сервиса.

[1] Стандарт Банка России СТО БР ИББС-1.2-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации», введенный в действие Распоряжением Банка России от 17.05.2014 № Р-399.

[2] PCI DSS (Payment Card Industry Data Security Standard) – стандарт безопасности данных индустрии платежных карт, разработанный Советом по стандартам безопасности индустрии платежных карт (Payment Card Industry Security Standards Council, PCI SSC), учрежденным международными платежными системами Visa, MasterCard, American Express, JCB и Discover.

Комплаенс-контроль

Таблица 1

Пример классификации требований по информационной безопасности

Классы требований, сформированные на основе СТО БР	Классы требований, сформированные на основе PCI DSS
Обеспечение информационной безопасности при назначении и распределении ролей и обеспечение доверия к персоналу	Обеспечение сетевой безопасности
Обеспечение безопасности на стадиях жизненного цикла автоматизированных систем	Обеспечение безопасной настройки системных компонентов
Обеспечение информационной безопасности при управлении доступом и регистрацией	Обеспечение безопасного хранения информации ограниченного распространения
Обеспечение информационной безопасности средствами антивирусной защиты	Обеспечение информационной безопасности при передаче по каналам связи информации ограниченного распространения
Обеспечение информационной безопасности при использовании ресурсов сети Интернет	Обеспечение антивирусной защиты
Обеспечение информационной безопасности при использовании средств криптографической защиты информации	Обеспечение безопасной разработки программного обеспечения и безопасное управление изменениями
Обеспечение информационной безопасности банковских платежных технологических процессов	Управление логическим доступом
Обеспечение информационной безопасности банковских информационных технологических процессов	Управление физическим доступом
Обеспечение информационной безопасности банковских технологических процессов, в рамках которых обрабатываются персональные данные	Мониторинг состояния информационной безопасности
Менеджмент информационной безопасности	Управление уязвимостями и тестирование систем и процессов обеспечения безопасности
	Поддержка политики информационной безопасности и управление процессами информационной безопасности

Пример минимально необходимой карты требований представлен в табл. 2. Дополнительно в карте может быть отражена информация об ответственных за выполнение требований и о внутренних документах организации, которые содержат соответствующие положения, перечисление связанных рисков, ссылку на матрицу контролей, описание компенсационных мероприятий для требований, выполняемых не напрямую, и т.п. Составление карт требований позволяет своевременно выявлять сложности, описанные выше.

Возникающие вопросы необходимо решать коллегиально с привлечением профильного подразделения (в нашем случае — службы

Управление соответствием: комплаенс как сервис с автоматической пролонгацией статуса

Таблица 2

Пример карты требований

Класс требования	Краткое описание требования	Описание лучших практик реализации требования	Источник требования, ссылка на требование, пояснение		
			Положение № 382-П	PCI DSS	СТО БР
1	2	3	4	5	6
Обеспечение информационной безопасности при назначении и распределении ролей и обеспечение доверия к персоналу	Установление обязанностей и ответственности персонала организации по обеспечению информационной безопасности	Политика, процедуры обеспечения безопасности, а также должностные инструкции должны однозначно определять обязанности всего персонала организации, относящиеся к информационной безопасности		П. 1.1.5, 3.6.8, 12.4, 12.5, 12.5.1–12.5.5	П. М1.1–М.1.4, М1.19, М1.20
	Запрет выполнения несовместимых ролей	Запретить совмещение в рамках одной роли функций: — разработки и сопровождения; — разработки и эксплуатации; — сопровождения и эксплуатации; — IT-администратора и администратора безопасности; — администрирования и выполнения операций; — контроля и выполнения операций	П. 2.4.2, 2.4.3	П. 6.4.2	П. М1.5–М1.9
Обеспечение безопасности на стадиях жизненного цикла автоматизированных систем	Привлечение службы информационной безопасности к участию на всех этапах жизненного цикла АБС	Включать требования по информационной безопасности в техническое задание на этапе создания и модернизации информационной системы. Техническое задание должно быть согласовано со службой информационной безопасности. Служба информационной безопасности должна участвовать в приемке и вводе в действие АБС	П. 2.5.1, 2.5.2		П. М2.1–М2.3, М2.9
	Разработка безопасных приложений и информационных систем	Процесс разработки программного обеспечения должен быть основан на отраслевых стандартах и (или) известных рекомендациях.		П. 2.2.1–2.2.3, 2.2.5, П. 6.3, 6.5, 6.5.1–	

Комплаенс-контроль

Окончание табл. 2

1	2	3	4	5	6
		Информационная безопасность должна учитываться в течение всего цикла разработки программного обеспечения. В процессе разработки программного обеспечения необходимо предотвращать распространенные уязвимости программного кода. Каждый сервер должен выполнять одну основную функцию. Необходимо обеспечить функционирование только необходимых сервисов		6.5.10, 6.7	

информационной безопасности), внешнего аудитора (для требований, обязательно проверяемых внешней организацией), а также службы внутреннего контроля.

Как минимизировать риски несоответствия?

Решение этой проблемы заключается в построении эффективного процесса управления рисками. Важно не просто оценить риски несоответствия, но и понять, на какие риски направлены требования нормативно-правовых актов. Как правило, создавая закон или стандарт, регулятор задается целью понизить вероятность нежелательных для субъекта права последствий и ущерб от них. Понимание мотивации регулятора существенно помогает правильно составить мероприятия и контрольные процедуры, направленные на выполнение требований.

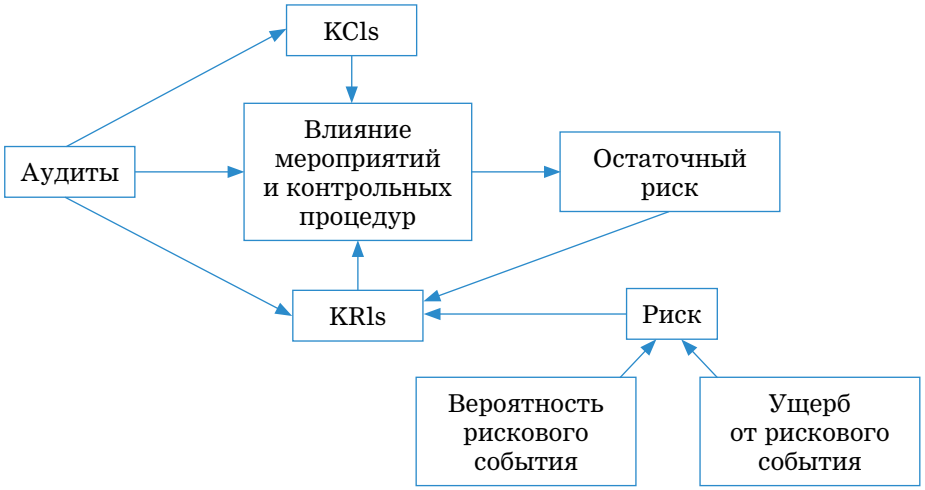
Рассмотрим, каким образом процесс управления рисками связан с процессом управления соответствием (рис. 1). Согласно классической схеме риск рассчитывается на основе вероятности рискового события и предполагаемого ущерба от него. В случае принятия решения о необходимости обработки риска определяются мероприятия, направленные на его снижение. На этом этапе полезно обратиться к карте требований как источнику возможных мер.

Выбрав для реализации соответствующие требования регуляторов, организация будет выполнять их не только для снятия риска несоответствия, а в первую очередь для снижения основного профильного

Управление соответствием: комплаенс как сервис с автоматической пролонгацией статуса

Рисунок 1

Оценка рисков и управление соответствием



риска, что обычно находится в приоритете. Знание подразделениями-исполнителями профильных рисков увеличивает эффективность выполнения мероприятий и контрольных процедур. При этом, если риск, на который направлено требование, признан в организации несущественным, можно выполнять это требование на минимально необходимой формальной основе.

При управлении рисками полезно использовать следующие инструменты, связанные с управлением соответствием:

— управление мероприятиями, направленными на снижение риска;

— ключевые индикаторы риска (KRI);

— ключевые показатели состояния контрольных процедур, связанных с риском (KCI);

— внутренний и внешний аудит.

Результаты работы этих инструментов можно включать в расчет остаточного риска.

Управление мероприятиями, направленными на снижение риска, заключается как минимум в контроле следующих параметров:

— эффективности мероприятий, направленных на снижение вероятности и (или) ущерба рискового события (показателя того, насколько мероприятие снижает риск);

— степени выполнения мероприятий, направленных на снижение вероятности и (или) ущерба рискового события.

Комплаенс-контроль

Ключевые индикаторы риска предназначены для мониторинга состояния риска, но также могут являться источником информации о состоянии мероприятий, направленных на снижение риска.

Ключевые показатели состояния контрольных процедур дают уверенность, что проведен мониторинг и организация оперативно отреагировала на ситуацию с риском, которая была идентифицирована с помощью KRI. На практике KCI отслеживают эффективность и степень выполнения контрольных процедур.

Разница между контрольной процедурой и мероприятием минимальна — в итоге любые действия должны быть направлены на снижение риска. В зарубежной литературе для их обозначения часто используется один термин — control (контроль). В русском языке удобнее называть мероприятием процедуру, непосредственно направленную на снижение риска (выполнение требования) (рис. 2), а контролем — процедуру проверки правильности выполнения мероприятия (рис. 3).

Рисунок 2

Выполнение требования стандарта PCI DSS по блокировке учетных записей уволенных сотрудников с целью снижения риска нарушения конфиденциальности информации ограниченного распространения

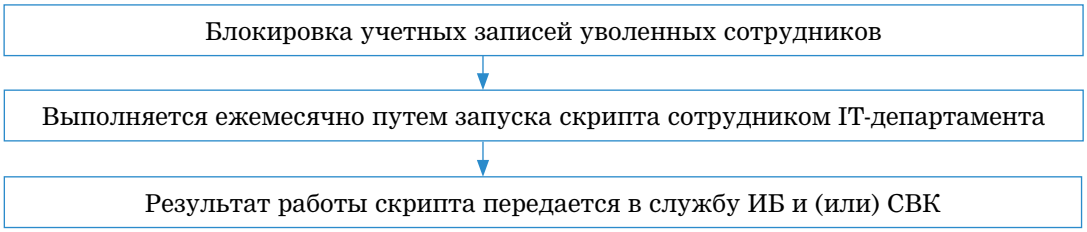
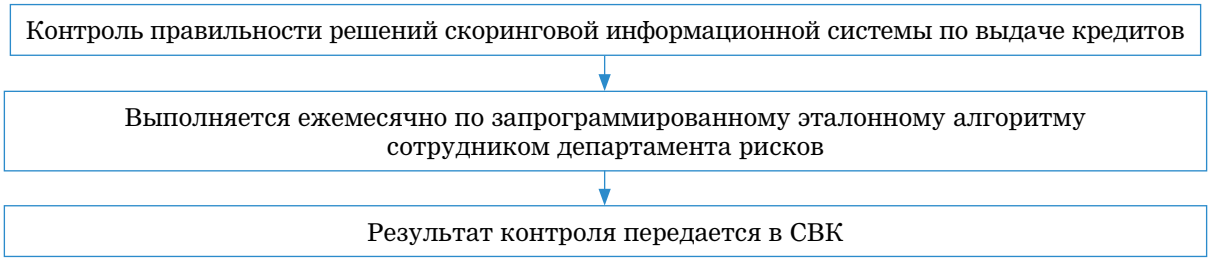


Рисунок 3

Выполнение внутреннего контроля департаментом рисков по соглашению с СВК



Управление соответствием: комплаенс как сервис с автоматической пролонгацией статуса

Внутренний и внешний аудит, являясь средством GAP-анализа, показывает правильность процессов, эффективность выбранных показателей KRI, KCI. Например, для контроля, изображенного на рис. 3, сотрудник СВК может проверять целостность и правильность работы эталонного алгоритма.

Взаимодействие подразделений в мероприятиях и контрольных процедурах

В мероприятиях и контрольных процедурах должны быть задействованы все подразделения организации, между которыми должны быть разделены бизнес-функции, исполнительские функции и независимые надзорные функции.

Бизнес-функции сосредоточены у владельцев мероприятий и контрольных процедур и заключаются:

— в формировании дизайна мероприятий и контрольных процедур;

— мониторинге эффективности мероприятий или контролей и пересмотре их дизайна.

Исполнительские функции распределены между профильными подразделениями: IT-департаментом, службой информационной безопасности, департаментами розничного и корпоративного бизнеса и пр. Исполнители выполняют контроли и мероприятия по своему профилю, осуществляют сбор свидетельств в рамках контролей и мероприятий и передают их в надзорные подразделения.

Независимые надзорные функции сосредоточены в СВК:

— участие в создании дизайна мероприятий и контрольных процедур;

— согласование дизайна мероприятий и контрольных процедур;

— проверка эффективности мероприятий и контролей и направление владельцам предложений по их дизайну;

— оценка адекватности свидетельств, собранных в рамках контролей и мероприятий;

— проведение выборочных аудитов соответствия процессов.

Инструментом процесса управления мероприятиями и контрольными процедурами является матрица контролей, содержащая описание дизайна мероприятий и контролей.

Матрица контролей

Инструментом процесса управления мероприятиями и контрольными процедурами является матрица контролей, содержащая описание дизайна мероприятий и контролей. Матрица может содержать следующие поля: наименование мероприятия и контроля; исполнители; ответственные за контроль; дата назначения; срок исполнения; периодичность исполнения; свидетельства исполнения; отчетность; профильный риск.

Комплаенс-контроль

При определении дизайна мероприятий и контролей необходимо помнить о правилах, повышающих их эффективность:

1) их стоимость не должна превышать размер возможного ущерба от реализации риска, на снижение которого они направлены;

2) они должны быть действительно необходимы, то есть привязаны к риску;

3) их выполнение должно мотивироваться менеджментом организации;

4) они должны выполняться на нескольких уровнях (например, менеджер должен согласовывать бюджет на канцелярские товары в целом, но не должен согласовывать покупку карандашей);

5) они должны быть простыми, и это одно из самых важных правил. Практика показывает, что сложность реализации приводит к низкой эффективности. Хорошие контроли или мероприятия являются автоматизированными, выполняемыми по умолчанию.

Сервисный подход к управлению соответствием

На основании матрицы контролей можно реализовать сервисный подход к управлению соответствием, который применим как внутри организации, так и при взаимодействии с внешними аудиторами. Заказчиком сервиса выступает подразделение — владелец процесса, на которое распространяются требования. Исполнителями являются профильные подразделения и при необходимости — внешний аудитор или консультант. Важно понимать, что необходимость соблюдения независимости внешнего аудита не является основанием для назначения аудитора на роль заказчика. Например, такая ошибка построения контрольной среды допускается, когда аудитором является регулятор, который может в ультимативной форме требовать предоставления ему свидетельств.

Основным документом, регламентирующим порядок взаимодействия всех сторон при сервисном подходе, является Соглашение об уровне сервиса. Соглашение должно определять план контрольных действий, который фиксирует роли всех участвующих сторон от бизнеса, исполнителей и независимого контроля, определяет порядок взаимодействия этих подразделений, удобно распределяет проверочную деятельность по времени.

Соглашение должно фиксировать параметры из матрицы контролей. При работе с внешним аудитором необходимо отдельно прописать требования по обеспечению непрерывности проверяемых процессов и информационных систем, а также время обработки и анализа собранных свидетельств.

Управление соответствием: комплаенс как сервис с автоматической пролонгацией статуса

Необходимость пригласить внешнего аудитора или консультанта для управления соответствием возникает по следующим причинам:

— из-за отсутствия внутренней экспертизы у персонала;

— нехватки времени у персонала;

— отсутствия экономической выгоды (затраты на привлечение внешнего консультанта ниже).

Основная цель внешнего консультанта — организовать процесс сбора свидетельств для регулятора, его задачами являются:

— формирование и согласование области работ (карта требований и границы аудита);

— проведение оценки рисков (при необходимости);

— формирование и согласование матрицы контролей;

— формирование и согласование выборки по контрольным процедурам;

— контроль предоставления свидетельств в соответствии с периодичностью, заданной регулятором, или исходя из риск-ориентированного подхода;

— управление свидетельствами (сбор, безопасное хранение, передача заказчику и регулятору (при необходимости), безопасное уничтожение свидетельств по истечении срока хранения);

— анализ соответствия предоставленных свидетельств требованиям регулятора или требованиям по снижению риска;

— предоставление экспертизы о методах проверок регулятора;

— предоставление экспертизы в предметной области;

— формирование отчетности;

— участие на стороне заказчика в проверках организации регулятором.

Наиболее эффективным будет привлечение внешнего консультанта из компании, которая аккредитована регулятором на выполнение соответствующих контрольных процедур. В области информационной безопасности к подходящим проектам относятся работы по поддержанию соответствия нормативным документам Банка России (комплексу стандартов СТО БР ИББС, Положению № 382-П), стандартам международных платежных систем (PCI DSS, PA DSS, Visa PIN Security, Visa ACS), законодательству о защите персональных данных (Закону № 152-ФЗ и подзаконным актам).

Преимущества реализации сервисного подхода при поддержании соответствия приведены в табл. 3. На рис. 4 приведен пример поддержания соответствия требованиям стандарта PCI DSS о ежеквартальном внешнем сканировании на наличие уязвимостей с использованием соглашений об уровне услуг (SLA).

На основании матрицы контролей можно реализовать сервисный подход к управлению соответствием, который применим как внутри организации, так и при взаимодействии с внешними аудиторами.

Комплаенс-контроль

Рисунок 4

Проведение ежеквартального внешнего сканирования на наличие уязвимостей с использованием SLA

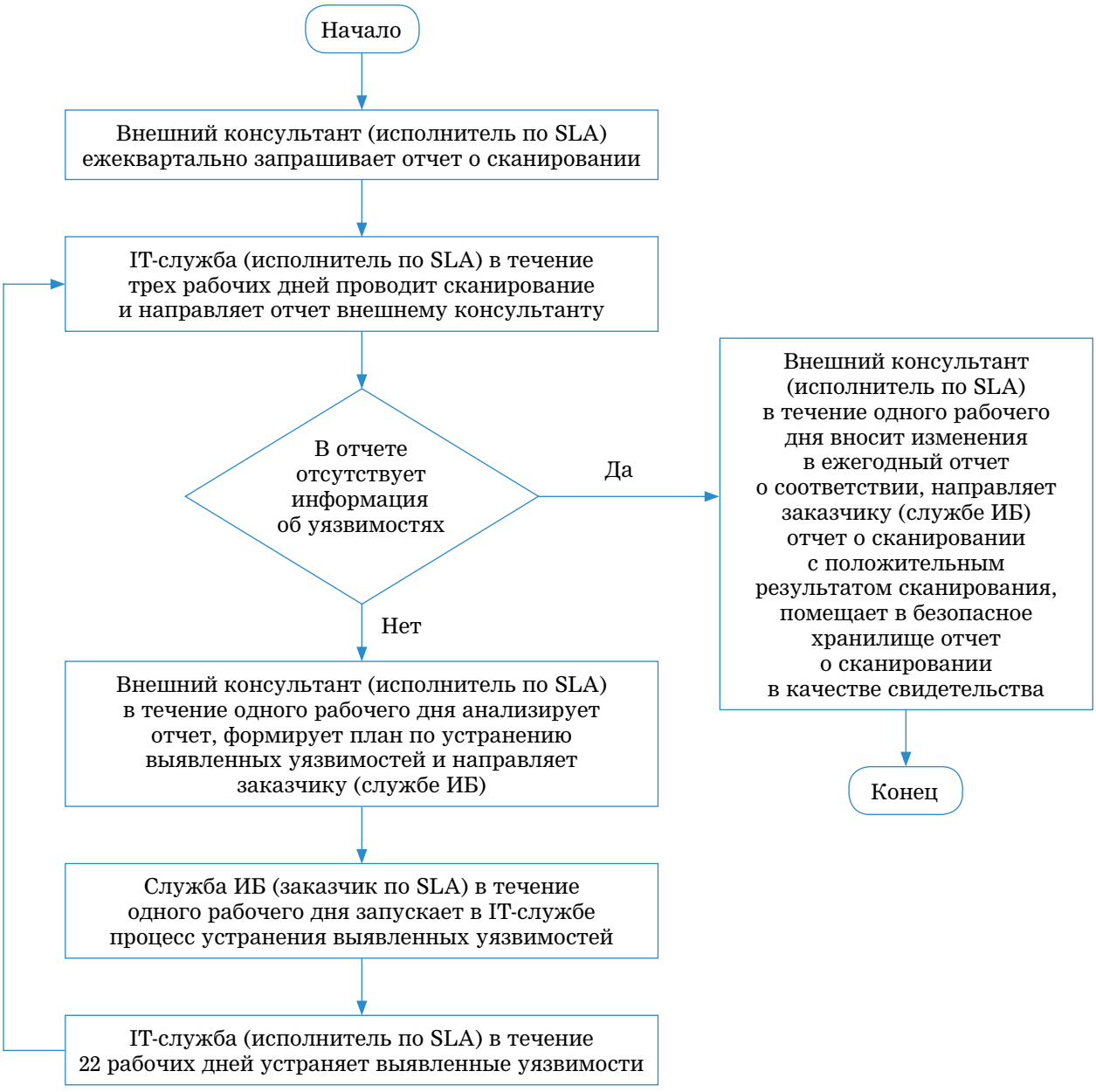


Таблица 3

Преимущества реализации сервисного подхода при поддержании соответствия

Поддержание соответствия в течение всего периода работ	Ежегодный аудит
Распределение трудозатрат на проверяемые подразделения в течение всего периода работ. Выявление недостатков в течение всего периода работ (как правило, одного года) и их исправление по расписанию	Повышенная нагрузка на проверяемые подразделения в период аудита. Выявление всех недостатков в течение аудита (как правило, одного месяца) и их исправление в авральном режиме
Период работ позволяет сопровождать всю область проверок	Вероятны ошибки определения области проверки и репрезентативности выборки
Консалтинг проводится в течение всего периода работ	Консалтинг проводится только на этапе аудита
К окончанию периода работ возникает уверенность в подтверждении соответствия. Пакет свидетельств сформирован, отчетность подготовлена и отправлена регулятору. Статус соответствия пролонгирован на год	Отсутствует уверенность в положительном результате аудита, т.к. с момента прошлогодней проверки требуемые регулятором процессы могли быть серьезно нарушены, на исправление необходимо значительное время

Механизмы для оперативного мониторинга выполнения контрольных процедур

Рассмотрим проблему отсутствия механизмов для оперативного мониторинга выполнения контрольных процедур, а также отсутствия средств автоматизации, позволяющих оперативно обрабатывать информацию о состоянии контролируемых процессов.

Проблемы могут быть у организаций, в структуре которых функционируют хотя бы пять полноценных региональных филиалов. У них возникают сложности в процессе:

— ведения отдельной карты требований, карты рисков, матрицы контролей;

— сбора значительных объемов информации и свидетельств в центральном офисе;

— оперативного анализа информации и свидетельств;

— организации реагирования на выявленные несоответствия;

— предоставления отчетности различных уровней детализации.

Решением являются продукты класса GRC (governance, risk management and compliance), представляющие функционал базы данных с возможностью обработки, структурирования и хранения информации о требованиях, рисках, мероприятиях и контрольных процедурах. Решения представляют удобный интерфейс ввода информации со всех региональных подразделений, позволяют обрабаты-

Комплаенс-контроль

вать и анализировать исходные данные, формировать отчетность разных уровней представления, что позволяет эффективно управлять процессами соответствия и риск-менеджмента. Например, нет необходимости сообщать руководителю топ-уровня низкоуровневую информацию о DDoS-атаке. Достаточно назвать направление, требующее реагирования, и сообщить о повышении риска до границы риск-аппетита в форме представления «светофор»: «красный уровень угрозы в филиалах № 1 и № 5 по блоку «Информационная безопасность, ФИО ответственного руководителя блока».

При управлении соответствием в области информационной безопасности необходимо помнить об автоматизированных инструментах, которые обычно используются службами информационной безопасности:

— мониторинг событий (SIEM);
— противодействие утечкам информации (DLP);
— обнаружение сетевых вторжений (IDS/IDM);
— контроль целостности (FIM);
— сканирование на уязвимости;
— и др.

Результаты работы всех этих инструментов также полезно ввести в систему GRC для автоматизированной обработки данных, влияющих на уровень соответствия.

При взаимодействии с внешним консультантом можно использовать как системы GRC, так и специализированные продукты класса helpdesk, которые позволяют реализовать сервис в формате 24×7 с разделением доступа, обеспечением безопасности канала связи и области хранения конфиденциальной информации, а также обладают возможностями оперативного управления запросами со стороны заказчика с соблюдением параметров, заложенных в SLA.

В заключение следует подчеркнуть, что выполнение надзорной функции должно быть отделено от исполнительской, при этом к участию в контрольной среде полезно привлекать абсолютно всех работников организации. В организации поддерживается необходимый уровень соответствия, если у руководства есть мотивация создать эффективные коммуникации между различными подразделениями и стремление донести до всех субъектов контрольной среды цели, на достижение которых направлен процесс обеспечения соответствия. Рассмотренные в статье инструменты управления мероприятиями и контрольными процедурами, управления рисками, средства автоматизации деятельности помогают преобразовать мотивацию менеджмента в реальную пользу для организации, снижая ее профильные риски.