Кибербезопасность

Topical Requirement

Руководство по применению

Тематических требований

The Institute of
Internal Auditors

Содержание

Обзор тематических требований

Наряду с Global Internal Audit Standards™ (Международными стандартами внутреннего аудита) и Международным руководством важнейшей составляющей The International Professional Practices Framework® (Международных основ профессиональной практики) являются Тематические требования. Международный институт внутренних аудиторов (IIA) требует, чтобы Тематические требования использовались в сочетании с Global Internal Audit Standards™ (Международными стандартами внутреннего аудита) , которые формируют авторитетную основу требуемой практики. Ссылки на Стандарты приводятся в данном руководстве в качестве источника более подробной информации.

Тематические требования определяют то, как внутренние аудиторы рассматривают распространенные области риска, и тем самым способствуют систематизации и повышению качества услуг внутреннего аудита. Тематические требования устанавливают базовый уровень и предоставляют соответствующие критерии для оказания услуг по обеспечению уверенности, относящихся к предмету Тематических требований (Стандарт 13.4 «Критерии оценки»). Соответствие Тематическим требованиям является обязательным при оказании услуг по обеспечению уверенности и рекомендуется при оказании консультационных услуг. Тематические требования не охватывают все потенциальные аспекты, которые следует учитывать при выполнении аудиторских заданий по обеспечению уверенности, а предоставляют минимальный набор требований для проведения , надежной оценки в соответствующей области.

Тематические требования прямо связаны с моделью «трех линий» (IIA) и Международными стандартами внутреннего аудита. Процессы руководства организацией, управления рисками и внутреннего контроля являются основными компонентами Тематических требований, в соответствии со Стандартом 9.1 "Понимание процессов руководства организацией, управления рисками и внутреннего контроля". В соответствии с моделью "трех линий", руководство организацией связано с Советом/наблюдательным органом, управление рисками – со второй линией, а внутренний контроль или процессы контроля – с первой линией. Менеджмент представлен на первой и второй линиях, а внутренний аудит изображен на третьей линии как независимый и объективный поставщик уверенности, подотчетный Совету / наблюдательному органу (Принцип 8 «Осуществление надзора со стороны Совета»).

Применимость, риск и профессиональное суждение

Тематические требования должны соблюдаться, когда функции внутреннего аудита выполняют задания по обеспечению уверенности в тех вопросах, в отношении которых

действуют Тематические требования, или когда аспекты Тематических требований выявлены в рамках других заданий по обеспечению уверенности.

Как описано в Стандартах, оценка рисков является важной частью планирования, выполняемого руководителем внутреннего аудита. Для определения заданий по обеспечению уверенности, которые должны быть включены в план работы внутреннего аудита, необходимо по крайней мере ежегодно проводить оценку стратегий, целей и рисков организации (Стандарт 9.4 «План внутреннего аудита»). При планировании отдельных заданий по обеспечению уверенности внутренние аудиторы должны оценить риски, относящиеся к заданию (Стандарт 13.2 «Оценка рисков в рамках аудиторского задания»).

Если область Тематических требований определена в процесса риск ориентированного планирования и включена в план аудита, то требования, изложенные в Тематических требованиях, должны быть использованы для оценки данной области в рамках применимых аудиторских заданий. Кроме того, когда внутренние аудиторы выполняют задание (включенное или не включенное в план) и при этом проявляются элементы Тематических требований, Тематические требования должны быть оценены на предмет применимости в рамках задания. И наконец, если имеется запрос на выполнение задания, которое изначально не было в плане и включает соответствующую область , необходимо оценить применимость Тематических требований.

Профессиональное суждение играет ключевую роль в применении Тематических требований. Оценки рисков лежат в основе решений руководителей внутреннего аудита о том, какие задания включить в план внутреннего аудита (Стандарт 9.4 «План внутреннего аудита»). Кроме того, внутренние аудиторы используют профессиональное суждение, чтобы определить, какие аспекты будут охвачены в рамках каждого аудиторского задании (Стандарты 13.3 «Цели и объем аудиторского задания», 13.4 «Критерии оценки» и 13.6 «Программа аудиторского задания»). В Приложении А «Примеры практического применения» описано, как внутренние аудиторы определяют применимость Тематических требований.

Необходимо сохранить доказательства того, что все требования Тематических требований были оценены на предмет применимости, включая обоснование исключения каких-либо требований. Соответствие Тематическим требованиям должно документироваться с использованием профессионального суждения аудитора, как описано в Стандарте 14.6 «Документация аудиторского задания».

В то время как тТематические требования в области кибербезопасности предоставляют базовый набор процессов внутреннего контроля, организациям с очень высоким киберриском может потребоваться оценка дополнительных аспектов.

Если руководитель внутреннего аудита определяет, что функция внутреннего аудита не обладает необходимыми знаниями для выполнения аудиторских заданий в области Тематических требований, работа по выполнению задания может быть передана на аутсорсинг (Стандарты 3.1 «Компетентность», 7.2 «Квалификация руководителя

внутреннего аудита», 10.2 «Управление кадровыми ресурсами»). Даже в случае передачи работы на аутсорсинг это не освобождает функцию внутреннего аудита от необходимости соблюдать Тематические требования. Руководитель внутреннего аудита несет полную ответственность за обеспечение соответствия. Кроме того, если руководитель внутреннего аудита считает, что у функции внутреннего аудита недостаточно ресурсов, он должен сообщить Совету о неблагоприятных последствиях дефицита ресурсов и мерах по его устранению (Стандарт 8.2 «Ресурсы»).

Деятельность, документация и отчетность

Применяя Тематические требования, внутренние аудиторы также должны соответствовать Стандартам, проводя свою работу в соответствии с Разделом V: Предоставление услуг внутреннего аудита. В Стандартах Раздела V описаны процессы планирования аудиторских заданий (Принцип 13 «Осуществляйте эффективное планирование аудиторских заданий»), выполнения аудиторских заданий (Принцип 14 «Выполняйте аудиторское задание») и информирования о заключениях по результатам аудиторского задания (Принцип 15 «Информируйте о результатах аудиторского задания и осуществляйте мониторинг планов действий»).

Область применения Тематических требований может быть зафиксирована в плане внутреннего аудита или в рабочей документации задания на основании профессионального суждения аудиторов. Все требования могут охватывать одно или несколько аудиторских заданий . Кроме того, не все требования могут быть применимы. Необходимо сохранить доказательства проведения оценки Тематических требований на предмет применимости, включая обоснованиелюбых исключений.

Дополнительный инструмент, приведенный в Приложении C, можно использовать в качестве справочного и для документирования работы, выполняемой внутренними аудиторами.

Обеспечение качества

Согласно Стандартам руководители внутреннего аудита должны разработать, внедрить и поддерживать программу обеспечения и повышения качества, охватывающую все аспекты функции внутреннего аудита (Стандарт 8.3 «Качество»). Результаты должны быть доведены до сведения Совета и высшего исполнительного руководства. В этих сообщениях должны содержаться сведения о соответствии функции внутреннего аудита Стандартам и достижении целевых параметров деятельности.

Соответствие Тематическим требованиям будет проверяться в ходе оценок качества. Для подготовки к оценке качества внутренние аудиторы могут использовать инструмент, представленный в Приложении C.

Кибербезопасность

Кибербезопасность – это обширная тема, связанная с большинством технологических аспектов любой организации. Помимо информационных технологий, кибербезопасность обычно является частью бизнес-процессов, что требует от

внутренних аудиторов проведения оценки киберрисков при планировании, определении объема и выполнении заданий по обеспечению уверенности.

Национальный институт стандартов и технологий (NIST), входящий в состав Министерства торговли США, дает следующее определение кибербезопасности: «Способность защищать или оберегать использование киберпространства от кибератак». Тематические требования в области кибербезопасности фокусируются на внешнем периметре, который организации защищают для снижения рисков, связанных с неавторизованными пользователями и вредоносными киберугрозами. Кибербезопасность – это часть общей информационной безопасности, которую NIST определяет как «защиту информации и информационных систем от неавторизованного доступа, использования, раскрытия, нарушения работы, искажения или уничтожения в целях обеспечения конфиденциальности, целостности и доступности».

Тематические требования в области кибербезопасности включают:

- Руководство – четко определенные базовые цели и стратегии в области кибербезопасности, которые поддерживают цели, политику и процедуры организации.
- Управление рисками – процессы выявления, анализа, управления и мониторинга киберугроз, включая процесс оперативной эскалации относящихся к киберрискам вопросов.
- Средства контроля – установленные менеджментом и периодически оцениваемые процессы внутреннего контроля для снижения киберрисков.

Рекомендации

Внутренние аудиторы могут следовать следующим рекомендациям для оценки требований, содержащихся в Тематических требованиях в области кибербезопасности. Эти рекомендации, содержащие перекрестные ссылки на требования, являются иллюстративными, но не обязательными. Внутренним аудиторам следует полагаться на профессиональное суждение при определении того, что включать в свои оценки.

Рекомендации по руководству организацией

Чтобы оценить, как процессы руководства организацией применяются для достижения целей кибербезопасности, внутренние аудиторы могут проверить следующее:

A. Формализованный, документально оформленный стратегический план и цели в области кибербезопасности, включая доказательства того, что Совет периодически (как правило, ежеквартально) изучает обновленную информацию о кибербезопасности, предоставляемую руководителем подразделения информационной безопасности, например, директором по информационной безопасности (CISO). Доказательства могут включать отчетность по:
    - Мониторингу достижения стратегических целей.
    - Бюджетным потребностям для поддержки целей и задач в области кибербезопасности.
    - Рискам и средствам внутреннего контроля, включая информацию о ходе устранения недостатков.
    - Ключевым показателям эффективности (KPI) для оценки успеха.
    - Кадровым ресурсам, необходимым для найма, обучения и развития персонала в области кибербезопасности.

B. Политики, процедуры и другую соответствующую документацию, используемуя для управления процессами в области кибербезопасности, включая:
    - Политики, которые пересматриваются и обновляются как минимум один раз в год. Возникающие киберриски могут потребовать более частого пересмотра и обновления.
    - Процесс определения достаточности политик и процедур для поддержки деятельности по обеспечению кибербезопасности.
    - Широко распространенные стандарты (NIST, COBIT и прочие) для укрепления процессов кибербезопасности и средств внутреннего контроля.

C. Роли и обязанности, способствующие достижению целей в области кибербезопасности, включая организационную структуру, которая обеспечивает нахождение подразделения кибербезопасности на уровне, достаточно значимом для достижения организационной поддержки.
    - Процесс периодической оценки знаний, навыков и умений персонала, выполняющего функции в области кибербезопасности.

D. Доказательство взаимодействия с соответствующими заинтересованными сторонами (например, высшим исполнительным руководством, операционными подразделениями, отделом управления рисками, отделом по управлению кадровыми ресурсами, юридическим отделом, отделом комплаенс, стратегическими поставщиками и другими), включая информирование о существующих и возникающих киберрисках и известных потенциальных уязвимостях. Доказательством взаимодействия могут служить протоколы совещаний, отчеты или электронные письма.

Рекомендации по управлению рисками

Чтобы оценить, как процессы управления рисками применяются для достижения целей кибербезопасности, внутренние аудиторы могут проверить следующее:

A. Как организация оценивает риски кибербезопасности и управляет ими, включая то, как угрозы и уязвимости:
   - Первоначально выявляются и способы информирования о них.
   - Анализируются с точки зрения риска для достижения целей организации.
   - Снижаются, включая планы действий по снижению риска до приемлемого уровня.
   - Контролируются, включая постоянное предоставление отчетности до полного устранения угроз.

B. Как организация периодически получает информацию об управлении рисками в области кибербезопасности от функциональных подразделений, таких как информационные технологии, управление рисками, отдел управления кадровыми ресурсами, юридический отдел, отдел комплаенс, операционные подразделения, бухгалтерия и финансовый отдел. Для получения информации может использоваться межфункциональная группа по кибербезопасности или руководящий комитет по ИТ.

C. Как организация возложила ответственность за управление рисками кибербезопасности на отдельное лицо или группу лиц.
   - Ответственному лицу (лицам) следует периодически (ежеквартально, ежемесячно или по мере необходимости) распространять в рамках организации обновленную информацию о рисках кибербезопасности, которая также может включать требования к ресурсам для реализации стратегий по снижению рисков.

D. Процессы эскалации рисков кибербезопасности, включая порядок оценки, определения и приоритезации уровня угрозы или риска. Проверка может включать определение:

- Установленных в организации уровней риска – высокий, средний и низкий – с подробным объяснением каждого уровня риска и процедурами эскалации для каждой категории риска.
- Списка выявленных в настоящее время рисков кибербезопасности и статус устранения каждого из них.
- Применимых юридических, нормативных требований и требований комплаенса.
- Воздействие как финансовых, так и нефинансовых (например, репутационных) рисков.

E. Процесс информирования менеджмента и сотрудников о рисках кибербезопасности, который включает:

- Периодическое (минимум один раз в год) обучение сотрудников в области кибербезопасности, например, проведение необъявленных имитационных фишинговых кампаний для проверки и отслеживания осведомленности организации.
- Предоставление обновленной информации об устранении существующих проблем кибербезопасности с указанием предполагаемых сроков завершения работ.
- Мониторинг несоблюдения требований, включающий информирование Совета и высшего исполнительного руководства.
- Переоценку угроз при изменении склонности организации к риску и толерантности к нему.

F. Процессы реагирования на инциденты и восстановления, внедренные организацией, которые включают:

- Документированный план, который пересматривается и обновляется по мере возникновения изменений в деятельности организации. План должен включать:
  - Способы обнаружения инцидентов и информирования о них.
  - Способы локализации инцидентов для предотвращения дальнейшего ущерба.
  - Способы восстановления и реагирования с целью возобновить деятельность организации.
  - Способы анализа инцидента с целью извлечь уроки и определить способы предотвращения подобных событий в будущем.
- Периодическое (минимум один раз в год) тестирование (сценарное обсуждение) и представление отчета о результатач высшему исполнительному руководству и соответствующим заинтересованным

сторонам. По результатам тестирования могут быть разработаны планы действий.

Рекомендации по процессу внутреннего контроля

Чтобы оценить, как процессы внутреннего контроля применяются для достижения целей кибербезопасности, внутренние аудиторы могут проверить следующее:

A. Подход менедмента к созданию эффективной среды внутреннего контроля в области кибербезопасности, включая следующие аспекты:
   - Оценка и внедрение средств внутреннего контроля, необходимых для снижения повышенных рисков и защиты секретных, критически важных, личных или конфиденциальных данных, на основе процесса оценки организационных рисков.
   - Определение потребностей в ресурсах для поддержания ключевых средств контроля в области кибербезопасности.
   - Рассмотрение средств контроля поставщиков в качестве части среды контроля, что включает проверку отчетов поставщиков о контроле в сервисной организации (SOC) до начала деловых отношений и в течение всего срока их действия.
   - Периодическая проверка того, что средства контроля в области кибербезопасности функционируют таким образом, что снижают риски и способствуют достижению целей в области кибербезопасности.
   - Процесс устранения недостатков внутреннего контроля или устранения замечаний по результатам оценок, проведенных функцией внутреннего аудита или другими поставщиками услуг по обеспечению уверенности (например, тестирование на возможность проникновения).

B. Процесс управления кадровыми ресурсами организации для найма и обучения специалистов в области кибербезопасности, включая то, как организация выявляет возможности для повышения квалификации специалистов в области кибербезопасности с целью поддержания технических знаний и улучшения осведомленности организации о возникающих проблемах.
   - В качестве примера можно привести участие в тренингах, участие в группах по обмену знаниями и постоянное профессиональное образование, включающее получение сертификатов в кибер-области.

C. Процесс постоянного выявления, приоритезации, мониторинга и отчетности о возникающих угрозах и уязвимостях в области кибербезопасности, ориентированный на повседневную деятельность. В ходе проверки может быть установлено, что созданы процессы для оценки угроз и уязвимостей, связанных с новыми или появляющимися технологиями, такими как использование искусственного интеллекта.

D. Процессы и средства контроля, установленные менеджментом для управления ИТ-активами и их защиты на протяжении всего жизненного цикла, включая выбор, использование, техническое обслуживание и вывод из эксплуатации

аппаратного и программного обеспечения, а также услуг поставщиков. К аппаратным средствам относятся серверы, сетевое оборудование (например, маршрутизаторы или брандмауэры), настольные компьютеры, ноутбуки, мобильные телефоны, планшеты и периферийные устройства. Программное обеспечение включает в себя операционные системы (например, Windows), программное обеспечение для планирования ресурсов предприятия, приложения, антивирусные программы и прочее. Рекомендации относительно аппаратного и программного обеспечения могут включать в себя:

- Использование организацией шифрования, антивирусного программного обеспечения, управления мобильными устройствами, требований об использовании сложных паролей, виртуальных частных сетей (VPN)/сетевого доступа с нулевым доверием (ZTN) для аутентификации и периодического обновления встроенного ПО.
- Процесс управления активами, гарантирующий, что выданное компанией аппаратное обеспечение имеет соответствующую конфигурацию безопасности при выдаче и надлежащим образом утилизируется при выводе активов из эксплуатации.
- Средства контроля, связанные с базами данных, которые включают ограничение доступа пользователей и администраторов, обеспечение использования шифрования, резервного копирования и тестирования баз данных, а также наличие надежных средств контроля сетевой безопасности.
- Способы учета угроз или уязвимостей кибербезопасности в жизненном цикле разработки системы (SDLC).
- Подход, используемый в методологии DevSecOps для обеспечения кибербезопасности в процессе разработки программного обеспечения с целью упреждающего выявления уязвимостей.

E. Процессы, используемые для усиления кибербезопасности, в том числе:

- Настройка параметров безопасности для минимизации рисков кибербезопасности.
- Управление мобильным устройством (включая использование электронной почты и приложений) настроено таким образом, чтобы снизить риски кибербезопасности и обеспечить удаленное управление в случае взлома устройства пользователя.
- Использование шифрования для неактивных данных, например, информации, хранящейся на жестком диске, или передаваемых данных, например, для шифрования сообщений электронной почты.
- Обновление серверов или программного обеспечения (например, операционной системы) последними версиями систем безопасности.
- Управление доступом пользователей, например, использование многофакторной аутентификации (MFA) и уникальных идентификаторов

пользователей со сложными паролями, срок действия которых периодически истекает.

- Мониторинг средств контроля, которые позволяют убедиться, что ресурсы доступны и работают должным образом, позволяя изучать и анализировать потенциальные проблемы в области кибербезопасности, угрожающие деятельности.
- Интеграция средств кибербезопасности в SDLC для выявления и устранения уязвимостей в области кибербезопасности до запуска программного обеспечения.

F. Связанные с сетью средства контроля, обеспечивающие безопасность периметра организации, включая способы использования организацией следующего:
   - Сегментация сети.
   - Брандмауэры.
   - Средства контроля доступа пользователей.
   - Ограничения на внешние и внутренние соединения.
   - Средства контроля над интернетом вещей (IoT) для взаимосвязанных сетей.
   - Системы обнаружения и предотвращения вторжений для предотвращения, обнаружения кибератак и восстановления после них.

G. Средства контроля безопасности конечных точек, применяемые к таким сервисам, как электронная почта, интернет-браузеры, видеоконференции, обмен сообщениями (Zoom, MS Teams и другие), социальные сети, облачные технологии и протоколы совместного использования файлов. Средства контроля могут включать ограничение использования определенных расширений файлов (например, файлов .exe) и многофакторную аутентификацию при совместном использовании файлов.

Приложение A. Примеры практического применения

В следующих примерах описаны сценарии, в которых могут быть применимы Тематические требования в области кибербезопасности:

Пример 1: Вопросы кибербезопасности являются частью задания по внутреннему аудиту, включенного в план внутреннего аудита.

Когда функция внутреннего аудита завершает процесс планирования, основанный на оценке рисков, и включает в план внутреннего аудита одно или несколько заданий по вопросам кибербезопасности, Тематические требования являются обязательными при выполнении таких заданий. Соответствие может быть достигнуто путем применения требований в ходе выполнения одного или нескольких заданий в плане внутреннего аудита.

Кибербезопасность – это обширная тема, и не все требования из Тематических требований могут быть применены в каждом задании. Если внутренние аудиторы применяют профессиональное суждение и определяют, что одно или несколько требований Тематического требований в области кибербезопасности неприменимы и поэтому должны быть исключены из задания, они должны зафиксировать и сохранить обоснование исключения этих требований. Например, основанием для исключения некоторых требований может быть то, что функция внутреннего аудита выполняет различные задания по кибербезопасности в порядке очередности или она определила, что значимость риска в данном задании низкая.

Пример 2: Риски кибербезопасности выявлены в ходе аудиторского задания, не ориентированного на кибербезопасность.

Внутренние аудиторы могут выявить риски кибербезопасности при оценке процесса, не имеющего прямого отношения к кибербезопасности. Например, внутренние аудиторы могут оценивать процесс работы с кредиторской задолженностью в рамках задания, не направленного на кибербезопасность, и не включать риски кибербезопасности в сферу охвата при планировании задания. Однако после проведения первоначальной проверки внутренние аудиторы определяют, что такие риски должны входить в сферу охвата. Например, они выявляют риски кибербезопасности, связанные с подачей первоначального запроса на заказ через Интернет (Стандарт 13.2 «Оценка рисков в рамках аудиторского задания»).

После выявления соответствующих рисков внутренние аудиторы должны проанализировать Тематические требования в области кибербезопасности и

определить, какие требования применимы. В данном примере они могут исключить процесс управления кибербезопасностью или процесс управления рисками кибербезопасности. Они должны зафиксировать и сохранить в рабочей документации обоснование исключения других требований из Тематических требований в области кибербезопасности.

Пример 3: Есть запрос на выполнение задания в области кибербезопасности, которое изначально не было включено в план внутреннего аудита.

Заинтересованные стороны, такие как Совет, менеджмент или регулирующий орган, могут сделать внутренним аудиторам запрос на проведение оценки кибербезопасности, который не был включен в первоначальный план аудита. Например, если организация подверглась кибератаке, Совет может сделать запрос на выполнение аудиторского задания для оценки средств контроля кибербезопасности. Если Тематические требования применимы, необходимо провести их оценку и зафиксировать любые исключения.

Приложение B. Сопоставление с руководствами

Организация может предпринимать собственные усилия по обеспечению кибербезопасности, используя стандарты по управлению рисками и руководству организациями, такие как COBIT или NIST. Внутренние аудиторы, возможно, уже разработали программы аудита и процедуры тестирования на основе этих стандартов. Внутренним аудиторам следует согласовать планируемое тестирование средств контроля кибербезопасности с Тематическими требованиями, чтобы обеспечить адекватный охват. В приведенной ниже таблице Тематические требования по кибербезопасности сопоставлено с тремя широко используемыми стандартами: NIST Cybersecurity Framework 2.0, COBIT 2019 и NIST 800-53. На выбор именно этих стандартов повлияла их доступность.

Требования к руководству организацией	Ссылки на стандарты		
	NIST CSF 2.0	NIST 800-53	COBIT 2019
A. Разработаны и периодически обновляются стратегия и цели в области кибербезопасности. Совет периодически получает и рассматривает информацию о достижении целей кибербезопасности, включая рекомендации в отношении ресурсов и бюджета для поддержки стратегии кибербезопасности.	GV.RM-01; GV.RM-02; GV.RM-03; GV.RM-04; GV.OC-02; GV.RR-03; GV.RR-04; GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-03	PM-1, PM-4; AT-2; AT-3; PM-9; PM-28	EDM01; EDM03; EDM04; APO06; APO01; APO10; APO12
B. Политика и процедуры, связанные с кибербезопасностью, разработаны, периодически обновляются и укрепляют среду контрольня.	GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-02; GV.OV-03; GV.SC-01; GV.SC-03; GV.RR-03	AC-1, PM-9; AC-1; AT-1; CA-1; CM-1; IA-1; IR-1; MP-1; PE-1	EDM01; EDM02; EDM03; APO01; APO11

C. Определены роли и обязанности, способствующие достижению целей в области кибербезопасности, и существует процесс периодической оценки знаний, навыков и умений лиц, выполняющих эти роли.	GV.RR-02; GV.RR-04; GV.SC-02; GV.OC-02	PM-13; AT-2; AT-3	EDM02; APO01; APO07
D. Соответствующие заинтересованные стороны привлекаются для обсуждения и принятия мер по устранению существующих уязвимостей и возникающих угроз в среде кибербезопасности. В число заинтересованных сторон входят высшее исполнительное руководство, операционные подразделения, отдел управления рисками, отдел по управлению кадровыми ресурсами, юридический отдел, отдел комплаенс, поставщики и другие.	GV.OC-02; GV.RM-01; GV.RM-05; GV.RM-07; GV.OV-03; GV.SC-03	AC-1; CM-1	EDM05; EDM01.01; EDM03; MEA01.02; APO01; APO08; APO11; APO13; MEA02
Требования к управлению рисками	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
A. Процессы оценки и управления рисками в организации включают выявление, анализ, смягчение последствий и мониторинг угроз в области кибербезопасности и их влияния на достижение стратегических целей.	GV.RM-01; GV.RM-03; GV.OC-01	AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12

B. Управление рисками в области кибербезопасности осуществляется в рамках всей организации и может включать следующие области: информационные технологии, управление рисками организации, управление кадровыми ресурсами, юридические вопросы, комплаенс, операционную деятельность, цепочки поставок, бухгалтерский учет, финансы и другие.	GV.RM-01; GV.RM-05; GV.RR-01; GV.RR-02; GV.OC-03; GV.SC-07	PM-29; AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
C. Установлены подотчетность и ответственность за управление рисками в области кибербезопасности, а также определены лицо или группа лиц, которые будут периодически отслеживать и сообщать о процессе управления рисками в области кибербезопасности, включая информацию о ресурсах, необходимых для снижения рисков и выявления возникающих угроз в области кибербезопасности.	GV.RR-01; GV.RR-02; GV.RR-03; GV.0V-01; GV.OV-02; GV.OV-03	PM-9; PM-29	EDM03; APO01; APO10; APO12
D. Установлен процесс быстрой эскалации информации о любом риске в области кибербезопасности (возникающем или ранее выявленном), который достигает неприемлемого уровня в соответствии с внутренними нормативными документами по управлению рисками или применимыми правовыми и нормативными требованиями. Следует учитывать как финансовые, так и нефинансовые последствия рисков в области кибербезопасности.	GV.RM; ID.RA; RS.MA-04	CA-7; RA-3; RA-7	EDM03; APO01, APO10; APO12

E. Разработан процесс информирования менеджмента и сотрудников о рисках в области кибербезопасности, а также периодического рассмотрения менеджментом проблем, пробелов, недостатков или нарушений контроля, включая предоставление отчетности и устранение недостатков.	PR.AT; GV.RR.01; GV.RR-04; GV.PO	AT-2	APO01; APO02; EDM03; MEA03
F. Организация внедрила процесс реагирования на инциденты в области кибербезопасности и последующего восстановления, который включает обнаружение, локализацию, восстановление и анализ после инцидента. Процесс реагирования на инциденты и последующего восстановления периодически проверяется.	RS; RC	IR-4; IR-5; IR-6; IR-7; IR-8; IR-10; SA-15	DSS02; DSS03; DSS04; DSS05.07
Требования к процессу внутреннего контроля	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
A. Установлен процесс, обеспечивающий наличие средств внутреннего контроля и средств контроля со стороны поставщиков для защиты конфиденциальности, целостности и доступности систем и данных организации. Проводятся периодические оценки с целью определить, функционируют ли средства контроля таким образом, чтобы способствовать достижению целей организации в области кибербезопасности и своевременному решению проблем.	ID.IM-01; ID.IM-02; ID.IM-03; PR; DE; RS; RC; ID.RA06; GV.RM-05; GV.SC; ID.IM-02; RS.MA-01; DE.CM-06	AC-3; AC-4; AC-10; AC-13; AC-17; PM-30; RA-3; SA-9; SR-2	MEA02; MEA04; EDM03; APO09; APO10; DSS01

B. Для работы по кибербезопасности установлен и периодически оценивается процесс управления кадровыми ресурсами, включающий возможности обучения с целью развития и поддержания технических компетенций.	PR.AT-01; PR.AT-02; GV.RR-03	AT-2; AT-3; IR-2; PM-14	APOO7; DSS04
C. Установлен процесс, позволяющий постоянно отслеживать и сообщать о возникающих угрозах и уязвимостях в области кибербезопасности, а также выявлять, приоритизировать и реализовывать возможности для улучшения работы в области кибербезопасности.	ID.RA-02; ID.RA-03, ID.RA-04	CA-7; PM-31; RA-5	DSS03.05
D. Кибербезопасность включена в управление жизненным циклом (выбор, использование, техническое обслуживание и вывод из эксплуатации) всех ИТ-активов, включая аппаратное и программное обеспечение, а также услуги поставщиков.	ID.AM; PR.PS-03; PR.IR; DE.CM-09; ID.AM-08; ID.RA-09; PR.PS-06	AU-9; CM-7; SC-49; SC-51; CM-2; SA-3; SA-10; SA-15; SA-17; SA-20; AU-6; IR-7	DSS05.03; BAI03; BAI09; BAI03; BAI11; DSS05.01; DSS02; DSS03; DSS06.06
E. Установлены процессы для поддержания кибербезопасности, включая , конфигурирование, управление устройствами конечных пользователей, шифрование, внесение исправлений, управление доступом пользователей, а также мониторинг доступности и производительности. Рекомендации по кибербезопасности учитываются при разработке программного обеспечения (методология DevSecOps).	PR.PS-01; PR.PS-06; PR.DS-01; PR.DS-02; PR.PS-05; DE.CM-03	CM-6; SI-2; AC-3; CA-7; SA-4; AC-16; AC-18	BAI10; DSS05; DSS06.03; DSS01.03; MEA01

F. Установлены средства контроля, связанные с работой сети, такие как контроль доступа к сети и ее сегментация; использование и размещение брандмауэров; ограниченные соединения с внешними сетями; виртуальная частная сеть (VPN) / сетевой доступ с нулевым доверием (ZTNA), средства контроля сети интернета вещей (IoT), а также системы обнаружения и предотвращения вторжений (IDS и IPS).	PR.IR; DE.CM-01	AC-6; AC-17; AC-18; AC-20; SC-7; SC-10; CA-8	DSS05.02
G. Установлены средства контроля защиты конечных точек для таких сервисов, как электронная почта, интернет-браузеры, видеоконференции, обмен сообщениями, социальные сети, облачные технологии, а также протоколы совместного использования файлов.	PR.DS-01; PR.DS-02; PR.DS-10; PR.IR	AC-2; AC-16; AU-10; CA-3; SI-8; SI-20; SC-8	BAI10

Приложение C. Дополнительное средство документирования

Ожидается, что внутренние аудиторы будут применять профессиональное суждение на основе оценки рисков при определении применимости требований и надлежащим образом документировать исключение определенных требований. Тематическое требование может документироваться в плане внутреннего аудита или в рабочей документации на основе профессионального суждения аудитора. Одно или несколько заданий внутреннего аудита могут охватывать все требования. Кроме того, не все требования могут быть применимы. Приведенная ниже форма для печати предоставляет один из вариантов документирования соответствия Тематическим требованиям в области кибербезопасности, но ее использование не является обязательным.

Кибербезопасность – руководство организацией

Требование	Выполненный охват или основание для исключения	Ссылка на документацию
A. Разработаны и периодически обновляются стратегия и цели в области кибербезопасности. Совет периодически получает и рассматривает информацию о достижении целей в области кибербезопасности, включая рекомендации в отношении ресурсов и бюджета для поддержки стратегии кибербезопасности.		
B. Политика и процедуры, связанные с кибербезопасностью, разработаны, периодически обновляются и укрепляют среду контроля.		
C. Определены роли и обязанности, способствующие достижению целей в области кибербезопасности, и существует процесс периодической оценки знаний, навыков и умений лиц, выполняющих эти роли.		

Требование	Выполненный охват или основание для исключения	Ссылка на документацию
D. Соответствующие заинтересованные стороны привлекаются для обсуждения и принятия мер по устранению существующих уязвимостей и возникающих угроз в среде кибербезопасности. В число заинтересованных сторон входят высшее исполнительное руководство, операционные подразделения, отдел управления рисками, отдел по управлению кадровыми ресурсами, юридический отдел, отдел комплаенс, поставщики и другие.		

Кибербезопасность - управление рисками

Требование	Выполненный охват или основание для исключения	Ссылка на документацию
A. Процессы оценки и управления рисками в организации включают выявление, анализ, смягчение последствий и мониторинг угроз в области кибербезопасности и их влияния на достижение стратегических целей.		
B. Управление рисками в области кибербезопасности осуществляется в рамках всей организации и может включать следующие области: информационные технологии, управление рисками организации, управление кадровыми ресурсами, юридические вопросы, комплаенс, операционную деятельность, цепочки поставок, бухгалтерский учет, финансы и другие.		

Требование	Выполненный охват или основание для исключения	Ссылка на документацию
C. Установлены подотчетность и ответственность за управление рисками в области кибербезопасности. Определены лицо или группа лиц, которые будут периодически отслеживать и сообщать о процессе управления рисками в области кибербезопасности, включая информацию о ресурсах, необходимых для снижения рисков и выявления возникающих угроз в области кибербезопасности.		
D. Установлен процесс быстрой эскалации информации о любом риске в области кибербезопасности (возникающем или ранее выявленном), который достигает неприемлемого уровня, в соответствии с внутренними нормативными документами по управлению рисками или применимыми правовыми и нормативными требованиями. Следует учитывать финансовые и нефинансовые последствия рисков в области кибербезопасности.		
E. Разработан процесс информирования менеджмента и сотрудников о рисках в области кибербезопасности, а также периодического рассмотрения менеджментом проблем, пробелов, недостатков или нарушений контроля, включая своевременное предоставлением отчетности и устранение недостатков.		

Требование	Выполненный охват или основание для исключения	Ссылка на документацию
F. Организация внедрила процесс реагирования на инциденты в области кибербезопасности и последующего восстановления, который включает обнаружение, локализацию, восстановление и анализ после инцидента. Процесс реагирования на инциденты и последующего восстановления периодически проверяется.		

Кибербезопасность - процессы внутреннего контроля

Требование	Выполненный охват или основание для исключения	Ссылка на документацию
A. Установлен процесс, обеспечивающий наличие средств внутреннего контроля и средств контроля со стороны поставщиков для защиты конфиденциальности, целостности и доступности систем и данных организации. Проводятся периодические оценки с целью определить функционируют ли средства контроля таким образом, чтобы способствовать достижению целей организации в области кибербезопасности и оперативному решению проблем.		
B. Установлен и периодически оценивается процесс управления кадровыми ресурсами, включающий возможности обучения с целью развития и поддержания технических компетенций для работы по кибербезопасности		

Требование	Выполненный охват или основание для исключения	Ссылка на документацию
C. Установлен процесс, позволяющий постоянно отслеживать и сообщать о возникающих угрозах и уязвимостях в области кибербезопасности, а также выявлять, приоритизировать и реализовывать возможности для улучшения работы в области кибербезопасности.		
D. Кибербезопасность включена в управление жизненным циклом (выбор, использование, техническое обслуживание и вывод из эксплуатации) всех ИТ-активов, включая аппаратное и программное обеспечение, а также услуги поставщиков.		
E. Установлены процессы для поддержания кибербезопасности, включая конфигурирование, управление устройствами конечных пользователей, шифрование, внесение исправлений, управление доступом пользователей, а также мониторинг доступности и производительности. Рекомендации по кибербезопасности учитываются при разработке программного обеспечения (методология DevSecOps).		

Требование	Выполненный охват или основание для исключения	Ссылка на документацию
F. Установлены средства контроля, связанные с работой сети, такие как контроль доступа к сети и ее сегментация; использование и размещение брандмауэров; ограниченные соединения с внешними сетями; виртуальная частная сеть (VPN) / сетевой доступ с нулевым доверием (ZTNA), средства контроля сети интернета вещей (IoT), а также системы обнаружения и предотвращения вторжений (IDS и IPS).		
G. Установлены средства контроля защиты конечных точек для таких сервисов, как электронная почта, интернет-браузеры, видеоконференции, обмен сообщениями, социальные сети, облачные технологии, а также протоколы совместного использования файлов.		

О Международном институте внутренних аудиторов

Международный институт внутренних аудиторов (IIA) представляет собой международную профессиональную ассоциацию, обслуживающую более 255 000 членов из различных стран мира и предоставившую более 200 000 сертификатов Certified Internal Auditor® (CIA®) (Дипломированный внутренний й аудитор) по всему миру. Основанный в 1941 году, Международный институт внутренних аудиторов является всемирно признанным лидером в области стандартизации, сертификации, обучения, проведения исследований и разработки технических руководств в области внутреннего аудита. Для получения дальнейшей информации посетите www.theiia.org.

Отказ от ответственности

Авторское право

Февраль 2025 года

The Institute of
Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101