Кибербезопасность

Topical Requirement

Тематические требования

The Institute of
Internal Auditors

Тематические требования в области кибербезопасности

The International Professional Practices Framework® (Международные основы профессиональной практики) включают в себя Global Internal Audit Standards™ (Международные стандарты внутреннего аудита), Тематические требования и Международное руководство. Тематические требования являются обязательными и должны использоваться в сочетании со Стандартами, которые формируют авторитетную основу требуемой практики.

Тематические требования предоставляют четкие руководства для внутренних аудиторов, устанавливая минимальный базовый уровень для аудита определенных областей риска. Профиль рисков организации может потребовать от внутренних аудиторов рассмотрения дополнительных аспектов области риска.

Соответствие Тематическим требованиям повысит согласованность, качество и надежность услуг и результатов внутреннего аудита. В конечном счете, наличие Тематических требований повышает уровень профессии внутреннего аудитора.

Внутренние аудиторы должны применять Тематические требования в соответствии с Международными стандартами внутреннего аудита. Соответствие Тематическим требованиям является обязательным условием для оказания услуг по обеспечению уверенности и рекомендуемым для оказания консультационных услуг.

Тематические требования применимы, если данная область риска является одной из следующих:

A. Предметом аудиторского задания в плане внутреннего аудита.
B. Выявлена во время выполнения аудиторского задания.
C. Предметом запроса на выполнение задания, не включенного в первоначальный план внутреннего аудита.

Необходимо документировать и сохранить доказательства того, что все требования в из Тематических требований были оценены на предмет применимости. Не все требования могут быть применены в каждом аудиторском задании. Если отдельные требования были исключены, необходимо зафиксировать и сохранить соответствующее обоснование. Соответствие Тематическим требованиям является обязательным и будет оцениваться в ходе оценки качества.

Дополнительные сведения см. в Руководстве по применению Тематических требований в области кибербезопасности.

Кибербезопасность

Национальный институт стандартов и технологий (NIST) дает следующее определение кибербезопасности: "Способность защищать или оберегать использование киберпространства от кибератак". 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".

Кибербезопасность снижает риски за счет усиления общей среды контроля и защиты информационных активов организации от неавторизованного доступа, нарушения работы, искажения или уничтожения. Кибератаки могут привести к прямым и косвенным последствиям, часто значительным, поскольку компьютеры, сети, программы, данные и конфиденциальная информация являются важнейшими компонентами большинства организаций.

Оценка процессов руководства организацией, управления рисками и внутреннего контроля в области кибербезопасности

Настоящие Тематические требования обеспечивают последовательный, комплексный подход к оценке разработки и внедрения процессов руководства, управления рисками и внутреннего контроля в области кибербезопасности. Требования определяют минимальный базовый уровень для оценки кибербезопасности в организации.

РУКОВОДСТВО ОРГАНИЗАЦИЕЙ: оценка руководства в области кибербезопасности

Требования:

Внутренние аудиторы должны оценить следующие аспекты руководства организацией в вопросах кибербезопасности:

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 и периодически обновляются для укрепления среды 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.
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.

УПРАВЛЕНИЕ РИСКАМИ: оценка управления рисками в области кибербезопасности

Требования:

Внутренние аудиторы должны оценить следующее в связи с управлением рисками организации в области кибербезопасности:

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.

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 данных 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 предоставление отчетности и устранение недостатков.

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.

СРЕДСТВА ВНУТРЕННЕГО КОНТРОЛЯ: оценка процессов внутреннего контроля в области кибербезопасности

Требования:

Внутренние аудиторы должны оценить следующее в отношении процессов внутреннего контроля организации в области кибербезопасности:

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.

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 усиления 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 (методолгия DevSecOps).

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); 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 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.

Авторское право

The Institute of
Internal Auditors

Штаб-квартира
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, США
Телефон: +1-407-937-1111
Факс: +1-407-937-1101