Кібербезпека

Topical Requirement

Тематична Вимога

The Institute of
Internal Auditors

Тематична Вимога з Кібербезпеки

Тематичні Вимоги є обов'язковим компонентом Основних Положень Міжнародної Професійної Практики (International Professional Practices Framework®) разом з Глобальними Стандартами Внутрішнього Аудиту (Global Internal Audit Standards™) та Глобальними Настановами. Тематичні Вимоги слід використовувати разом з Глобальними Стандартами Внутрішнього Аудиту, які забезпечують авторитетну основу для необхідних практик.

Тематичні Вимоги забезпечують чіткі очікування для внутрішніх аудиторів, встановлюючи мінімальний базовий рівень для аудиту визначених тем ризиків. Профіль ризику організації може вимагати від внутрішніх аудиторів розгляду додаткових аспектів теми.

Відповідність Тематичним Вимогам підвищує послідовність у наданні послуг внутрішнього аудиту та покращує якість і надійність послуг і результатів внутрішнього аудиту. Зрештою, Тематичні Вимоги підвищують рівень професії внутрішнього аудиту.

Внутрішні аудитори повинні застосовувати Тематичні Вимоги відповідно до Глобальних Стандартів Внутрішнього Аудиту. Відповідність Тематичним Вимогам є обов'язковою для послуг з надання впевненості та рекомендованою для консультаційних послуг.

Тематична Вимога застосовується, якщо тема є:

A. Предметом завдання в плані внутрішнього аудиту.
B. Виявленою під час виконання завдання.
C. Предметом запиту на виконання завдання, якого немає в плані внутрішнього аудиту.

Необхідно задокументувати та зберегти докази того, що кожна вимога в Тематичній Вимозі була оцінена на предмет застосовності. Не всі вимоги можуть застосовуватися до кожного завдання; якщо вимоги виключені, обґрунтування мають бути задокументовані та збережені. Відповідність Тематичній Вимозі є обов'язковою і буде оцінюватися під час оцінки якості.

Для отримання додаткової інформації див. Посібник користувача "Тематична Вимога з Кібербезпеки".

Кібербезпека

Національний Інститут Стандартів і Технологій (NIST) визначає кібербезпеку просто: "Здатність обороняти або захищати використання кіберпростору від кібератак". Кібербезпека є частиною загальної інформаційної безпеки, яку NIST визначає як "захист інформації та інформаційних систем від несанкціонованого доступу, використання, розкриття, порушення, модифікації або знищення з метою забезпечення конфіденційності, цілісності та доступності".

Кібербезпека знижує ризики, посилюючи загальне середовище контролю та захищаючи інформаційні активи організації від несанкціонованого доступу, порушення, зміни або знищення. Кібератаки можуть призвести до прямих і непрямих наслідків, які часто є значними, оскільки комп'ютери, мережі, програми, дані та конфіденційна інформація є критично важливими компонентами більшості організацій.

Оцінка процесів управління кібербезпекою, ризик-менеджменту та контролю

Ця Тематична Вимога забезпечує послідовний, комплексний підхід до оцінки дизайну та впровадження процесів управління кібербезпекою, ризик-менеджменту та контролю. Вимоги представляють собою мінімальний базовий рівень для оцінки кібербезпеки в організації.

УПРАВЛІННЯ: Оцінка управління кібербезпекою

Вимоги:

Внутрішні аудитори повинні оцінити наступне стосовно управління кібербезпекою організації:

A. Формалізована стратегія та цілі кібербезпеки розроблені та періодично оновлюються. Оновлена інформація про досягнення цілей кібербезпеки періодично повідомляється та розглядається радою, включаючи ресурси та бюджетні міркування для підтримки стратегії кібербезпеки.

B. Політики та процедури, пов'язані з кібербезпекою, встановлюються та періодично оновлюються для посилення середовища контролю.

C. Визначено ролі та обов'язки, які підтримують цілі кібербезпеки, а також існує процес періодичної оцінки знань, навичок та здібностей осіб, які виконують ці ролі.

D. Відповідні зацікавлені сторони залучаються до обговорення та реагування на існуючі вразливості та нові загрози в середовищі кібербезпеки. До зацікавлених сторін належать вище керівництво, операційні підрозділи, підрозділ ризик-менеджменту, підрозділ управління персоналом, юридичний підрозділ, підрозділ комплаєнс, постачальники та інші.

РИЗИК-МЕНЕДЖМЕНТ: Оцінка управління ризиком кібербезпеки

Вимоги:

Внутрішні аудитори повинні оцінити наступне стосовно управління ризиком кібербезпеки організації:

A. Процеси оцінки та управління ризиками в організації включають виявлення, аналіз, пом'якшення та моніторинг загроз кібербезпеки та їхнього впливу на досягнення стратегічних цілей.

B. Управління ризиком кібербезпеки здійснюється в рамках всієї організації і може охоплювати такі сфери: інформаційні технології, управління ризиками підприємства, управління персоналом, юридичний підрозділ, комплаєнс, операційна діяльність, ланцюжок поставок, бухгалтерський облік, фінанси та інші.

C. Встановлено підзвітність та відповідальність за управління ризиком кібербезпеки. Визначено особу або групу осіб, які періодично контролюють та звітують про те, як здійснюється управління ризиком кібербезпеки, включаючи ресурси, необхідні для зменшення ризиків та виявлення нових загроз кібербезпеки.

D. Встановлено процес швидкої ескалації будь-якого ризику кібербезпеки (нового або раніше виявленого), який досягає неприйнятного рівня відповідно до встановлених в організації керівних принципів управління ризиками або застосовних законодавчих та регуляторних вимог. Слід враховувати фінансові та нефінансові наслідки ризику кібербезпеки.

E. Встановлено процес інформування керівництва та працівників про ризики кібербезпеки, а також періодичного перегляду керівництвом проблем, прогалин, недоліків або збоїв у контролі зі своєчасним звітуванням та виправленням

F. В організації впроваджено процес реагування та відновлення після інцидентів кібербезпеки, який включає виявлення, стримування, відновлення та аналіз після інциденту. Процес реагування та відновлення після інцидентів періодично тестується.

КОНТРОЛЬ: Оцінка процесів контролю кібербезпеки

Вимоги:

Внутрішні аудитори в контексті процесів контролю кібербезпеки в організації повинні оцінити наступне:

A. Встановлено процес, який забезпечує наявність як внутрішніх засобів контролю, так і засобів контролю, що надаються постачальниками, для захисту конфіденційності, цілісності та доступності систем і даних організації. Періодично проводяться оцінки, щоб визначити, чи функціонують засоби контролю таким чином, щоб сприяти досягненню цілей кібербезпеки організації та оперативному вирішенню проблем.

B. Встановлено процес управління талантами, який включає навчання для розвитку та підтримки технічних компетенцій, пов'язаних з операціями кібербезпеки. Процес періодично переглядається.

C. Встановлено процес постійного моніторингу та звітування про нові загрози та вразливості у сфері кібербезпеки, а також виявлення, визначення пріоритетів та реалізації можливостей для покращення операцій кібербезпеки.

D. Кібербезпека включена в управління життєвим циклом (вибір, використання, обслуговування та виведення з експлуатації) всіх IT-активів, включаючи обладнання, програмне забезпечення та послуги постачальників.

E. Встановлено процеси для посилення кібербезпеки, включаючи конфігурацію, адміністрування пристроїв кінцевих користувачів, шифрування, виправлення, управління доступом користувачів, а також моніторинг доступності та продуктивності. Міркування кібербезпеки враховуються при розробці програмного забезпечення (DevSecOps).

F. Встановлено засоби контролю, пов'язані з мережею, такі як контроль доступу до мережі та сегментація; використання та розміщення міжмережевих екранів; обмеження з'єднань від зовнішніх мереж та до них; віртуальна приватна мережа (VPN)/доступ до мережі з нульовою довірою (ZTNA); мережевий контроль Інтернету речей (IoT); та системи виявлення/запобігання вторгненням (IDS та IPS).

G. Засоби контролю безпеки кінцевих точок зв'язку встановлюються для таких сервісів, як електронна пошта, інтернет-браузери, відеоконференції, обмін повідомленнями, соціальні мережі, хмарні сервіси та протоколи обміну файлами.

Про Інститут внутрішніх аудиторів

Інститут внутрішніх аудиторів (The Institute of Internal Auditors, IIA) - це міжнародна професійна асоціація, яка обслуговує понад 255 000 членів з різних країн і видала понад 200 000 сертифікатів Certified Internal Auditor® (CIA®) по всьому світу. Заснований в 1941 році, Глобальний Інститут Внутрішніх Аудиторів визнаний в усьому світі як лідер професії внутрішнього аудиту в галузі стандартів, сертифікації, освіти, досліджень і технічних рекомендацій.
Для отримання додаткової інформації відвідайте сайт: www.theiia.org.

Авторське право

Лютий 2025 року

The Institute of Internal Auditors

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