Кібербезпека

Topical Requirement
Тематична Вимога
Посібник користувача

The Institute of
Internal Auditors

Зміст

Огляд Тематичних Вимог

Тематичні Вимоги є важливим компонентом Основних Положень Міжнародної Професійної Практики (International Professional Practices Framework®), а також Глобальних Стандартів Внутрішнього Аудиту (Global Internal Audit Standards™) та Глобальних Настанов. Інститут Внутрішніх Аудиторів вимагає, щоб Тематичні Вимоги використовувалися разом з Глобальними Стандартами Внутрішнього Аудиту, які є авторитетною основою необхідних практик. Посилання на Стандарти зустрічаються в цьому посібнику як джерело більш детальної інформації.

Тематичні Вимоги формалізують те, як внутрішні аудитори працюють з поширеними сферами ризику, щоб сприяти підвищенню якості та відповідності професії. Тематичні Вимоги встановлюють базовий рівень і надають відповідні критерії для виконання послуг з надання впевненості, пов'язаних з предметом Тематичної Вимоги (Стандарт 13.4 Критерії оцінки). Відповідність Тематичним Вимогам є обов'язковою для послуг з надання впевненості та рекомендується для оцінювання під час надання консультаційних послуг. Тематичні Вимоги не охоплюють усіх потенційних аспектів, які необхідно враховувати при виконанні завдань з надання впевненості; вони, скоріше, мають на меті забезпечити мінімальний набір вимог, який сприяє послідовній та надійній оцінці теми.

Тематичні Вимоги чітко пов'язані з моделлю "трьох ліній" IBA та Глобальними Стандартами Внутрішнього Аудиту. Процеси управління, ризик-менеджменту та контролю є основними компонентами Тематичних Вимог, які відповідають Стандарту 9.1 Розуміння процесів управління, ризик-менеджменту та контролю. Відповідно до моделі "трьох ліній", управління пов'язане з радою/керівним органом, ризик-менеджмент - з другою лінією, а заходи або процеси контролю - з першою лінією. У той час як управлінський персонал представлений як у першій, так і в другій лінії, функція внутрішнього аудиту знаходиться в третій лінії як незалежний та об'єктивний постачальник послуг з надання впевненості, підзвітний раді/керівному органу (Принцип 8 Перебувати під наглядом ради).

Сфери застосування, ризик та професійне судження

Тематичних Вимог слід дотримуватися, коли підрозділи внутрішнього аудиту виконують завдання з надання впевненості з питань, для яких існують Тематичні Вимоги, або коли аспекти Тематичних Вимог виявляються в межах інших завдань з надання впевненості.

Як зазначено в Стандартах, оцінка ризиків є важливою частиною планування керівником внутрішнього аудиту. Визначення завдань з надання впевненості для включення до плану внутрішнього аудиту вимагає оцінки стратегій, цілей та ризиків організації щонайменше раз на рік (Стандарт 9.4 План внутрішнього аудиту). При плануванні окремих завдань з надання впевненості, внутрішні аудитори повинні оцінювати ризики, пов'язані із завданням (Стандарт 13.2 Оцінка ризиків завдання).

Якщо в процесі планування внутрішнього аудиту, заснованого на оцінці ризиків, визначено предмет Тематичної Вимоги та включено його до плану аудиту, то для оцінки цього предмету в межах відповідних завдань необхідно використовувати вимоги, викладені в Тематичній Вимозі. Крім того, коли внутрішні аудитори виконують завдання (як включені, так і не включені до плану) і виявляють елементи Тематичної Вимоги, необхідно оцінити доцільність застосування Тематичної Вимоги в межах цього завдання. Нарешті, якщо запитується завдання, яке спочатку не було включено до плану, але включає в себе цю тему, необхідно оцінити доцільність застосування Тематичної Вимоги.

Професійне судження відіграє ключову роль у застосуванні Тематичної Вимоги. Оцінка ризиків визначає рішення керівника внутрішнього аудиту про включення завдань до плану внутрішнього аудиту (Стандарт 9.4 План внутрішнього аудиту). Крім того, внутрішні аудитори використовують професійне судження для визначення аспектів, які будуть охоплені в межах кожного завдання (Стандарти 13.3 Цілі та обсяг завдання, 13.4 Критерії оцінки та 13.6 Робоча програма). У Додатку А "Приклади практичного застосування" описано, як внутрішні аудитори визначають, чи застосовується Тематична Вимога.

Необхідно зберігати докази того, що кожна вимога в Тематичній Вимозі була оцінена на предмет доцільності застосування, включно з обґрунтуванням, що пояснює виключення будь-яких вимог. Відповідність Тематичним Вимогам повинна бути задокументована з використанням професійного судження аудитора, як описано в Стандарті 14.6 Документування завдання.

Хоча Тематична Вимога з кібербезпеки надає базовий перелік процесів контролю для розгляду, для організацій, які оцінюють кіберризики як дуже високі, може бути необхідною оцінка додаткових аспектів.

Якщо керівник внутрішнього аудиту вирішує, що підрозділ внутрішнього аудиту не має необхідних знань для виконання завдань з аудиту об'єкта, що відповідає Тематичним Вимогам, то завдання може бути передано на аутсорсинг (Стандарти 3.1 Компетентність, 7.2 Кваліфікація керівника внутрішнього аудиту, 10.2 Управління людськими ресурсами). Навіть у цьому випадку аутсорсинг не звільняє службу внутрішнього аудиту від відповідальності за дотримання Тематичних Вимог. Керівник внутрішнього аудиту несе остаточну відповідальність за забезпечення відповідності. Крім того, якщо керівник внутрішнього аудиту визначає, що ресурсів внутрішнього аудиту недостатньо, він повинен проінформувати раду про наслідки недостатності ресурсів і про те, як буде вирішуватися проблема нестачі ресурсів (Стандарт 8.2 Ресурси).

Проведення аудиту, документування та звітність

Застосовуючи Тематичні Вимоги, внутрішні аудитори також повинні дотримуватися Стандартів, виконуючи свою роботу відповідно до Розділу V: Проведення внутрішнього аудиту. Стандарти Розділу V описують планування завдань (Принцип 13 Ефективно планувати завдання), виконання завдань (Принцип 14 Виконувати завдання) та

повідомлення про результати завдань (Принцип 15 Повідомляти про результати завдання та здійснювати моніторинг планів заходів).

Охоплення Тематичної Вимоги може бути задокументоване як у плані внутрішнього аудиту, так і в робочих документах завдань на основі професійного судження аудиторів. Вимоги можуть бути охоплені одним або кількома завданнями з внутрішнього аудиту. Крім того, не всі вимоги можуть застосовуватися. Необхідно зберігати докази того, що Тематична Вимога була оцінена на предмет доцільності застосування, включно з обґрунтуванням, що пояснює будь-які винятки.

Додатковий інструмент у Додатку С можна використовувати як довідник і для документування роботи, яку виконують внутрішні аудитори.

Забезпечення якості

Стандарти вимагають від керівника внутрішнього аудиту розробляти, впроваджувати та підтримувати програму забезпечення та підвищення якості, яка охоплює всі аспекти діяльності функції внутрішнього аудиту (Стандарт 8.3 Якість). Результати повинні бути доведені до відома ради та вищого керівництва. Комунікації повинні містити інформацію про відповідність функції внутрішнього аудиту Стандартам та досягнення цілей діяльності.

Відповідність Тематичним Вимогам буде оцінюватися під час оцінки якості. Для підготовки до перевірки якості внутрішні аудитори можуть використовувати інструмент, наведений у Додатку С.

Кібербезпека

Кібербезпека - це широка тема, пов'язана з більшістю технологічних аспектів діяльності будь-якої організації. Окрім інформаційних технологій, кібербезпека зазвичай є частиною бізнес-процесів, що вимагає від внутрішніх аудиторів оцінювати ризики, пов'язані з кібербезпекою, при плануванні, визначенні обсягу та виконанні завдань з надання впевненості.

Національний Інститут Стандартів і Технологій (NIST), що входить до складу Міністерства Торгівлі США, визначає кібербезпеку просто як "здатність обороняти та захищати використання кіберпростору від кібератак". Тематична Вимога з кібербезпеки фокусується на зовнішньому периметрі, який організації захищають, щоб зменшити ризики від несанкціонованих користувачів та зловмисних кіберзагроз. 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".

Вимоги Тематичної Вимоги з кібербезпеки включають:

- Управління - чітко визначені базові цілі та стратегії кібербезпеки, які підтримують організаційні цілі, політики та процедури.

- Ризик-менеджмент - процеси ідентифікації, оцінки, управління та моніторингу кіберзагроз, включно з процесом негайної ескалації кіберризиків.
- Контроль - встановлені керівництвом процеси контролю, які періодично оцінюються для зменшення кіберризиків.

Міркування

Внутрішні аудитори можуть використовувати наведені нижче міркування для оцінки вимог, зазначених в Тематичній Вимозі з Кібербезпеки. Ці міркування, які містять перехресні посилання на вимоги, є ілюстративними, але не обов'язковими. Внутрішні аудитори повинні покладатися на професійне судження при визначенні того, що включати в свою оцінку.

Міркування щодо управління

Щоб оцінити, як процеси управління застосовуються до цілей кібербезпеки, внутрішні аудитори можуть розглянути:

A. Формалізований, задокументований стратегічний план та цілі з кібербезпеки, включно з доказами того, що правління періодично (як правило, щоквартально) розглядає оновлення з кібербезпеки, надані керівником підрозділу інформаційної безпеки, наприклад, керівником служби інформаційної безпеки (CISO). Докази можуть включати звітність щодо:
    - Моніторингу досягнення стратегічних цілей.
    - Бюджетних потреб для підтримки цілей і завдань кібербезпеки.
    - Зосередження на ризиках і внутрішньому контролі, включно з прогресом у виправленні ситуації.
    - Ключових показників ефективності (KPI) для вимірювання успіху.
    - Людських ресурсів, необхідних для найму, навчання та розвитку персоналу з кібербезпеки.

B. Політики, процедури та інша відповідна документація, що використовується для управління процесами кібербезпеки, включно з:
    - Політиками, які переглядаються та оновлюються щонайменше раз на рік. Нові кіберризики можуть вимагати більш частого перегляду та оновлення.
    - Процесами визначення того, чи є політики та процедури достатніми для підтримки операцій з кібербезпеки.
    - Загальноприйнятими стандартами (NIST, COBIT тощо) для посилення процесів кібербезпеки та внутрішнього контролю.

C. Ролі та обов'язки, що сприяють досягненню цілей кібербезпеки, включно зі структурою, яка гарантує, що функція кібербезпеки підпорядковується рівню в організації, достатньому для забезпечення організаційної підтримки.
    - Процес періодичного оцінювання знань, навичок та вмінь персоналу, який виконує функції з кібербезпеки.

D. Докази взаємодії з відповідними зацікавленими сторонами (наприклад, вищим керівництвом, операційним підрозділом, підрозділом ризик-менеджменту, підрозділом управління персоналом, юридичним підрозділом, підрозділом

комплаєнс, стратегічними постачальниками та іншими), включно з повідомленнями про існуючі та нові кіберризики та відомі потенційні вразливості. Підтвердженнями комунікації можуть бути протоколи зустрічей, звіти або електронні листи.

Міркування щодо ризик-менеджменту

Щоб оцінити, як процеси ризик-менеджменту застосовуються до цілей кібербезпеки, внутрішні аудитори можуть розглянути:

A. Як організація оцінює ризики кібербезпеки та управляє ними, включно з тим, як загрози та вразливості:
   - Первинно виявлено та повідомлено.
   - Аналізуються для оцінки ризику щодо досягнення цілей організації.
   - Пом'якшуються, зокрема планами дій для зниження ризику до прийнятного рівня.
   - Підлягають моніторингу, зокрема з планом постійного звітування до повного усунення загроз.

B. Як організація отримує періодичну інформацію щодо управління ризиком кібербезпеки від функціональних підрозділів, таких як інформаційні технології, управління корпоративними ризиками, підрозділ управління персоналом, юридичний підрозділ, підрозділ комплаєнс, операційний підрозділ, бухгалтерія та фінанси. Для отримання інформації можна використовувати міжфункціональну команду з кібербезпеки або керівний комітет з інформаційних технологій.

C. Як організація закріпила підзвітність та відповідальність за управління ризиком кібербезпеки за окремою особою або командою.
   - Відповідальна особа повинна періодично (щоквартально, щомісячно або за потреби) повідомляти про поточні оновлення ризиків кібербезпеки в організації, а також може включати вимоги до ресурсів, необхідних для стратегій пом'якшення ризиків.

D. Процеси ескалації ризиків кібербезпеки, включно з тим, як оцінюється, застосовується та пріоритезується рівень загрози або ризику. Перегляд може включати ідентифікацію:
   - Визначених організацією рівнів ризику - високого, помірного та низького - з детальним поясненням кожного рівня ризику та процедур ескалації для кожної категорії ризику.
   - Переліку ризиків кібербезпеки, які наразі виявлені, та статус пом'якшення ризиків для кожної події.
   - Застосування правових, регуляторних та комплаєнс вимог.

- Впливу як фінансових, так і нефінансових (наприклад, репутаційних) ризиків.

E. Процес інформування керівництва та працівників про ризики кібербезпеки, який включає:

- Періодичне (щонайменше раз на рік) навчання співробітників з кібербезпеки, наприклад, неоголошені, змодельовані фішингові кампанії для перевірки та відстеження обізнаності організації.
- Інформування щодо усунення існуючих проблем кібербезпеки з очікуваними датами завершення.
- Моніторинг невідповідностей, що включає інформування ради та вищого керівництва.
- Переоцінка загроз, коли в організації змінюється ризик-апетит та толерантність до ризику.

F. Процеси, впроваджені організацією щодо реагування на інциденти та відновлення, які включають:

- Задокументований план, який переглядається та оновлюється в міру того, як діяльність організації змінюється з часом. План повинен включати:
  - Виявлення та звітування про інциденти.
  - Стримування інцидентів для запобігання подальшій шкоді.
  - Заходи реагування з метою відновлення діяльності організації.
  - Аналіз інциденту для винесення уроків та запобіганню подібним подіям у майбутньому.
- Періодичне (щонайменше раз на рік) тестування (практичні вправи) та звітування про результати вищому керівництву та відповідним зацікавленим сторонам. За результатами тестування можуть бути розроблені плани дій.

Міркування щодо процесу контролю

Щоб оцінити, як процеси контролю застосовуються до цілей кібербезпеки, внутрішні аудитори можуть розглянути:

A. Підхід керівництва до побудови ефективного середовища внутрішнього контролю у сфері кібербезпеки, включно з:

- Оцінкою та впровадженням внутрішнього контролю, необхідного як для пом'якшення підвищених ризиків, так і для захисту чутливих, критично важливих, персональних або конфіденційних даних, на основі процесу оцінки ризиків організації.

- Визначенням потреб у ресурсах для підтримки ключових засобів контролю кібербезпеки.
- Розглядом засобів контролю постачальників як частини середовища контролю, що включає перевірку звітів про засоби контролю постачальників (Service Organization Controls, скорочено SOC) перед початком ділових відносин і протягом усього терміну відносин.
- Періодичною перевіркою того, що засоби контролю кібербезпеки функціонують таким чином, щоб зменшити ризики та сприяти досягненню цілей кібербезпеки.
- Процесом усунення недоліків внутрішнього контролю або реагування на спостереження за результатами оцінок, проведених внутрішнім аудитом або іншими постачальниками послуг з надання впевненості (наприклад, тестування на проникнення).

B. Процес управління талантами організації для набору та навчання фахівців з кібербезпеки, включно з тим, як організація визначає можливості для підвищення спроможності фахівців з кібербезпеки підтримувати технічні знання та покращувати обізнаність організації щодо нових проблем.
    - Приклади включають участь у тренінгах, залучення до груп обміну знаннями та безперервну професійну освіту, що включає отримання сертифікатів, пов'язаних з кібербезпекою.

C. Процес виявлення, пріоритезації, моніторингу та звітування керівництва про нові загрози та вразливості кібербезпеки на постійній основі, який зосереджений на щоденних операціях. Огляд може включати впровадження процесів для оцінки загроз та вразливостей, пов'язаних з новими або новітніми технологіями, такими як використання штучного інтелекту.

D. Процеси та засоби контролю, встановлені керівництвом для управління та захисту IT-активів протягом усього життєвого циклу, включаючи вибір, використання, обслуговування та виведення з експлуатації апаратного та програмного забезпечення, а також послуг постачальників. Апаратне забезпечення включає сервери, мережеве обладнання (наприклад, маршрутизатори або міжмережеві екрани), стаціонарні комп'ютери, ноутбуки, мобільні телефони, планшети та периферійні пристрої. Програмне забезпечення включає операційні системи (наприклад, Windows), програмне забезпечення для планування ресурсів підприємства, додатки, антивірусні програми тощо. Апаратне та програмне забезпечення може включати:
    - Використання організацією шифрування, антивірусного програмного забезпечення, управління мобільними пристроями, складних вимог до паролів, віртуальної приватної мережі (VPN)/ мережі з нульовою довірою (ZTN) для автентифікації та періодичного оновлення прошивки.

- Процес управління активами, який гарантує, що апаратне забезпечення компанії має відповідну конфігурацію безпеки під час введення в експлуатацію та належну утилізацію при списанні.
- Контроль, пов'язаний з базами даних, який включає в себе обмеження доступу користувачів і адміністраторів, забезпечення використання шифрування, резервне копіювання і тестування баз даних, а також наявність потужних засобів контролю мережевої безпеки.
- Як загрози та вразливості кібербезпеки враховуються в життєвому циклі розробки системи (System Development Life Cycle, скорочено SDLC).
- Підхід, що використовується підрозділом розробки, безпеки та експлуатації (DevSecOps) для забезпечення врахування в процесі розробки програмного забезпечення кібербезпеки для проактивного виявлення вразливостей.

E. Процеси, що використовуються для посилення кібербезпеки, включно з:
   - Налаштуванням параметрів безпеки для мінімізації ризиків кібербезпеки.
   - Адмініструванням мобільних пристроїв (включаючи використання електронної пошти та додатків), налаштованих таким чином, щоб зменшити ризики кібербезпеки та дистанційно керувати ними, якщо пристрій користувача скомпрометовано.
   - Використанням шифрування для даних "у стані спокою", наприклад, інформації, що зберігається на жорсткому диску, або даних "під час передачі", наприклад, шифрування електронних листів.
   - Забезпеченням оновлень серверів або програмного забезпечення (наприклад, операційної системи) останніми версіями безпеки.
   - Управлінням доступом користувачів, наприклад, використанням багатофакторної автентифікації (MFA) та унікальних ідентифікаторів користувачів зі складними паролями, термін дії яких періодично закінчується.
   - Моніторингом наявних засобів контролю для визначення того, чи належним чином використовуються ресурси, що дозволяє переглядати та аналізувати потенційні проблеми кібербезпеки, які загрожують продуктивності.
   - Інтеграцією кібербезпеки в SDLC для виявлення та усунення вразливостей кібербезпеки до того, як програмне забезпечення буде передано в експлуатацію.

F. Засоби контролю, пов'язані з мережею, які захищають периметр організації, включно з тим, як організація їх використовує:
   - Сегментація мережі.

- Міжмережеві екрани.
- Контроль доступу користувачів.
- Обмеження як на зовнішні, так і на внутрішні з’єднання.
- Засоби контролю, пов'язані з Інтернетом речей (IoT) для взаємопов'язаних мереж.
- Системи виявлення/запобігання вторгненням для запобігання, виявлення та відновлення після атак на кібербезпеку.

G. Засоби контролю безпеки кінцевих точок зв'язку, що застосовуються до таких сервісів, як електронна пошта, інтернет-браузери, відеоконференції, обмін повідомленнями (Zoom, MS Teams та інші), соціальні мережі, хмарні сервіси та протоколи спільного доступу до файлів. Засоби контролю можуть включати обмеження використання певних розширень файлів (наприклад, .exe-файлів) і багатофакторну автентифікацію для спільного доступу до файлів.

Додаток А. Приклади практичного застосування

Наступні приклади описують сценарії, в яких можуть застосовуватися Тематичні Вимоги з Кібербезпеки:

Приклад 1: Завдання з перевірки кібербезпеки включено до плану внутрішнього аудиту.

Коли функція внутрішнього аудиту в процесі планування на основі оцінки ризиків включає одне або декілька завдань з кібербезпеки до плану внутрішнього аудиту, дотримання Тематичних Вимог є обов'язковим при виконанні таких завдань. Відповідність може бути досягнута шляхом включення вимог до одного або декількох завдань в плані внутрішнього аудиту.

Кібербезпека - це широка тема, і не кожна вимога Тематичних Вимог може застосовуватися до кожного завдання. Коли внутрішні аудитори застосовують професійне судження і визначають, що одна або декілька вимог Тематичних Вимог з Кібербезпеки не застосовуються і тому повинні бути виключені із завдання, внутрішні аудитори повинні задокументувати та зберегти обґрунтування для виключення цих вимог. Наприклад, обґрунтуванням для виключення деяких вимог може бути те, що функція внутрішнього аудиту виконує різні завдання з кібербезпеки на ротаційній основі або визначила, що значущість ризику в завданні є низькою.

Приклад 2: Ризики кібербезпеки виявлено під час виконання завдань з аудиту, які не стосуються кібербезпеки.

Внутрішні аудитори можуть виявити ризики кібербезпеки, оцінюючи процес, який безпосередньо не пов'язаний з кібербезпекою. Наприклад, внутрішні аудитори можуть оцінювати процес управління кредиторською заборгованістю в рамках завдання, не пов'язаного з кібербезпекою, і не визначати ризики кібербезпеки як такі, що входять до обсягу перевірки при плануванні завдання. Однак, після проведення первинного вивчення процесу, внутрішні аудитори визначають, що такі ризики повинні бути включені в обсяг завдання; наприклад, вони виявляють ризики кібербезпеки, пов'язані з подачею замовлення на закупівлю через Інтернет (Стандарт 13.2 Оцінка ризиків завдання).

Після виявлення відповідних ризиків внутрішні аудитори повинні переглянути Тематичні Вимоги з Кібербезпеки та визначити, які з них застосовні. У цьому прикладі вони можуть виключити процес управління кібербезпекою або процес управління ризиками кібербезпеки. Вони повинні задокументувати в робочих документах завдання

обґрунтування виключення інших вимог Тематичної Вимоги з Кібербезпеки та зберегти документацію.

Приклад 3: Отримання запиту на виконання позапланового завдання з кібербезпеки.

Зацікавлені сторони, такі як рада, менеджмент або регулятор, можуть подати запит на проведення внутрішніми аудиторами оцінки кібербезпеки поза межами плану аудиту. Наприклад, якщо організація стала об'єктом кібератаки, рада може попросити внутрішній аудит провести оцінку засобів контролю кібербезпеки. Тематична Вимога в такому випадку застосовується, відповідні вимоги повинні бути оцінені, а будь-які винятки задокументовані.

Додаток Б. Зіставлення зі стандартами

Організація може застосовувати власні методики з кібербезпеки, використовуючи стандарти ризик-менеджменту та управління, такі як COBIT або NIST. Внутрішні аудитори, можливо, вже розробили програми аудиту та процедури тестування на основі цих стандартів. Внутрішнім аудиторам слід узгодити заплановане тестування засобів контролю кібербезпеки з Тематичною Вимогою, щоб забезпечити належне покриття. У наведеній нижче таблиці Тематична Вимога з Кібербезпеки зіставлена з трьома загальноприйнятими стандартами: NIST Cybersecurity Framework 2.0, COBIT 2019 та NIST 800-53. Ці стандарти були обрані для порівняння, оскільки вони є доступними і відкритими.

	Посилання на стандарт		
Вимоги до управління	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
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.	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. Політики та процедури, пов'язані з кібербезпекою, встановлюються та періодично оновлюються для посилення середовища контролю.	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. Визначено ролі та обов'язки, які підтримують цілі кібербезпеки, а також існує процес періодичної оцінки знань, навичок та здібностей осіб, які виконують ці ролі.	GV.RR-02; GV.RR-04; GV.SC-02; GV.OC-02	PM-13; AT-2; AT-3	EDM02; APO01; APO07

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.	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
Вимоги до ризик-менеджменту	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
A. Процеси оцінки та управління ризиками в організації включають виявлення, аналіз, пом'якшення та моніторинг загроз кібербезпеки та їхнього впливу на досягнення стратегічних цілей.	GV.RM-01; GV.RM-03; GV.OC-01	AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
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.	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. 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.	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. 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.	GV.RM; ID.RA; RS.MA-04	CA-7; RA-3; RA-7	EDM03; APO01, APO10; APO12
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.	PR.AT; GV.RR.01; GV.RR-04; GV.PO	AT-2	APO01; APO02; EDM03; MEA03
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.	RS; RC	IR-4; IR-5; IR-6; IR-7; IR-8; IR-10; SA-15	DSS02; DSS03; DSS04; DSS05.07
Вимоги до процесів контролю	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
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.	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. Встановлено процес управління талантами, який включає навчання для розвитку та підтримки технічних компетенцій, пов'язаних з операціями кібербезпеки. Процес періодично переглядається.	PR.AT-01; PR.AT-02; GV.RR-03	AT-2; AT-3; IR-2; PM-14	APO07; DSS04
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.	ID.RA-02; ID.RA-03, ID.RA-04	CA-7; PM-31; RA-5	DSS03.05
D. Кібербезпека включена в управління життєвим циклом (вибір, використання, обслуговування та виведення з експлуатації) всіх IT-активів, включаючи обладнання, програмне забезпечення та послуги постачальників.	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. 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).	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. 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).	PR.IR; DE.CM-01	AC-6; AC-17; AC-18; AC-20; SC-7; SC-10; CA-8	DSS05.02
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.	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

Додаток C. Додатковий інструмент документування

Очікується, що внутрішні аудитори будуть використовувати професійне судження при визначенні застосовності вимог на основі оцінки ризиків та належним чином документувати винятки з певних вимог. Тематична Вимога може бути задокументована в плані внутрішнього аудиту або в робочих документах завдань на основі професійного судження аудитора. Ці вимоги можуть охоплювати одне або декілька завдань з внутрішнього аудиту. Крім того, не всі вимоги можуть застосовуватися. Наведена нижче форма для друку надає один з варіантів документування відповідності Тематичній Вимозі з Кібербезпеки, але її використання не є обов'язковим.

Кібербезпека - Управління

Вимоги	Виконане покриття або обґрунтування для виключення	Посилання на документацію
A. Формалізована стратегія та цілі кібербезпеки розроблені та періодично оновлюються. Оновлена інформація про досягнення цілей кібербезпеки періодично повідомляється та розглядається радою, включаючи ресурси та бюджет, 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.		

Вимоги	Виконане покриття або обґрунтування для виключення	Посилання на документацію
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.		

Кібербезпека - Ризик-менеджмент

Вимоги	Виконане покриття або обґрунтування для виключення	Посилання на документацію
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.		

Вимоги	Виконане покриття або обґрунтування для виключення	Посилання на документацію
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.		

Кібербезпека – Процеси контролю

Вимоги	Виконане покриття або обґрунтування для виключення	Посилання на документацію
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 операційною діяльністю 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 операційної діяльності 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.		

Вимоги	Виконане покриття або обґрунтування для виключення	Посилання на документацію
E. Встановлено процеси для посилення кібербезпеки, включаючи конфігурацію, адміністрування пристроїв кінцевих користувачів, шифрування, встановлення виправлень, 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.

Відмова від відповідальності

IIA публікує цей документ з інформаційною та освітньою метою. Цей матеріал не має на меті надати вичерпні відповіді на конкретні індивідуальні обставини і, як такий, може використовуватися лише як орієнтир. IIA рекомендує звертатися за порадою до незалежних експертів, які мають безпосереднє відношення до будь-якої конкретної ситуації. IIA не несе відповідальності за те, що хтось покладається виключно на цей матеріал.

Авторське право

Лютий 2025 року

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