# EY CISO як послуга

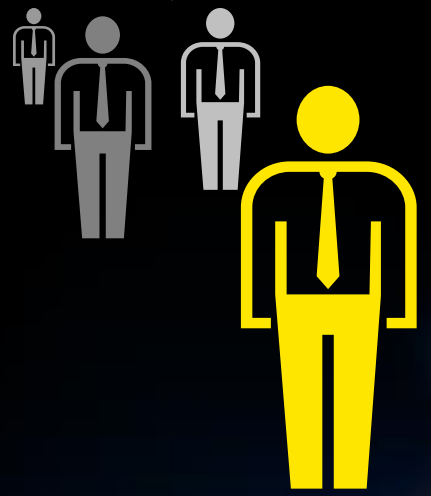
EY Ukraine Digital

The better the question. The better the answer. The better the world works.

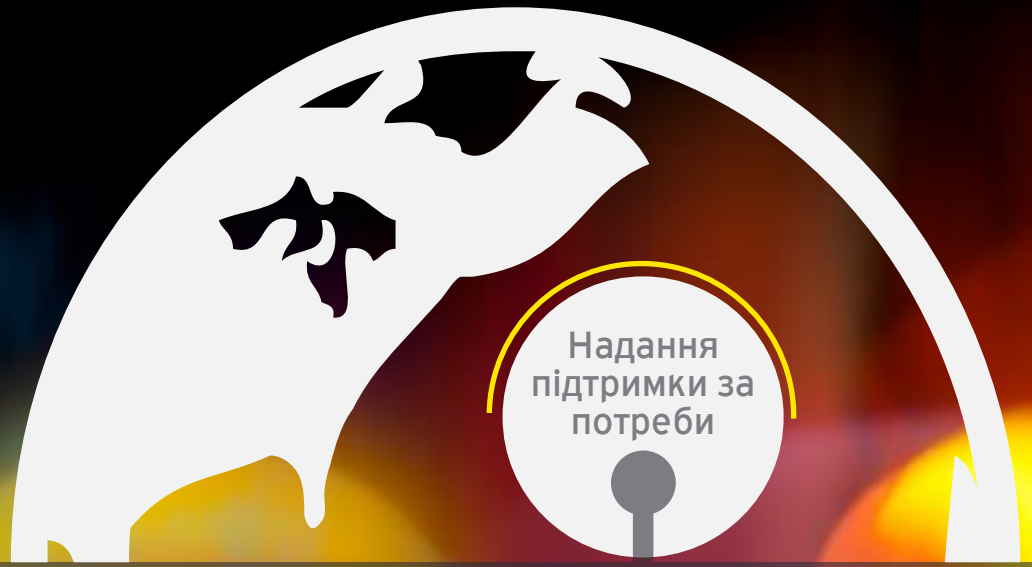
Shape the future with confidence

# Чи є у вас головний керівник, який забезпечує лідерство в сфері кібербезпеки у вашій організації?

## Ми пропонуємо рішення - CISO as a Service – your one-stop-shop in cybersecurity leadership



**Ваш персональний CISO від нас, з підтримкою команди професіоналів**




**Участь у діяльності організації для підвищення рівня безпеки**

### Оцінка

Ваш початковий та поточний стан, існуючі вразливості та недоліки

### Стратегія

Бажаний стан та необхідні кроки для його досягнення в межах запланованого терміну

### Впровадження

Узгоджені організаційні та технічні заходи, включаючи навчання

### Перегляд

Динаміка загроз та достатність заходів для їх подолання

### Реагування

Розробка екстрених планів та підтримка під час серйозних інцидентів кібербезпеки

# Як ваша організація управляє кібербезпекою?

Ринкові тенденції

Кібербезпека залишатиметься постійним викликом, а ризики у 2025 році зберігатимуться – зокрема, через атаки на ресурси та сервіси, що функціонують за допомогою цифрових технологій, включно з фінансовими системами та інфраструктурою зв'язку[1]

Одна єдина атака – чи то витік даних, шкідливе програмне забезпечення, програма вимагач або DDoS-атака – може мати серйозні наслідки. 43% організацій втратили наявних клієнтів через кібератаки[2]

Хоча 48% малих та середніх підприємств вже зазнали кібератак, 43% із них досі не розуміють, які саме заходи безпеки є необхідними[3]

Сьогодні в індустрії кібербезпеки у світі працює близько 5,5 мільйона осіб, проте все ще не вистачає приблизно 5 мільйонів кваліфікованих спеціалістів у цій сфері[4]


***Джерела:***

1. *Global Risks Report 2024 from the World Economic Forum*
2. *Hiscox Cyber Readiness Report 2024*
3. *Cyber security for SMBs: Navigating Complexity and Building Resilience*
4. *2024 ISC2 Cybersecurity Workforce Study*


## Організації й надалі стикаються з серйозними викликами у сфері кібербезпеки

### Безпека та Відповідність

Організації стикаються з труднощами у забезпеченні доступу до конфіденційних даних лише уповноваженим користувачам, що може призводити до витоків інформації.

Виконання вимог регуляторного законодавства (GDPR, HIPAA, PCI DSS) ускладнює ситуацію, адже недотримання стандартів може спричинити значні штрафи та завдати шкоди репутації.

### Операційна Ефективність

Багато організацій стикаються з неефективністю у сфері кібербезпеки, особливо в частині реагування на інциденти та виявлення загроз.

Повільні процеси призводять до затримок у реагуванні на кіберінциденти, що підвищує вразливість до атак.

### Ефективність Витрат

Зростаючі витрати, пов'язані з кіберінцидентами, реагуванням на атаки та порушенням вимог відповідності, є серйозною проблемою.

Організації все частіше усвідомлюють, що інвестування в проактивні заходи кібербезпеки дозволяє зменшити довгострокові витрати, пов'язані з інцидентами та адміністративним навантаженням.

### Досвід Користувача

Пошук балансу між безпекою та зручністю для користувачів є поширеним викликом.

Складні системи доступу та громіздкі протоколи безпеки викликають роздратування у співробітників, що призводить до недотримання політик безпеки та збільшує ризики, оскільки працівники шукають обхідні шляхи.

У сучасному динамічному цифровому середовищі **ефективні заходи кібербезпеки є необхідними для управління ризиками та підвищення операційної ефективності**. Однак постійна еволюція кіберзагроз робить організації все більш вразливими до порушень і збоїв, що підкреслює критичну потребу в сильному лідерстві у сфері кібербезпеки для протидії цим викликам.

## CISO as a Service ключові кваліфікаційні питання

Чи дозволяють ваші наявні можливості ефективно керувати ризиками та витратами, пов'язаними з кібербезпекою?

1. Чи визначили ви, яку саме інформацію необхідно захищати?
2. Чи ідентифікували ви потенційні загрози та рівень впливу на вашу організацію?
3. Чи проводили ви оцінку ризиків та визначали заходи реагування?
4. Чи здатний ваш поточний персонал впровадити всі визначені заходи захисту?
5. Чи маєте ви встановлені процедури та технічні можливості для виявлення й реагування на інциденти?

# CISO як послуга – спеціалізований лідер кібербезпеки

## Огляд послуги

- CISO as a Service - це рішення з кібербезпеки на основі підписки, яке надає організаціям підтримку за потреби від досвідченого менеджера з кібербезпеки EY та команди експертів, що забезпечують індивідуальні стратегії кібербезпеки
- Ця послуга дозволяє бізнесу ефективно управляти ризиками кібербезпеки, дотримуватися регуляторних вимог та адаптуватися до змін ландшафту загроз - без фінансового навантаження, пов'язаного з наймом постійного CISO
- Використовуючи експертизу та ресурси EY, ви отримуєте комплексну позицію в сфері кібербезпеки, яка відповідає вашим конкретним потребам та стандартам

## Ключові функції

- **Експертиза за потреби:** Доступ до вашого надійного менеджера з кібербезпеки EY та команди професіоналів, коли вам це потрібно
- **Індивідуальна стратегія:** Розробка персоналізованих планів кібербезпеки, які відповідають вашим бізнес-цілям та вимогам галузі
- **Безперервний моніторинг:** Постійна оцінка та звітування щодо стану кібербезпеки з метою виявлення та мінімізації ризиків
- **Підтримка дотримання регуляторних вимог:** Консультації щодо дотримання галузевих стандартів та нормативних вимог для захисту організації.
- **Планування реагування на інциденти:** Підготовка та підтримка швидкого та ефективного реагування на інциденти кібербезпеки

## Переваги

- **Економічність:** Уникайте високих витрат, пов'язаних з наймом постійного CISO, отримуючи при цьому експертні консультації
- **Масштабовані рішення:** Легко коригуйте рівень обслуговування відповідно до змін потреб вашої організації
- **Посилення кіберзахисту:** Покращуйте загальну готовність та стійкість вашої організації до кіберзагроз
- **Спокій за безпеку:** Зосередьтеся на основному бізнесі, знаючи, що ваша кібербезпека – в надійних руках фахівців

## Підхід до реалізації

### 1 Оцінка

- Провести всебічну оцінку поточного стану кібербезпеки організації
- Виявити вразливості, ризики та прогалини у відповідності до вимог

### 2 Стратегія

- Співпрацювати з зацікавленими сторонами для створення індивідуальної стратегії кібербезпеки
- Визначити ключові цілі, завдання, пріоритети та терміни

### 3 Впровадження

- Підтримувати впровадження необхідних заходів і технологій для моніторингу та захисту
- Надати навчання та ресурси команді клієнта для ефективного виконання

### 4 Перегляд

- Регулярно оцінювати середовище кібербезпеки та оновлювати стратегію за потреби
- Генерувати звіти щодо стану безпеки, інцидентів та рівня відповідності до вимог

### 5 Реагування

- Встановити чіткий план реагування на інциденти та проводити симуляції
- Забезпечити методологічну підтримку під час реальних інцидентів для мінімізації впливу

## Ключові показники ефективності

- **Час реагування на інциденти:** Середній час, витрачений на реагування та вирішення інцидентів
- **Рівень дотримання:** Відсоток дотримання відповідних регуляцій та стандартів
- **Виконання стратегій:** Відсоток впроваджених заходів кібербезпеки в межах запланованого терміну
- **Покращення захисту:** Зменшення кількості виявлених вразливостей з часом

## Передумови послуги

- **Співпраця з клієнтом:** Успішна реалізація залежить від активної участі та комунікації з боку команди клієнта
- **Розподіл ресурсів:** Наявність бюджету та людських ресурсів з боку клієнта для підтримки впровадження рекомендованих заходів
- **Доступ до даних:** Наявність відповідних даних та журналів з систем клієнта для оцінки вразливостей та моніторингу стану кібербезпеки

# Ключові варіанти надання послуг

## Базовий – до 40 годин/місяць

- **Доступ до CISO:** Оперативний доступ до вашого надійного та досвідченого менеджера з кібербезпеки EY та його команди для постійної підтримки
- **Стратегічне планування:** Розробка індивідуальної стратегії кібербезпеки, що відповідає вашим бізнес-цілям
- **Операційна підтримка:** Надання рекомендацій щодо організації процесів безпеки та шаблонів політик безпеки
- **Консультації з питань відповідності:** Підтримка у розумінні й дотриманні відповідних регуляторних вимог (наприклад, GDPR,HIPAA).
- **Квартальні зустрічі:** Регулярні зустрічі для оцінки прогресу, коригування стратегій та планів дій

**Підходить для:** Малих та середніх підприємств, які шукають базове керівництво в сфері кібербезпеки та підтримку дотримання вимог.

## Стандартний – до 80 годин/місяць

- **Усі функції базового варіанту:** Містить все, що є у Базовому варіанті
- **Безперервний моніторинг:** Постійний аналіз кібербезпекового середовища для виявлення недоліків у контролях та вразливостей
- **Планування реагування на інциденти:** Розробка індивідуального плану реагування на інциденти для забезпечення оперативних та скоординованих дій
- **Контроль навчання співробітників:** Створення та регулярний перегляд графіку навчань персоналу щодо кращих практик кібербезпеки та підвищення обізнаності
- **Щомісячні безпекові звіти:** Детальні звіти щодо стану кібербезпеки, інциденти та відповідності нормативним вимогам

**Підходить для:** Організацій, які потребують проактивного моніторингу та структуровані можливості реагування на інциденти.

## Розширений – 160+ годин/місяць

- **Усі функції стандартного варіанту:** Включає все, що є в Стандартному варіанті
- **Виконання операційних процесів:** Безперервне виконання ключових процесів кібербезпеки
- **Підтримка під час кризових ситуацій:** Оперативна допомога у разі серйозних інцидентів безпеки, включно зі стратегіями комунікації та взаємодією зі стейкхолдерами
- **Щорічний огляд безпеки:** Комплексна оцінка практик кібербезпеки та відповідності вимогам, із наданням практичних рекомендацій для покращення

**Підходить для:** Великих підприємств або організацій з високими вимогами до безпеки, які потребують надійного, постійного керівництва і підтримки в сфері кібербезпеки.

Розділ 2

# Внутрішня інформація про послугу

# Детальний підхід до послуги

## 1 Оцінка

- Опитати ключових стейкхолдерів, щоб зрозуміти поточні процеси, виклики та культуру безпеки.
- Виконати зіставлення регуляторних вимог із чинними процедурами для виявлення невідповідностей.
- Провести аналіз на відповідність галузевим фреймворкам (наприклад, NIST, ISO 27001).
- Перевірити налаштування безпеки критично важливих елементів інформаційної інфраструктури з метою виявлення вразливостей.
- Проаналізувати наявні інструменти безпеки для виявлення функціональних або технологічних прогалин.
- Провести загальну оцінку ризиків, пов'язаних з виявленими вразливостями та слабкими місцями
- Розробити комплексний звіт із узагальненням виявлених проблем, включаючи пріоритетні рекомендації щодо їх усунення.

## 2 Стратегія

- Проводити воркшопи із зацікавленими сторонами для збору відгуків та узгодження цілей безпеки.
- Провести SWOT-аналіз (Сильні та Слабкі сторони, Можливості, Загрози) для визначення напрямків трансформації
- Розробити цільовий стан кібербезпеки та надати рекомендації для його досягнення.
- Встановити систему управління проектами для визначення завдань, часових рамок та відповідальних сторін.
- Використовувати діаграми Ганта або дошки Канбан для візуалізації часових рамок проекту та прогресу.
- Встановити вимірювані KPI для відстеження ефективності стратегії кібербезпеки з часом.

## 3 Впровадження

- Співпрацювати з постачальниками щодо закупівлі, встановлення та налаштування інструментів кібербезпеки.
- Розробити плани інтеграції для забезпечення безперебійної роботи нових інструментів з існуючими системами.
- Розробити процеси та супутню документацію та підтримку щодо впровадження в операційну діяльність.
- Створити навчальну програму, адаптовану до специфічних інструментів та процесів організації.
- Розробити підхід для впровадження бази знань або інтранет-сайту з ресурсами, часто задаваними питаннями та найкращими практиками

## 4 Перегляд

- Планувати періодичні оцінки безпеки (наприклад, щоквартальний або щомісячний огляд стратегії, оцінка вразливостей) для оцінки ефективності заходів безпеки.
- Використовувати канали розвідки загроз для отримання інформації про нові загрози та вразливості.
- Визначити ключові показники для оцінки ефективності поточних операцій (наприклад, час реагування на інциденти, рівень відповідності вимогам).
- Проводити регулярні опитування для збору відгуків від зацікавлених сторін щодо ефективності заходів кібербезпеки.
- Розповсюджувати звіти серед зацікавлених сторін, висвітлюючи ключові показники, інциденти та сфери для покращення.
- Оновлювати стратегію кібербезпеки відповідно до змін у ландшафті загроз, вимог до відповідності та організаційних цілей.

## 5 Реагування

- Збирати та аналізувати історію інцидентів та ефективність реагування.
- Розробити детальний план реагування на інциденти з визначенням ролей, відповідальності та процедур.
- Використовувати настільні вправи та симуляції для тестування ефективності плану реагування на інциденти та виявлення сфер для покращення.
- Розробити протоколи зв'язку для забезпечення своєчасних оновлень під час інцидентів.
- Використовувати встановлені протоколи для керування процесом реагування, забезпечуючи ефективний зв'язок та координацію.
- Проводити огляди після інцидентів для аналізу ефективності реагування та виявлення отриманих уроків

# Бізнес-модель канва lean

## Проблема

Багато організацій не мають досвіду для ефективного управління ризиками кібербезпеки

Малі та середні підприємства (МСП) не можуть дозволити собі постійного головного директора з інформаційної безпеки (CISO)

Кіберзагрози, що швидко розвиваються, потребують постійного моніторингу та адаптації стратегії

### Існуючі альтернативи

Штатний CISO

Постачальники керованих послуг безпеки (MSSPs)

Традиційні консалтингові послуги

## Рішення

Доступ на вимогу до досвідчених фахівців з кібербезпеки

Розробка та впровадження індивідуальної стратегії кібербезпеки

Безперервний моніторинг та звітність щодо стану кібербезпеки та відповідності

## Ключові показники

Кількість залучених та утриманих клієнтів

Задоволеність клієнтів та індекс лояльності клієнтів (NPS)

Зменшення кількості інцидентів кібербезпеки у клієнтів

Зростання доходів від пропозицій CISO як послуги

## Унікальна ціннісна пропозиція

EY пропонує експертне лідерство в кібербезпеці та операційну підтримку, адаптовані до специфічних потреб організацій, забезпечуючи надійний захист від загроз, що розвиваються, без накладних витрат на штатного CISO

### Концепція високого рівня

Віртуальний CISO для всіх

Експертиза з кібербезпеки на вимогу

Легка допомога з кібербезпеки, коли вона потрібна

Універсальний магазин кібербезпеки

## Конкурентна перевага

Визнана репутація та довіра EY в індустрії

Доступ до великої мережі експертів з кібербезпеки та ресурсів

Всебічне розуміння регуляторних вимог та стандартів відповідності

## Канали

Прямі продажі через існуючі клієнтські відносини EYЦифрові маркетингові кампанії, орієнтовані на SME та великі підприємстваПартнерство з постачальниками технологій та галузевими асоціаціями

## Сегменти клієнтів

Малі та середні підприємства (SME) різних галузей

Великі підприємства, які шукають додаткове лідерство в кібербезпеці

Організації, що проходять цифрову трансформацію або міграцію в хмару

Регульовані галузі - бізнеси у таких секторах, як фінанси, охорона здоров'я та енергетика

### Ранні користувачі

Існуючі клієнти без функції кібербезпеки

Стартапи у сфері технологій та фінтеху

Шведські SME (клієнти Павла)

## Структура витрат

Заробітні плати та пільги для фахівців EY з кібербезпеки

Витрати на маркетинг та продажі

Технології та інструменти для моніторингу та звітності

Навчання та розвиток персоналу (наприклад, сертифікації)

## Потоки доходів

Модель ціноутворення на основі підписки для постійних послуг CISO

Одноразові платежі за конкретні проекти або оцінки

Консалтингові гонорари за додаткові послуги кібербезпеки (наприклад, навчання, відповідність ISO)

# Портрет клієнта (Малі та середні підприємства)

## Посади

- Власники бізнесу
- IT-менеджери
- Операційні менеджери
- Офіцери з питань відповідності
- Головні фінансові директори (CFO)
- Менеджери з маркетингу
- Менеджери з управління персоналом

## Демографічні дані

- Вік: 30-55 років
- Місцезнаходження: Великі міста, такі як Київ, Львів, Одеса та Дніпро, а також регіональні центри
- Освіта: Ступінь бакалавра або вища, часто в галузі бізнесу, IT або суміжних сферах
- Рівень доходу: Від 20 000 до 100 000 грн на місяць

## Інтереси

- Кібербезпека та інформаційна безпека
- Розвиток бізнесу та стратегії зростання
- Управління ризиками та відповідність
- Технологічні рішення та інновації
- Нетворкінг з іншими власниками бізнесу та професіоналами
- Участь у громадських справах та місцевих бізнес-заходах
- Онлайн-навчання та професійний розвиток
- Цифровий маркетинг та стратегії соціальних мереж
- Фінансове управління та техніки зниження витрат

## Больові точки

- Обмежений бюджет для ресурсів кібербезпеки
- Відсутність внутрішньої експертизи для ефективного управління ризиками кібербезпеки
- Складність у відстеженні вимог регулятивної відповідності, особливо з урахуванням недавніх змін
- Занепокоєння щодо потенційного впливу кібер-інцидентів на діяльність та репутацію бізнесу
- Обмеженість у часі при управлінні кібербезпекою поряд з іншими бізнес-обов'язками
- Страх втратити довіру клієнтів через витоки даних
- Складність у розумінні складного жаргону та рішень кібербезпеки
- Виклики у навчанні співробітників обізнаності з кібербезпеки

## Поведінка

- Активно шукають інформацію про рішення кібербезпеки та найкращі практики
- Взаємодіють з контентом, пов'язаним з розвитком бізнесу, технологіями та управлінням ризиками
- Беруть участь у місцевих бізнес-мережах та онлайн-форумах
- Імовірно відвідують воркшопи та семінари з кібербезпеки та управління бізнесом
- Регулярно використовують платформи соціальних мереж (наприклад, Facebook, LinkedIn) для бізнес-нетворкінгу та обміну інформацією
- Схильні слідувати за галузевими впливовими особами та лідерами думок у соціальних мережах
- Беруть участь в онлайн-курсах або вебінарах для покращення знань
- Читають галузеві публікації та блоги, щоб бути в курсі тенденцій

# Портрет клієнта (Великі підприємства)

## Посади

Головні директори з інформаційної безпеки (CISO)

IT-директори

Менеджери з питань відповідності

Керівники з управління ризиками

Головні технічні директори (CTO)

Аналітики безпеки

## Демографічні дані

Вік: 35-60 років

Місцезнаходження: Великі міста зі значною корпоративною присутністю

Освіта: Ступінь магістра в галузі IT, кібербезпеки, бізнес-адміністрування або суміжних сферах

Рівень доходу: Від 50 000 до 200 000 грн на місяць

## Інтереси

Передові рішення та технології кібербезпеки

Регулятивна відповідність та управління ризиками

Галузеві тенденції та найкращі практики в кібербезпеці

Нетворкінг з іншими керівниками та галузевими лідерами

Участь у конференціях та семінарах з кібербезпеки

Дослідження нових технологій та інновацій у сфері безпеки

Розвиток лідерства та коучинг для керівників

Стратегічне планування та забезпечення безперервності бізнесу

Аналітика даних та бізнес-аналітика

## Больові точки

Складні організаційні структури, що призводять до фрагментованих практик кібербезпеки

Високі ставки для відповідності галузевим регуляціям та потенційні штрафи

Потреба в додатковому лідерстві з кібербезпеки для підтримки існуючих команд

Необхідність постійно бути на крок попереду кібер-загроз та нових вразливостей

Виклики розподілу ресурсів для підтримки комплексних заходів безпеки

Складність інтеграції нових технологій безпеки з існуючими системами

Занепокоєння щодо ефективності поточних заходів безпеки

Виклики у донесенні потреб кібербезпеки до вищого керівництва

## Поведінка

Регулярно проводять оцінки безпеки та аудити

Взаємодіють з контентом лідерів думок та галузевими звітами

Відвідують нетворкінг-події та конференції виконавчого рівня

Співпрацюють з міжфункціональними командами для покращення стану безпеки

Використовують професійні мережеві платформи (наприклад, LinkedIn) для отримання галузевих інсайтів

Беруть участь у круглих столах та аналітичних центрах з кібербезпеки

Слідкують за галузевими новинами та оновленнями, щоб бути в курсі подій

Займаються безперервним професійним розвитком через сертифікації та навчання

# Портрет клієнта (Організації цифрової трансформації)

## Посади

Офіцери цифрової трансформаціїIT-менеджери проектів

Головні технічні директори

Менеджери з інновацій

Бізнес-аналітики

Спеціалісти з управління змінамиАналітики даних

## Демографічні дані

Вік: 30-50 років

Місцезнаходження: Регіони з сильним фокусом на технології та інновації (наприклад, Київ, Львів, Одеса)

Освіта: Ступінь бакалавра або магістра в IT, бізнесі або суміжних сферах; багато мають сертифікації з управління проектами або цифрової трансформації.

Рівень доходу: Від 40 000 до 150 000 грн на місяць

## Інтереси

Стратегії цифрової трансформації та інновацій

Хмарні обчислення та SaaS-рішення

Найкращі практики кібербезпеки

Гнучке управління проектами

Нетворкінг з професіоналами технологій та інновацій

Безперервне навчання та професійний розвиток

Користувацький досвід (UX) та мапування шляху клієнта

Конфіденційність даних та відповідність

Нові технології (AI, IoT, блокчейн)

## Больові точки

Підвищена схильність до кібер-загроз під час переходу на цифрові платформи

Потреба в оновлених стратегіях безпеки для захисту нових цифрових активів

Балансування швидкості інновацій з потребою в безпеці та відповідності

Занепокоєння щодо впливу порушень безпеки на цифрові ініціативи та довіру клієнтів

Опір змінам всередині організації щодо нових технологій

Складність узгодження цілей IT та бізнесу під час трансформації

Виклики в управлінні очікуваннями зацікавлених сторін та комунікації

Обмежені ресурси для впровадження комплексних заходів безпеки

## Поведінка

Активно шукають експертні поради щодо інтеграції кібербезпеки в ініціативи цифрової трансформації

Взаємодіють з контентом, пов'язаним з цифровими інноваціями та кібербезпекою

Беруть участь у воркшопах та вебінарах, зосереджених на технологічних трендах

Використовують онлайн-платформи для співпраці та обміну знаннями

Експериментують з новими технологіями та методологіями у своїх проектах

Слідкують за галузевими тенденціями та оновленнями через розсилки та блоги

Беруть участь у пілотних проектах для тестування нових рішень перед повним впровадженням

Налагоджують мережі з колегами для обміну досвідом та найкращими практиками

# Портрет клієнта (Регульовані галузі)

## Посади

Офіцери з питань відповідності

Менеджз управління ризикамиери

Офіцери з захисту даних

IT-менеджери безпеки

Головні директори з питань відповідності (CCO)

Юридичні радники

Внутрішні аудитори

## Демографічні дані

Вік: 35-60 років

Місцезнаходження: Великі міста зі значною корпоративною присутністю

Освіта: Вищі ступені в галузі права, відповідності, кібербезпеки або суміжних сферах; багато мають відповідні сертифікації (наприклад, CISA, CRISC).

Рівень доходу: Від 50 000 до 200 000 грн на місяць

## Інтереси

Регулятивна відповідність та захист даних

Оцінка та управління ризиками

Технології та рішення кібербезпеки

Нетворкінг з професіоналами з питань відповідності та регулювання

Участь у галузевих регулятивних органах та асоціаціях

Отримання оновлень щодо регулятивних змін та найкращих практик

Правові та етичні аспекти кібербезпеки

Антикризове управління та планування реагування на інциденти

Управління даними та інформаційний менеджмент

## Больові точки

Навігація в складних регулятивних рамках та стандартах відповідності

Захист чутливих даних та підтримка довіри клієнтів

Високі ставки для відповідності, що призводять до потенційних штрафів та репутаційних збитків

Потреба в надійних заходах кібербезпеки для відповідності регулятивним вимогам

Тиск щодо впровадження рішень безпеки, які узгоджуються з вимогами відповідності

Складність донесення потреб відповідності до технічних команд

Виклики у відстеженні швидких змін у регуляціях та технологіях

Обмеження ресурсів для підтримки заходів відповідності та безпеки

## Поведінка

Регулярно проводять аудити та оцінки відповідності

Взаємодіють з контентом, пов'язаним з регулятивними змінами та найкращими практиками

Відвідують галузеві конференції та семінари, присвячені відповідності та кібербезпеці

Співпрацюють з юридичними командами та командами відповідності для забезпечення узгодженості заходів безпеки

Використовують професійні мережі для обміну інсайтами та стратегіями щодо викликів відповідності

Беруть участь у навчальних сесіях, щоб бути в курсі регулятивних вимог

Слідкують за галузевими новинами та оновленнями через спеціалізовані публікації та веб-сайти

Беруть участь у дискусіях на форумах з відповідності та онлайн-спільнотах

**EY** | Building a better working world

Дотримуючись своєї місії — удосконалюючи бізнес, змінювати світ на краще, — компанія EY сприяє створенню довгострокового корисного ефекту для клієнтів, співробітників і суспільства в цілому, а також допомагає зміцнювати довіру до ринків капіталу.

Використовуючи дані, ШІ та технології, команди EY допомагають клієнтам впевнено будувати майбутнє та знаходити відповіді на найактуальніші питання сьогодення та майбутнього.

Фахівці компанії EY працюють в галузях аудиту, консалтингу, оподаткування, стратегії і транзакцій. Завдяки галузевим інсайтам, глобально пов'язаній багатопрофільній мережі та екосистемам партнерів, команди EY надають послуги у більше ніж 150 країнах світу.

Все для того, щоб визначати майбутнє впевнено.



ED MMYY



ey.com/ua