

Міністерство освіти і науки України  
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії

(повна назва факультету)

Кафедра кібербезпеки

(повна назва кафедри)

## КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр

(назва освітнього ступеня)

на тему: Дослідження застосування генеративного штучного інтелекту  
для аналізу вимог інформаційної безпеки

Виконав(ла): студент(ка) VI курсу, групи СБм-61  
спеціальності 125 Кібербезпека

(шифр і назва спеціальності)

Сміх О.М.  
(прізвище та ініціали)

(підпис)

Керівник

Козак Р.О.  
(прізвище та ініціали)

(підпис)

Нормоконтроль

Лечаченко Т.А.  
(прізвище та ініціали)

(підпис)

Завідувач кафедри

Загородна Н.В.  
(прізвище та ініціали)

(підпис)

Рецензент

(прізвище та ініціали)

(підпис)

м. Тернопіль  
2023

Міністерство освіти і науки України  
Тернопільський національний технічний університет імені Івана Пулюя

Факультет Комп'ютерно-інформаційних систем і програмної інженерії  
(повна назва факультету)

Кафедра Кібербезпеки  
(повна назва кафедри)

ЗАТВЕРДЖУЮ

Завідувач кафедри

Загородна Н.В.

(підпис)

(прізвище та ініціали)

« »

2023 р.

## ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр  
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека  
(шифр і назва спеціальності)

студенту Сміх Олені Миколаївній  
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження застосування генеративного штучного інтелекту  
для аналізу вимог інформаційної безпеки

Керівник роботи Козак Руслан Орестович, к.т.н., доцент  
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 16 » листопада 2023 року № 4/7-1061

2. Термін подання студентом завершеної роботи \_\_\_\_\_

3. Вихідні дані до роботи Дослідження застосування генеративного штучного інтелекту для  
аналізу вимог інформаційної безпеки

4. Зміст роботи (перелік питань, які потрібно розробити)

Вступ, 1 Теоретично-аналітична частина, 1.1 Сучасні тенденції та проблеми аналізу вимог  
інформаційної безпеки, 1.2 Огляд технології генеративного штучного інтелекту (ГШІ), 1.3 Огляд  
застосування генеративного штучного інтелекту в галузі інформаційної безпеки, 1.4 Недоліки  
та можливі ризики використання генеративних платформ, 2 Практична частина, 2.1 Вибір  
моделей генеративного штучного інтелекту, 2.2 Визначення ролей та розробка запитань,  
2.3 Розробка критеріїв оцінювання, 2.4 Проведення дослідження та аналіз результатів  
використання генеративних моделей ШІ з метою аналізу вимог інформаційної безпеки,  
3 Охорона праці та безпека в надзвичайних ситуаціях, 3.1 Охорона праці, 3.2 Безпека в  
надзвичайних ситуаціях, Висновки, Перелік використаних джерел

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

---

---

---

---

---

---

---

---

---

---

## 6. Консультанти розділів роботи

| Розділ                           | Прізвище, ініціали та посада консультанта | Підпис, дата   |                  |
|----------------------------------|---|----------------|------------------|
|                                  |   | завдання видав | завдання прийняв |
| Охорона праці                    | Осухівська Г.М., к.т.н., доцент           |                |                  |
| Безпека в надзвичайних ситуаціях | Стручок В.С., старший викладач            |                |                  |

7. Дата видачі завдання \_\_\_\_\_

**КАЛЕНДАРНИЙ ПЛАН**

| № з/п | Назва етапів роботи  | Термін виконання етапів роботи | Примітка |
|-------|--|--------------------------------|----------|
| 1.    | Ознайомлення із завдання кваліфікаційної роботи  |                                |          |
| 2.    | Підбір та аналіз наукових джерел про генеративний штучний інтелект та процес аналізу вимог інформаційної безпеки |                                |          |
| 3.    | Аналіз та вибір моделей генеративного штучного інтелекту   |                                |          |
| 4.    | Розробка запитань для генеративних моделей штучного інтелекту  |                                |          |
| 5.    | Розробка критеріїв та шкали для оцінювання результатів   |                                |          |
| 6.    | Проведення експерименту  |                                |          |
| 7.    | Проведення експертної оцінки результатів роботи моделей штучного інтелекту                                       |                                |          |
| 9.    | Аналіз результатів оцінювання моделей генеративного штучного інтелекту   |                                |          |
| 10.   | Виконання завдання до розділу «Охорона праці та безпека в надзвичайних ситуаціях»                                |                                |          |
| 11.   | Оформлення кваліфікаційної роботи  |                                |          |
| 12.   | Нормоконтроль  |                                |          |
| 13.   | Перевірка на плагіат   |                                |          |
| 14.   | Попередній захист кваліфікаційної роботи   |                                |          |
| 15.   | Захист кваліфікаційної роботи  |                                |          |

Студент

\_\_\_\_\_ (підпис)

\_\_\_\_\_ (прізвище та ініціали)

Керівник роботи

\_\_\_\_\_ (підпис)

\_\_\_\_\_ (прізвище та ініціали)

## АНОТАЦІЯ

Дослідження застосування генеративного штучного інтелекту для аналізу вимог інформаційної безпеки // Кваліфікаційна робота освітнього рівня «Магістр» // Сміх Олена Миколаївна // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2023 // С. 191, рис. – 2, табл. – 11, додат. – 2, бібліогр. – 30.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, ПОЛІТИКИ БЕЗПЕКИ, ШТУЧНИЙ ІНТЕЛЕКТ, ГЕНЕРАТИВНІ МОДЕЛІ, ISO 27001, АНАЛІЗ ВИМОГ.

У кваліфікаційній роботі розглядається технологія генеративного штучного інтелекту та її застосування для аналізу вимог інформаційної безпеки. Дослідження зосереджене на трьох моделях генеративного штучного інтелекту, які були відібрані шляхом аналізу. Адаптовано відомі підходи щодо тестування та оцінки застосовності моделей, що полягають у формулюванні запитань від конкретних ролей у сфері інформаційної безпеки та оцінки експертами відповідей, згенерованих моделями штучного інтелекту. Критерії для цієї оцінки сформульовано на основі досвіду експертів та унікальних можливостей генеративних моделей. Це дослідження не лише сприяє розвитку галузі штучного інтелекту, але й охоплює практичні можливості та ідеї для використання для фахівців із інформаційної безпеки та організацій, які шукають інноваційні підходи до аналізу вимог. У кваліфікаційній роботі розглядається перетин людського інтелекту та штучного інтелекту, представляючи спільне та комплексне дослідження ролі генеративних моделей штучного інтелекту у вдосконаленні інформаційної безпеки.

## ANNOTATION

Research on the Application of Generative Artificial Intelligence for the Analysis of Information Security Requirements // Qualification paper of the educational level “Master” // Olena Smikh // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cyber Security, SBm-61 group // Ternopil, 2023 // P. 191., fig. – 2, tables – 11, annexes 2, references – 30.

Keywords: INFORMATION SECURITY, SECURITY POLICIES, ARTIFICIAL INTELLIGENCE, GENERATIVE MODELS, ISO 27001, REQUIREMENTS ANALYSIS.

The qualification paper examines the technology of generative artificial intelligence and its application to the analysis of information security requirements. The study focuses on three models of generative artificial intelligence, which were selected through analysis. Well-known approaches to testing and evaluating the applicability of models have been adapted, which consist in formulating questions from specific roles in the field of information security and evaluating answers generated by artificial intelligence models by experts. The criteria for this evaluation are formulated based on the experience of experts and the unique capabilities of generative models. This research not only advances the field of artificial intelligence, but also provides practical opportunities and insights for information security professionals and organizations seeking innovative approaches to requirements analysis. The research examines the intersection of human intelligence and artificial intelligence, presenting a joint and comprehensive study of the role of generative models of artificial intelligence in improving information security.

## ЗМІСТ

|  |    |
|--|----|
| ВСТУП.....   | 8  |
| 1 ТЕОРЕТИЧНО-АНАЛІТИЧНА ЧАСТИНА.....   | 10 |
| 1.1 Сучасні тенденції та проблеми аналізу вимог інформаційної безпеки .....  | 10 |
| 1.2 Огляд технології генеративного штучного інтелекту (ГШІ).....   | 11 |
| 1.2.1 Загальний огляд технології ГШІ .....   | 11 |
| 1.2.2 Правове регулювання використання технології штучного інтелекту .....   | 13 |
| 1.3 Огляд застосування генеративного штучного інтелекту в галузі<br>інформаційної безпеки.....   | 16 |
| 1.4 Недоліки та можливі ризики використання генеративних платформ. ....  | 18 |
| 2 ПРАКТИЧНА ЧАСТИНА .....  | 21 |
| 2.1 Вибір моделей генеративного штучного інтелекту.....  | 21 |
| 2.2 Визначення ролей та розробка запитань .....  | 28 |
| 2.2.1 Визначення та розподіл ролей .....   | 28 |
| 2.2.2 Розробка запитань .....  | 29 |
| 2.2.3 Процес поставовки запитань до генеративних моделей ШІ .....  | 34 |
| 2.3 Розробка критеріїв оцінювання .....  | 36 |
| 2.3.1 Використання генеративних моделей для створення критеріїв<br>оцінювання.....   | 36 |
| 2.3.2 Уніфікація та узгодження критерії та шкал оцінювання генеративних<br>моделей штучного інтелекту .....                                | 45 |
| 2.4 Проведення дослідження та аналіз результатів використання генеративних<br>моделей ШІ з метою аналізу вимог інформаційної безпеки ..... | 52 |
| 2.4.1 Проведення експерименту: постановка запитань моделям ШІ.....   | 52 |
| 2.4.2 Аналіз відповідей моделей ГШІ за визначеними критеріями .....  | 54 |
| 2.4.3 Результати експертної оцінки.....  | 55 |
| 2.4.4 Рекомендації щодо подальших досліджень у сфері аналізу вимог<br>інформаційної безпеки .....  | 59 |
| 3 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ .....  | 61 |
| 3.1 Охорона праці .....  | 61 |
| 3.2 Безпека в надзвичайних ситуаціях.....  | 64 |
| ВИСНОВКИ.....  | 68 |

|                        |    |
|------------------------|----|
| ПЕРЕЛІК ПОСИЛАНЬ ..... | 70 |
| ДОДАТКИ.....           | 74 |
| ДОДАТОК А.....         | 74 |
| ДОДАТОК Б.....         | 76 |

## ВСТУП

В епоху стрімкого розвитку інформаційних технологій, зростає необхідність забезпечити належний рівень захисту для інновацій, які невпинно інтегруються у процеси усіх видів бізнесу. Організації вбачають потребу у розширенні постачання своїх сервісів по всьому світу, що створює для них нові виклики, зокрема у сфері інформаційної безпеки. Так, аби переконатись, що процеси та інформаційні системи організації належним чином захищені, потрібно правильно визначити і проаналізувати вимоги, які до них застосовні, включаючи вимоги локального законодавства, де ведеться бізнес, індустріальні вимоги, якщо проводять роботу із специфічним обладнанням, вимоги щодо обробки даних, загальноприйняті найкращі практики, контрактні вимоги та багато іншого. Аналіз вимог та їх застосовності – це досить складний і комплексний процес, який вимагає достатнього рівня обізнаності, великої кількості часових і людських ресурсів, розуміння контексту організації та її процесів, технічних особливостей тощо. Враховуючи також динамічність ландшафту кібезагроз, які організаціям потрібно випереджати у своїх заходах захисту, особливо складним завданням стає постійна підтримка актуальності вимог, адже вимоги досить часто можуть оновлюватись, а безперервно відслідковувати їх актуальність не завжди є вигідним рішенням для багатьох компаній.

Проте, поява прогресуючої технології генеративного штучного інтелекту (ГШІ), потенційно зможе змінити традиційні підходи аналізу вимог інформаційної безпеки та повністю автоматизувати даний процес. Дане дослідження спрямоване на вивчення потенціалу популярних генеративних моделей штучного інтелекту, таких як GPT-4, Bard та Claude щодо аналізу вимог інформаційної безпеки та формування на їх основі невід’ємних елементів безпеки в компанії, включаючи загальну організаційну та технічну структуру, політики, процедури, процеси, та заходи захисту.



Метою даного дослідження є оцінка ефективності моделей генеративного штучного інтелекту в проведенні аналізу вимог інформаційної безпеки, використовуючи їхні потужні можливості щодо розуміння природньої (людської) мови та доступу до величезного набору даних.

Основні завдання даного дослідження включають:

- вибір і аналіз моделей генеративного штучного інтелекту на основі їхніх можливостей та відповідності до вимог релевантного законодавства;
- формування запитань від дібраних ролей інформаційної безпеки для генерації відповідей моделями ГШІ;
- розробка критеріїв оцінювання та шкали оцінювання для визначення ефективності кожної моделі;
- проведення експерименту, що включає обробку питань генеративними моделями за певних умов;
- аналіз результатів, який включає експертну оцінку згенерованих відповідей за визначеними критеріями та шкалою з метою отримання порівняльної оцінки вибраних моделей.

Інтеграція ГШІ в інформаційну безпеку має потенціал кардинально змінити те, як організації долають труднощі щодо захисту даних та інших активів. Це дослідження спрямоване на важливу потребу в сучасному інформаційно-технологічному просторі, де перетинаються людський інтелект, штучний інтелект, стрімкий технологічний розвиток, невідомий прогрес кібератак та мінливе законодавство. Використовуючи можливості моделей ГШІ, дане дослідження має на меті запропонувати потенційні шляхи використання ГШІ для створення надійного середовища інформаційної безпеки шляхом розробки та вдосконалення політик та процедур на всіх ланках в організації.

# 1 ТЕОРЕТИЧНО-АНАЛІТИЧНА ЧАСТИНА

## 1.1 Сучасні тенденції та проблеми аналізу вимог інформаційної безпеки

Вимоги інформаційної безпеки відіграють надзвичайно важливу роль у захисті цілісності, конфіденційності та доступності конфіденційних даних і систем організації. У сучасному динамічному технологічному середовищі компанії стикаються з численними проблемами, пов'язаними з ефективним управлінням і впровадженням вимог інформаційної безпеки. Незважаючи на це, компаніям доводиться вирішувати ці проблеми для побудови надійного ландшафту для захисту своїх та клієнтських активів.

Вимоги інформаційної безпеки охоплюють набір правил, норм і стандартів, призначених для захисту інформаційних активів організації. Ці вимоги гарантують, що конфіденційні дані безпечно обробляються, зберігаються та передаються, захищаючи від несанкціонованого доступу, витоку даних та інших кіберзагроз. Компаніям потрібні вимоги до інформаційної безпеки, щоб гарантувати належний рівень безпеки, відповідати галузевим нормам і підтримувати довіру зацікавлених сторін. Проте процес визначення та аналізу відповідних нормативних актів, оцінка їх застосовності, розробка відповідних корпоративних документів та впровадження відповідних заходів захисту часто передбачає значний обсяг ручної роботи, а також витрати людських та часових ресурсів для підтримки вимог та релевантних документів в актуальному стані.

Для спрощення даного процесу організації часто застосовують платформи для автоматизації відповідності вимогам (compliance automation platforms), де вже зібрано та проаналізовано певний набір вимог міжнародних стандартів, а також розроблені загальні політики та процедури [1][2]. Проте, ці платформи також вимагають постійної актуалізації стандартів та регуляторик, як збоку розробників,

так і зі сторони кінцевих користувачів. Окрім цього, ліцензії на такі платформи доволі дорогі, перелік доступних стандартів не покриває всіх можливих випадків застосування, а створення політик та процедур все ще вимагає певного рівня компетенцій та розуміння потреб індустрії.

Саме тому виникає необхідність в універсальному рішенні, яке б могло охопити величезний спектр найрізноманітніших вимог, незалежно від локації, сфери діяльності компанії, її розміру та технологічних можливостей, при цьому будучи простим та зрозумілим у використанні та підтримці. Для вирішення даного питання було розглянуто технологію генеративного штучного інтелекту та її можливості щодо аналізу вимог інформаційної безпеки.

## **1.2 Огляд технології генеративного штучного інтелекту (ГШІ)**

### **1.2.1 Загальний огляд технології ГШІ**

Генеративні платформи штучного інтелекту є класом систем, призначених для автоматичного створення нового контенту. Ці платформи використовують розширені алгоритми, які часто використовують методи машинного навчання, щоб генерувати різноманітні результати, такі як текст, зображення, відео чи навіть музику. Відмінною особливістю цих платформ є їхня здатність створювати креативний контент відповідно до заданого контексту, імітуючи процеси аналізу та генерації, подібні до людських.

Ключовими характеристиками таких платформ є:

- Адаптивність – генеративні платформи адаптуються та навчаються на даних, розвиваючи свою здатність генерувати контент на основі шаблонів та доступної інформації, що використовуються під час навчання.

- Автономна креативність – ці платформи демонструють здатність автономно генерувати вміст без детальних вказівок людини, при цьому демонструючи креативність у своїх результатах.
- Навчання на основі даних – моделі машинного навчання в рамках генеративних платформ навчаються на основі величезних наборів даних, що дозволяє їм фіксувати та відтворювати підходи, знайдені в навчальних даних.
- Розуміння контексту – генеративні платформи демонструють контекстне розуміння вхідних даних, що дозволяє їм генерувати результати, які відповідають заданому контексту.

Уже зараз (наприкінці 2023 року) існує більше 14,700 зразків генеративних платформ[3]. Усі вони формально розподілені за наступними типами:

- Текстові генератори:
  - 1) Функція: створення тексту на основі заданої інформації чи запитання, що схожий на результат діяльності людського інтелекту.
  - 2) Приклад: GPT-3 (Generative Pre-trained Transformer 3) від OpenAI, Bard від Google, Claude від Anthropic.
- Генератори зображень:
  - 1) Функція: створення зображення, які часто неможливо відрізнити від тих, що створених людьми.
  - 2) Приклад: StyleGAN (Generative Adversarial Network), Midjourney.
- Відеогенератори:
  - 1) Функція: створення реалістичних відео за допомогою методів глибокого навчання.
  - 2) Приклад: DeepMind.
- Генератори музики:
  - 1) Функція: створення музики автономно, з використанням попередньо визначених шаблонів або стилів.

- 2) Приклад: створені ШІ композиції з використанням рекурентних нейронних мереж, наприклад Loudly, Soundraw.
- Інші спеціалізовані генератори:
    - 1) Функція: платформи, розроблені для конкретних завдань, наприклад створення фрагментів коду, рецептів або 3D-моделей.
    - 2) Приклад: GitHub Copilot для генерації коду.

### **1.2.2 Правове регулювання використання технології штучного інтелекту**

Оскільки увага до генеративного штучного інтелекту (ШІ) продовжує зростати, разом із цим зростає і необхідність у законодавчому регулюванні цієї технології, оскільки вона може швидко негативно вплинути на велику кількість людей. Вплив може мати форму дискримінації, увічнення стереотипів, порушення приватності, негативних упереджень і знищення основних людських цінностей.

У червні 2023 року у ЄС було запропоновано перший у світі проект регламенту щодо ШІ – EU Artificial Intelligence Act (AIA)[4]. Грунтуючись на засадах етики штучного інтелекту, пріоритетом для даного акту є гарантія того, що системи штучного інтелекту, які використовуються в ЄС, є «безпечними, прозорими, простежуваними, недискримінаційними та екологічно дружніми».[5] Щоб уникнути шкідливих наслідків, ЄС AIA наполягає на тому, щоб люди залишалися залученими до систем ШІ. Іншими словами, компанії не можуть просто дозволити штучному інтелекту та автоматизації працювати самостійно. Запропонований закон розподіляє ШІ на три різні категорії залежно від ризику, який він може становити для людей — кожен рівень ризику вимагає різного рівня регулювання. ЄС виділяє три рівні ризику: неприйнятний ризик, високий ризик і обмежений ризик:

- Неприйнятний ризик – використовувати технології, які є шкідливими та становлять загрозу для людей, буде заборонено. Такі приклади можуть включати когнітивний вплив окремих осіб або певних уразливих класів; ранжирування людей на основі їх соціального становища та масове використання розпізнавання облич для спостереження в реальному часі та віддаленої ідентифікації.
- Високий ризик – системи штучного інтелекту, які можуть негативно вплинути на безпеку або основні права та свободи, класифікуються ЄС у дві різні категорії. Перша категорія — це штучний інтелект, вбудований у роздрібні продукти, які наразі підпадають під дію правил безпеки продуктів ЄС. Це включає в себе іграшки, літаки, автомобілі, медичне обладнання, ліфти і так далі. Другу категорію потрібно буде зареєструвати в базі даних ЄС. Сюди входять такі технології, як біометрія, функціонування критичної інфраструктури, навчання та освіта, діяльність, пов'язана з працевлаштуванням, поліція, прикордонний контроль та юридичний аналіз законодавства.
- Обмежений ризик – системи з низьким рівнем ризику повинні щонайменше відповідати стандартам прозорості та відкритості, які дадуть людям можливість приймати обґрунтовані рішення. ЄС передбачає, що користувачі повинні бути повідомлені щоразу, коли вони взаємодіють з ШІ. Вони також вимагають, щоб моделі створювалися таким чином, щоб вони не створювали незаконний матеріал. Вони також вимагають, щоб виробники моделей розкривали, який матеріал, захищений авторським правом (якщо такий є), використовувався під час навчання.

Нещодавно дослідниками з Центру досліджень фундаментальних моделей Стенфордського університету (Stanford University's Center for Research on Foundation Models (CRFM)) та Інституту людського штучного інтелекту (Institute for Human-Centered Artificial Intelligence (HAI)) було опубліковано статтю [6] щодо

відповідності моделей генеративного штучного інтелекту до EU AIA. Для дослідження було проаналізовано даний акт наступним чином: двадцять дві вимоги акту були прокласифіковані і з них було обрано 12 вимог, які розділені між 4 різними категоріями. Команда вибрала лише ті вимоги, які було найлегше оцінити на основі загальнодоступних даних і документації, наданих розробниками моделей. Ці вимоги представлені у таблиці 1.1.

Таблиця 1.1 – Класифікація вимог EU Artificial Intelligence Act

| Категорія | Ключове слово            | Вимога (узагальнена)  | Розділ  |
|-----------|--------------------------|---|---|
| Data      | Data sources             | Describe data sources used to train the foundation model.   | Amendment 771, Annex VIII, section C, page 348  |
|           | Data governance          | Use data that is subject to data governance measures (suitability, bias, and appropriate mitigation) to train the foundation model. | Amendment 399, Article 28b, page 200  |
|           | Copyrighted data         | Summarize copyrighted data used to train the foundation model.  | Amendment 399, Article 28b, page 200  |
| Compute   | Compute                  | Disclose compute (model size, computer power, training time) used to train the foundation model.                                    | Amendment 771, Annex VIII, section C, page 348  |
|           | Energy                   | Measure energy consumption and take steps to reduce energy use in training the foundation model.                                    | Amendment 399, Article 28b, page 200  |
| Model     | Capabilities/limitations | Describe capabilities and limitations of the foundation model.  | Amendment 771, Annex VIII, section C, page 348  |
|           | Risks/mitigations        | Describe foreseeable risks, associated mitigations and justify any non0mitigated risks of the foundation model.                     | Amendment 771, Annex VIII, section C, page 348 and Amendment 399, Article 28b, page 200 |

## Продовження табл. 1.1

|            |                           |   |   |
|------------|---------------------------|---|---|
|            | Evaluations               | Benchmark the foundation model on public/industry standard benchmarks.                            | Amendment 771, Annex VIII, section C, page 348 and Amendment 399, Article 28b, page 200 |
|            | Testing                   | Report the results of internal and external testing of the foundational model.                    | Amendment 771, Annex VIII, section C, page 348 and Amendment 399, Article 28b, page 200 |
| Deployment | Machine-generated content | Disclose content from a generative foundation model is machine generated and not human-generated. | Amendment 101, Recital 60g, page 76   |
|            | Member states             | Disclose EU member states where the foundation model is on the market.                            | Amendment 771, Annex VIII, section C, page 348  |
|            | Downstream documentation  | Provide sufficient technical compliance for downstream compliance with the EU AI Act.             | Amendment 101, Recital 60g, page 76 and Amendment 399, Article 28b, page 200            |

Дослідники розглянули моделі від OpenAI, Anthropic, Google, Meta, Stability.ai та багатьох інших. Результати цих досліджень представлені у розділі 2.1 разом із іншими критеріями для відбору моделей генеративного штучного інтелекту для аналізу вимог інформаційної безпеки.

### 1.3 Огляд застосування генеративного штучного інтелекту в галузі інформаційної безпеки

Незважаючи на відносну технології генеративного штучного інтелекту, їй уже знайшли застосування у багатьох напрямках інформаційної безпеки, забезпечуючи інноваційні рішення для складних проблем, з якими стикаються організації, щоб захистити свої активи.



Одним із найбільш поширених прикладів застосування ГШІ є автоматичне виявлення загроз та реагування на них. Завдяки постійному аналізу величезних наборів даних і вивченню типових сценаріїв атак, ГШІ може автономно виявляти нові загрози та реагувати на них у режимі реального часу. Ця можливість підвищує ефективність заходів безпеки та швидкість реагування команд з операційного центру безпеки (Security Operations Center, SOC), забезпечуючи проактивний захист від нових кіберзагроз.

Також генеративний штучний інтелект знайшов своє застосування в оцінці ризиків інформаційної безпеки. ГШІ полегшує оцінку ризиків шляхом безперервного аналізу та адаптації до динамічного ландшафту загроз. Він оцінює потенційні ризики, пов'язані з новими та існуючими технологіями, вразливостями та нормативними змінами, що дозволяє організаціям завчасно відкоригувати свої заходи безпеки та внутрішні правила для ефективного попередження чи пом'якшення нових ризиків.

Окрім цього, ГШІ використовується у поєднанні із системи запобігання витоку інформації (Data Leakage Prevention, DLP). Аналізуючи вміст файлів і повідомлень у режимі реального часу, ГШІ може прокласифікувати інформацію відповідно до рівнів конфіденційності, заданих організацією та застосувати відповідні політики DLP, які обмежують чи контролюють поширення чи переміщення конфіденційних даних, запобігаючи ненавмисному чи зловмисному витоку даних.

Не менш важливим є внесок ГШІ у сферу приватності даних (privacy). Зокрема, алгоритми штучного інтелекту можуть використовуватись для анонімізації конфіденційних персональних даних з метою захисту персональних даних користувачів. Також досить цікавим є дослідження представників Канадського університету Гвельфа (University of Guelph) [7] щодо автоматичного генерування політики приватності використовуючи моделі глибокого навчання. Дане дослідження ще раз підкреслює важливість політики приватності та наявні

недоліки існуючих зразків. Для проведення дослідження було проаналізовано можливості моделей двох типів (Long Short-Term Memory (LSTM) та bidirectional Long Short-Term Memory bi-LSTM). Навчання та тестування проводилось на трьох рівнях документів: абзацу, речення та практичних даних. Це дослідження показали багатообіцяючі результати щодо застосування моделей штучного інтелекту для аналізу вимог приватності та створення відповідних документів.

Користь та унікальні можливості технологія ГШІ принесла не лише у галузь інформаційної безпеки та ІТ, але й у інші процеси та галузі, такі як проведення наукових досліджень та навчання у закладах вищої освіти[8], прийняття управлінських рішень [9], рекрутинг [10], живопис та мистецтво [11] і багато інших, тому неможливо оминути дану технологію у сучасному світі.

#### **1.4 Недоліки та можливі ризики використання генеративних платформ.**

Генеративний штучний інтелект — це потужна технологія, яка може внести покращення у безліч галузей. Однак важливо знати про ризики та проблеми, пов'язані з цією технологією, перш ніж використовувати її.

ГШІ можна використовувати для створення реалістичних медіафайлів (відео чи аудіо), які відображають, що певна особа робить чи говорить щось, що насправді не відповідає дійсності, з метою завдання репутаційної шкоди, поширення дезінформації, пропаганди, маніпулювання громадською думкою чи навіть шахрайства. Також генеративні моделі можна використовувати для створення фішингових електронних листів або іншого зловмисного контенту, за допомогою яких можна обманом змусити людей поділитись конфіденційною інформацією або натиснути на зловмисні посилання.

Окрім цього, виникають ризики, що стосується роботи з даними. Перш за все, розробники моделей можуть використовувати для навчання підроблені дані, або ж ці дані можуть підмінити зломисники, що може призвести до генерування неточних або оманливих результатів. Це може стати основою для атаки на системи ШІ, які використовуються в критично важливих програмах у сферах охорони здоров'я чи фінансів. Оскільки генеративні моделі штучного інтелекту часто навчаються на масивних наборах тексту та коду, то також існує ризик витоку даних. Ці дані можуть містити конфіденційну особисту інформацію, таку як імена, адреси, номери кредитних карток та багато іншого. Якщо генеративна модель AI не захищена належним чином, ці дані можуть потрапити до рук зловмисників, що в результаті може спричинити крадіжку особистих даних. Тобто, конфіденційні та персональні дані отримані чи згенеровані ГШІ можуть бути використані для вивчення шахрайства чи створення підроблених облікових записів.

За час існування технології генеративного штучного інтелекту користувачі також зіштовхнулись із проблемами, пов'язаними із етичними аспектами. ГШІ навчаються на даних, зібраних на неосяжних просторах Інтернету. Ці дані можуть містити стереотипні чи неетичні твердження, що може призвести до упереджених чи дискримінаційних відповідей ГШІ. А завдяки неймовірним можливостям даної технології, ГШІ вдається автоматизувати безліч завдань та процесів, що виконувались людьми вручну – як результат, людство занепокоїлось щодо можливої втрати робочих місць та всесвітньої економічної кризи.

Не менш важливим є те, що використання генеративних моделей має вплив і на навколишнє середовище, адже для того, аби згенерувати контент, потрібні значні обчислювальні потужності, що може мати негативні екологічні наслідки.

Вищезазначені ризики та проблеми – далеко не повний список, того, що несе за собою використання ГШІ. Саме тому надзвичайно важливо забезпечити відповідальне використання даної технології, як на законодавчому рівні, так і на

рівні кожної організації чи проекту. Зокрема варто врахувати наступні рекомендації:

- Потрібно перевіряти згенеровану інформацію на предмет того, чи вона справді відповідає дійсності. Якщо можливо, варто попросити модель надати посилання на першоджерело.
- Не варто використовувати згенеровані результати у оригінальному формулюванні, адже інформація, яка використовувалась ГШІ для генерації відповіді може бути захищене авторським правом, а пряме використання може стати порушенням інтелектуальної власності та появою плагіату у напрацюванні.
- Ні в якому разі не можна надавати моделям будь-яку комерційну, конфіденційну чи персональну інформацію при створенні запитів, адже це може стати причиною витоку чи крадіжки цих даних.
- Не варто довіряти ГШІ щодо граматичного та лексичного оформлення, адже моделі все ще роблять помилки. Окрім цього, потрібно звертати увагу на емоційне забарвлення контенту та наявність неетичних тверджень. Кожен користувач ГШІ повинен розуміти свою відповідальність за використання результатів ГШІ.

## 2 ПРАКТИЧНА ЧАСТИНА

### 2.1 Вибір моделей генеративного штучного інтелекту

Для аналізу вимог інформаційної безпеки в кваліфікаційній роботі увагу буде присвячено саме текстовим генераторам – це і буде першим критерієм до відбору. Окрім цього, при виборі платформ для аналізу потрібно врахувати і те, яка саме модель використовується всередині платформи, за користувацьким інтерфейсом. Враховуючи величезну кількість наявних рішень на основі GAI, кілька тисяч базуються на популярних моделях, наприклад GPT 3.5 чи GPT 4. Не менш важливим також є те, чи актуальні дані використовувались для навчання моделі, адже саме від цього залежить наскільки точними і релевантними будуть згенеровані відповіді. Ще одним досить вагомим аспектом є готовність платформи до використання середньостатистичним користувачем Інтернет – тобто людиною, яка не має навичок програмування і хоче швидко у форматі чату чи іншого зручного інтерфейсу отримати відповіді на свої запитання чи бажаний контент.

Генеративні платформи штучного інтелекту – це сфера, яка швидко розвивається, і постійно з'являються нові платформи. Нижче наведено огляд деяких найпопулярніших генеративних платформ ШІ сьогодні, їх переваг та недоліків:

- **ChatGPT від OpenAI (GPT 3.5/GPT 4):** це велика мовна модель від OpenAI, яка здатна генерувати текст, перекладати текст на безліч мов, створювати різні типи контенту та інформативно відповідати на запитання. ChatGPT все ще знаходиться в стадії розробки, але його вже використовують для створення широкого спектру вражаючих програм, включаючи чат-боти, генератори коду та інструменти для копірайтингу [12].

*Переваги:*

- 1) ChatGPT чудово розуміє природну (людську) мову, що робить його ефективним для програм, що передбачають вільний формат спілкування (наприклад, чат-бот, розумний помічник тощо);
- 2) цю платформу можна використовувати для широкого кола завдань, включаючи відповіді на загальні запитання та створення спеціалізованих документів чи коду;
- 3) завдяки тому, що ChatGPT навчений на різноманітних наборах даних, у нього є величезні переваги щодо надання відповідей у потрібних шаблонах, стилях та мовах, що допомагає краще підлаштувати відповіді під необхідний запит.

***Недоліки:***

- 1) іноді через його залежність від стандартизованого сприйняття доступної інформації ChatGPT може демонструвати відсутність чутливості до контексту, що призводить до генерації відповідей, які можуть здаватися непов'язаними або безглуздими;
  - 2) як і багато інших мовних моделей, ChatGPT може ненавмисно зберегти упередження, наявні в навчальних даних, що потенційно може призвести до упереджених результатів.
- **Bard від Google (LaMDA):** це велика мовна модель від Google AI, яка багато в чому схожа на ChatGPT. Проте Bard спеціально розроблений, щоб бути інформативним і вичерпним у своїх відповідях, а також навчений на величезному наборі прикладів коду, що дозволяє йому вправно допомагати користувачам у розробці програмного забезпечення [13].

***Переваги:***

- 1) Bard є універсальним генератором тексту, який чудово підходить для написання текстів різних форматів;

- 2) дана модель також демонструє високий рівень креативності у створенні наративів, що робить його цінним інструментом для авторів і творців контенту;
- 3) Bard є доволі адаптивним у створенні різноманітних текстових відповідей у різних жанрах і стилях написання. Окрім цього, у своїх відповідях модель надає одразу посилання на першоджерело та збагачує контент зображеннями;
- 4) Одразу пропонує кілька варіантів відповіді.

***Недоліки:***

- 1) хоч Bard вміє створювати креативний текст, він може зіткнутися з труднощами в забезпеченні загальної зв'язності та структури в довгих відповідях;
  - 2) як і будь-який текстовий генератор, Bard може час від часу створювати результати з контекстуальними невідповідностями або ненавмисними змінами тону.
- **Claude від Anthropic (Claude/Claude 2):** це нова генеративна платформа штучного інтелекту від Anthropic, яка навчається на величезному наборі тексту та коду. Він все ще знаходиться на стадії розробки, але вже продемонстрував свою здатність генерувати реалістичні та креативні результати, такі як код, вірші, сценарії та музичні твори. Claude особливо добре підходить для таких завдань, як розробка програмного забезпечення та творче написання. Однак іноді Claude може бути менш креативним, ніж звичайні користувачі [14].

***Переваги:***

- 1) Claude, створює візуально описові та творчо багаті текстові результати;
- 2) вміє створювати текстові описів із чіткими художніми стилями, що робить його придатним для творчих письмових проєктів.

***Недоліки:***

- 1) на відміну від моделей більш загального призначення, спеціалізація Claude на створенні художнього тексту робить його менш придатним для завдань поза сферою творчого письма.
- **AI21 Studio від AI21 Labs (Jurassic-1 Jumbo):** це модель штучного інтелекту для генерації тексту, розроблена компанією AI21 Labs. Це найбільша та найпотужніша модель ШІ для створення тексту на сьогодні. Jurassic-1 Jumbo навчається на величезному наборі тексту та коду, і його можна використовувати для генерації різноманітних текстових форматів, включаючи код, вірші, сценарії та музичні твори [15].

***Переваги:***

- 1) модель від AI21 Labs відома своїми розширеними можливостями розуміння природної мови, що дає їй змогу генерувати зв'язний і контекстуально відповідний текст;
- 2) Jurassic-1 Jumbo також продемонструвала креативність у створенні різноманітного та високоякісного контенту, що робить її цінними для різноманітних додатків, зокрема для допомоги при написанні та створенні різних типів інформації;
- 3) враховуючи те, що Jurassic-1 Jumbo є розширенням попередньої моделі (Jurassic-1), то ця модель точно має низку переваг від великомасштабної архітектури, що дозволяє розуміти та створювати контент на широкий спектр тем.

***Недоліки:***

- 1) великомасштабні мовні моделі від AI21 Labs можуть бути дорогими з обчислювальної точки зору, вимагаючи значних ресурсів для навчання;
- 2) як і у випадку з багатьма мовними моделями, може виникнути занепокоєння щодо упередженості у створеному контенті.



Забезпечення справедливості та усунення упередженості є постійним викликом у розробці моделей ШІ.

- **BLOOM від Hugging Face (BLOOM):** BLOOM – це модель штучного інтелекту генерації тексту, розроблена компанією Hugging Face. Вона навчена на великій кількості текстових даних, за допомогою ресурсів промислового масштабу [16].

***Переваги:***

- 1) модель навчається на величезному наборі даних, що дає їй широкий спектр знань і здатність генерувати текст у різноманітних стилях;
- 2) BLOOM дуже універсальна модель і може використовуватися для різноманітних завдань, зокрема для створення тексту, перекладу тексту 46 мовами, розробки програмного забезпечення 13 мовами програмування та генерації контенту і відповідей на запитання в інформативний спосіб;
- 3) Hugging Face має активну спільноту, яка допомагає у розробці та вдосконаленню моделей. Підтримка спільноти сприяє інноваціям і постійному вдосконаленню моделей;
- 4) Hugging Face також дотримується принципів відкритого коду, роблячи свої моделі та інструменти доступними для розробників та ентузіастів для дослідження та вдосконалення.

***Недоліки:***

- 1) без конкретної інформації та розуміння роботи BLOOM складно усунути слабкі сторони моделі. Однак загальні проблеми з великими мовними моделями, такі як вимоги до ресурсів і потенційні упередження, все ще можуть виникати;

- 2) враховуючи те, що це доволі велика модель і потужна модель, вона може мати обмеження щодо розгортання на середовищах з обмеженими ресурсами.

Отож, ознайомившись із найбільш популярними моделями та платформами, варто провести їх детальний аналіз відповідно до зазначених вище критеріїв та відповідності до EU Artificial Intelligence Act. Порівняльна характеристика та оцінка кожної моделі представлена у таблиці 2.1.

Таблиця 2.1 – Порівняльна оцінка ГШІ

| Модель/<br>платформа | Готовність до<br>використання<br>(інтерфес<br>користувача)  | Дата<br>оновлення<br>наборів<br>даних                            | Відповідність до EU Artificial<br>Intelligence Act (AIA)* |         |       |            | Загальна<br>оцінка |
|----------------------|---|--|---|---------|-------|------------|--------------------|
|                      |   |  | Data  | Compute | Model | Deployment |                    |
| ChatGPT              | Чатбот,<br>інтуїтивно<br>зрозумілий<br>функціонал (3)   | Січень<br>2022 для<br>GPT3.5,<br>Квітень<br>2023 для<br>GPT4 (2) | 3   | 0       | 14    | 8          | <b>30</b>          |
| Bard                 | Чатбот,<br>зрозумілий<br>функціонал,<br>може<br>генерувати у<br>певних<br>форматах, які<br>автоматично<br>можна<br>перенести в<br>інше<br>середовище<br>(напр. Таблиці<br>Google) (3) | Липень<br>2023 (3)   | 5   | 0       | 11    | 11         | <b>33</b>          |

Продовження табл. 2.1

|             |  |                       |    |   |    |   |           |
|-------------|--|-----------------------|----|---|----|---|-----------|
| Claude      | Чатбот, інтуїтивно зрозумілий функціонал, проте наразі недоступний у ЄС (потрібне VPN-з'єднання) (2)           | Січень-лютий 2023 (2) | 0  | 0 | 2  | 5 | <b>11</b> |
| AI21 Studio | API, вимагає вміння програмування та іншого продукту для інтеграції (0)  | Липень 2023 (3)       | 0  | 0 | 4  | 4 | <b>11</b> |
| BLOOM       | Доступний вихідний код, до якого можна вносити зміни для кастомізації моделі, вимагає вміння програмування (0) | Серпень 2023 (3)      | 11 | 8 | 10 | 7 | <b>39</b> |

Згідно із результатами даного аналізу можна зробити висновок, що найпопулярніше – не значить найкраще. Аби досягти дійсно цінних результатів згенерованого контенту потрібно переконатись, що модель дійсно враховує всі необхідні аспекти щодо роботи з даними, що ці дані актуальні та багато іншого. Також цей аналіз показав, що не варто обмежуватись лише готовими рішеннями, можливо навіть є сенс внести свій вклад у якусь існуючу, але менш популярну модель, щоб зробити її ідеальною для конкретного використання.

Проте, для цілей даного дослідження з метою спрощення проведення експерименту було обрано лише ті моделі для аналізу вимог, які не вимагають додаткових налаштувань та одразу доступні для використання у форматі чат-боту, а саме ChatGPT (GPT-4), Bard (LaMDA) та Claude (Claude).

## **2.2 Визначення ролей та розробка запитань**

### **2.2.1 Визначення та розподіл ролей**

Розуміння вимог інформаційної безпеки є абсолютно важливим для кожного спеціаліста в межах організації. Проте, особливо це є необхідним для тих, хто безпосередньо займається впровадженням та підтримкою інформаційної безпеки. Саме тому, було визначено три ключових ролі: менеджер відділу інформаційної безпеки, консультант з інформаційної безпеки та інженер з інформаційної безпеки. Кожна з цих ролей забезпечує різні аспекти інформаційної безпеки та фокусується на різних заходах захисту:

- менеджер, як головна особа, яка приймає рішення, відповідає за формування, підтримку та розвиток стратегічних аспектів інформаційної безпеки. Ця роль передбачає прийняття рішень на високому рівні, управління ризиками та розподіл ресурсів. Менеджери відіграють вирішальну роль у формуванні загальної безпеки організації, саме тому їхня роль є надзвичайно важливою для оцінки здатності генеративних моделей ШІ надавати стратегічні та базові ідеї для забезпечення інформаційної безпеки в компанії;
- консультант – консультанти відповідальні за забезпечення відповідності, впровадження найкращих галузевих практик та розробку політик. Їх роль полягає у тому, щоб допомогти організаціям узгодити внутрішні документи, процеси та процедури із нормативними вимогами та

галузевими стандартами. Формулюючи запитання, призначені для консультантів, дослідження має на меті оцінити здатність генеративних моделей штучного інтелекту надавати вказівки щодо відповідності вимогам та передовим практикам, що є важливими компонентами ефективної інформаційної безпеки;

- інженер – роль зосереджена на технічних тонкощах інформаційної безпеки. Завдання інженера включають налаштування системи, оцінку вразливостей і забезпечення технічної реалізації заходів безпеки. Запитання, призначені для ІБ-інженерів, стосуються технічних нюансів і дають зрозуміти, наскільки добре генеративні моделі ШІ можуть допомогти в забезпеченні детальних технічних аспектів вимог інформаційної безпеки.

Визначення цих ролей є невід’ємною частиною забезпечення всебічної оцінки результатів генеративного штучного інтелекту, яка охоплює стратегічні, консультативні та технічні аспекти в області інформаційної безпеки. Формулювання запитань, пов’язаних із цими конкретними ролями, є необхідним для того, щоб забезпечити комплексну оцінку досліджуваних генеративних моделей штучного інтелекту із врахуванням різних аспектів та рівнів деталізації запитань.

### **2.2.2 Розробка запитань**

Різноманітність сформульованих запитань є основним завданням для забезпечення комплексної оцінки генеративних моделей ШІ. У цьому розділі обговорюються стратегії, які використовуються для забезпечення охоплення широкого спектру тем і проблем у запитах до моделей ГШІ.

Перш за все, було виділено три окремі ролі з метою забезпечення оцінки на різних рівнях в організації. Таким чином, з’являється можливість оцінити, наскільки

добре справляються моделі, коли запити є загального характеру та більш конкретні, із врахуванням окремої системи чи нюансів роботи. Окрім цього, було докладено зусиль, щоб уникнути надмірності у запитаннях, тобто вони були сформульовані у такий спосіб, щоб запитання від різних ролей не спонукали моделі відповідати подібно. Специфіка і формулювання запитань залежить безпосередньо від того, що входить у функційні обов'язки кожної з ролей, щоб передбачити, що потенційно може запитати кожна з них для виконання своїх операційних задач. Наприклад, запитання від менеджера ІБ мають покривати високорівневі задачі, які б допомогли йому сформулювати стратегію інформаційної безпеки компанії та загальні правила щодо інформаційної безпеки компанії. Від консультанта очікується, що він буде надавати більш практичні поради щодо впровадження вимог інформаційної безпеки, допоможе узгодити організаційні процеси та процедури із світовими практиками, забезпечуючи відповідність із стандартами та регуляторними вимогами. Запитання від інженера ІБ передбачатимуть більш детальні технічні аспекти інформаційної безпеки, зокрема технічні засоби захисту даних та інформаційних систем, які б включали налаштування безпеки в конкретних середовищах та створення безпечної інфраструктури.

Окрім цього, під час формування запитань було важливо забезпечити, щоб моделі охоплювали широкий спектр тем і напрямків інформаційної безпеки. Саме тому, за основу для створення запитань було взято структуру та перелік заходів захисту міжнародного стандарту ISO/IEC 27001 [17]. Основною причиною для вибору даного стандарту є його універсальність для організацій будь-яких розмірів та індустрій. Для цілей тестування було обрано декілька доменів з даного стандарту, кожен з яких було відображено у запитаннях для кожної ролі. Таким чином, дослідження гарантує, що генеративні моделі будуть всебічно оцінені, із врахуванням різних аспектів та напрямів інформаційної безпеки.

Також, для підвищення реалістичності оцінки моделей ШІ, запитання були сформульовані так, щоб симулювати реальні сценарії, з яким насправді можуть

зіткнутись спеціалісти з інформаційної безпеки. Не менш важливим аспектом є встановлення контексту для запитання, тобто було надано уточнення стосовно того, які сервіси надає компанія, де вона знаходиться, кількість працівників та застосовувані технології. Мета даного кроку – розробити запитання максимально наближеними до реальних запитів, щоб надати релевантну та надійну оцінку відповідям моделей генеративного штучного інтелекту.

Щодо формату, то було прийняте рішення формулювати запитання англійською мовою, оскільки моделі генеративного штучного інтелекту відносно нові і ще досконало не володіють українською мовою. До того ж, це мультинаціональна мова, яка зазвичай застосовується як основна для написання міжнародних стандартів та корпоративних документів.

Як результат даного етапу було сформовано 24 запитання, які представлені у таблиці 2.2.

Таблиця 2.2 – Запитання для тестування моделей

| Домен                       | Менеджер ІБ |   | Консультант ІБ |  | Інженер ІБ |  |
|-----------------------------|-------------|---|----------------|--|------------|--|
| General                     | M1          | Could you please advise which security frameworks should EU-based software development company with 500 employees follow?                       | C1             | Which security policies should be developed for EU-based software development company with 500 employees based on ISO27001?    | E1         | Which technologies you can advise for EU-based software development company with 500 employees to build on ?       |
| Context of the organization | M2          | How organizational structure of EU-based software development company with 500 employees should look like to manage security risks effectively? | C2             | Could you please develop Statement of Applicability for ISO27001 for EU-based software development company with 500 employees? | E2         | How should secure infrastructure of EU-based software development company with 500 employees look like on diagram? |

Продовження табл. 2.2

|                 |    |   |    |   |    |  |
|-----------------|----|---|----|---|----|--|
| Access Control  | M3 | Please develop Access Control Policy based on ISO 27001 to ensure the security and privacy of company systems and data.   | C3 | Develop a procedure on how to implement access controls in accordance with ISO27001 within the EU-based software development company.   | E3 | Develop a detailed instruction on how to configure access controls in Microsoft Azure in accordance with ISO 27001.  |
| Encryption      | M4 | Please develop Encryption Policy that adheres to the encryption requirements of ISO 27001 to protect sensitive data.  | C4 | Could you please create a detailed guideline on what should be done in order to implement Encryption policy in accordance with ISO27001 within EU-based software development company?   | E4 | Could you please create a procedure for IT technician on how to manage cryptographic keys in accordance with ISO 27001 and how to configure encryption on Windows devices? |
| Risk Management | M5 | Please develop an Information Security Risk Management Policy in accordance with ISO 27001 aimed at effective security risk identification, management and treatment. | C5 | Please develop a detailed procedure on how to assess risks in accordance with ISO27001 at EU-based software development company, what scales should be used to define risk levels and provide several examples of how risk register should look like? | E5 | Could you please advise what security controls should be configured in order to prevent the risk of data leakage in Microsoft 365?   |



Продовження табл. 2.2

|                                       |    |   |    |   |    |  |
|---------------------------------------|----|---|----|---|----|--|
| Secure Software Development Lifecycle | M6 | Please develop Secure Software Development Lifecycle Policy as per ISO 27001 requirements ensuring the security of software throughout the development lifecycle.             | C6 | How to ensure the implementation of secure SDLC controls on the projects conforming to ISO27001 at EU-based software development company? | E6 | Could you please provide the detailed technical configuration that needs to be done to secure the GitHub environment in accordance with ISO 27001? |
| Awareness and Training                | M7 | Could you please develop Security Awareness and Training Policy in accordance with ISO 27001 to raise awareness about information security among employees?                   | C7 | How to ensure the implementation of secure SDLC controls on the projects conforming to ISO27001 at EU-based software development company? | E7 | Could you prepare a training script for privileged Windows user covering related risks and recommendations?  |
| Privacy                               | M8 | What regulations should be followed in case our EU-based company provides software development services for client in California, who requires us to work with personal data? | C8 | Are there any privacy risks or concerns that should be taken into account while developing software under CCPA regulation?                | E8 | How to ensure that configuration of Microsoft 365 aligns with the requirements of CCPA?  |

Для спрощення подальшого посилання на запитання та їх оцінки, кожному питанню було надано унікальний ідентифікатор.

### 2.2.3 Процес поставновки запитань до генеративних моделей ШІ

Узгодженість процесу постановки запитань до генеративних моделей штучного інтелекту має основоположну роль у проведенні даного дослідження. Для того, щоб результати даного дослідження були достовірними та об'єктивними, варто переконатись, що експеримент для кожної з моделей відбувається на рівних умовах, а саме:

- ідентичність питань: кожна генеративна модель ШІ – GPT-4, Bard і Claude – отримає однакові запитання. Ця одноманітність усуває будь-які відхилення щодо змінних, які пов'язані із змістом запитання, що може повпливати на відповідь. Ідентичний характер запитів гарантує, що моделі оцінюються на основі їхніх властивих можливостей, а не потенційних варіацій у формулюванні питань;
- розмежування за ролями та «чистий старт»: незалежно від обчислювальних ресурсів, швидкості реагування системи чи будь-яких інших важливих факторів експеримент підтримує узгоджене середовище для кожної моделі, тобто кожна з моделей буде отримувати своє перше запитання у новому чаті, щоб попередити можливий вплив на відповіді, залежно від попередніх запитів. Окрім цього, кожна модель буде отримувати запитання в чаті відповідно до ролі, тобто в одному чаті ролі не будуть змішуватись. Очікується, що саме така рівність у постановці запитань допоможе збільшити надійність результатів за рахунок мінімізації зовнішнього впливу;
- послідовність: підхід до послідовного представлення запитань для генеративних моделей ШІ забезпечує пряму порівняльну оцінку. Це означає, що кожна з моделей буде отримувати запитання у тому самому порядку для кожної ролі. Саме це допоможе оцінити ефективність кожної моделі з точки зору менеджера, консультанта та інженера, а також

переконатись, що ніякі додаткові фактори не впливають на відповідь генеративної моделі;

- одна спроба: кожна з моделей пропонує функції регенерації чи удосконалення відповіді, що безперечно зручно для кінцевого користувача. Також користувач завжди має змогу задати уточнюючі запитання, щоб отримати більш детальну відповідь. Проте аби переконатись, що всі моделі мають рівні умови при проведенні даного експерименту, було прийнято рішення оцінювати лише першу згенеровану відповідь і ніяким чином не модифікувати її.

Стосовно порядку постановки запитань, представленому вище, було розглянуто кілька можливих варіантів. Перший варіант передбачав, що всі запитання будуть поставлені в одному чаті, послідовно по ролях і доменах, тобто, якщо відобразити цей підхід, використовуючи унікальні ідентифікатори запитань з таблиці 2.2, таке подання мало б наступний вигляд: M1, C1, E1, M2, C2 тощо. Цей варіант було відкинуто через те, що запитання різних ролей і доменів змішуються, тож на етапі оцінки було б складно зрозуміти наскільки добре справилась кожна з моделей, адже такий варіант створює доволі великий ланцюжок запитань у чаті.

Другий варіант передбачав створення окремого чату для кожного домену, тобто у першому чаті було б 3 запитання: M1, C1, E1; у другому – M2, C2, C3, та E2 і так далі (по горизонталі відносно таблиці 2.2.). Такий варіант теж було відкинуто, оскільки попередні відповіді можуть використовуватись для формування більш детальних відповідей для іншої ролі, що може не зовсім коректно повпливати на результати за реальних умов використання генеративних моделей штучного інтелекту.

Третій варіант полягає у тому, що запитання будуть ставитись відповідно до визначених ролей (по вертикалі відносно таблиці 2.2.), тобто перший чат буде містити запитання M1-M8, другий – C1-C8, третій – E1-E8. Вважається, що саме цей підхід зможе надати найбільш точні та реалістичні варіанти, оскільки домени

досить різні, і не мають впливати на попередні відповіді, при цьому підтримується розмежування ролей і є можливість детальніше оцінити наскільки добре справляється кожна з моделей із запитом менеджера, консультанта та інженера окремо.

Четвертий варіант передбачав створення нового чату для кожного запитання. Цей варіант не було обрано у зв'язку з тим, що він би не дав можливості якісно оцінити наскільки добре підлаштована модель під конкретну роль, а також це б створило додаткові незручності та не відповідало б реальним прикладам використання чат-ботів, адже досить часто користувачі задають свої запитання у одному і тому ж або частково пов'язаних чатах.

Результати постановки питань до генеративних моделей штучного інтелекту детально розглянуті у розділі 2.4.

## **2.3 Розробка критеріїв оцінювання**

### **2.3.1 Використання генеративних моделей для створення критеріїв оцінювання**

Після того, як кожній з моделей були надані запити щодо вимог інформаційної безпеки від трьох ролей, постало питання щодо того, як ефективно і точно оцінити, яка з моделей впоралась краще із даним завданням. Враховуючи інтерактивність та всебічність застосування моделей ШІ, виникла ідея запитати в них, за якими критеріями вони б оцінювали відповіді, отримані в ході даного дослідження. Отож, мета даного кроку – виявити та визначити потенційні критерії оцінки шляхом постановки запитань і ретельного вивчення відповідей кожної моделі для виявлення неявних чи специфічних критеріїв запропонованих самими моделями.

Як і на попередньому кроці, усі моделі були в однакових умовах – їм було поставлено однаково запитання у новому чаті, щоб попередні відповіді не

повпливали на новий результат. У запиті щодо критеріїв оцінки генеративних моделей було надано повну інформацію щодо того, для чого потрібні ці критерії та стисло пояснено суть дослідження. Запит, як і у випадку із запитаннями, було надано англійською мовою і сформуований він наступним чином: *«I'm doing a research for my diploma on how GAI can help to analyze and generate information security requirements. I ask different GAI models to provide answers on different topics in terms of compliance with ISO27001 (e.g, generate policies, procedures, provide configuration and implementation guidelines, etc). What criteria I can use to evaluate which model did better based on answers generated?»*. Кожна з моделей запропонувала свій перелік критеріїв з поясненнями, що саме мається на увазі під кожним із них. Критерії оцінки від кожної моделі подані у таблицях 2.3-2.5.

Таблиця 2.3 – Критерії оцінювання від GPT 4

| № з/п | Критерій               | Опис/метод оцінювання   |
|-------|------------------------|---|
| 1.    | Accuracy and Relevance | Measure how closely the generated content aligns with ISO 27001 standards. This involves checking if the models provide information that is factually correct and directly applicable to the standard's requirements. |
| 2.    | Completeness           | Evaluate whether the models cover all necessary aspects of the standard. A comprehensive response should include various components like policies, procedures, and guidelines relevant to information security.       |
| 3.    | Consistency            | Assess if the models provide consistent answers across various queries. Consistency is crucial for maintaining standardization in security protocols and documentation.   |

Продовження табл. 2.3

|     |                                   |  |
|-----|-----------------------------------|--|
| 4.  | Clarity and Understandability     | Evaluate the clarity of the generated content. The policies and guidelines should be easy to understand and implement, especially for personnel who might not have deep technical knowledge. |
| 5.  | Practicality and Implementability | Determine how practical and actionable the guidelines and policies are. The suggestions should be feasible to implement within an organizational context.                                    |
| 6.  | Up-to-Date Information            | Ensure that the models provide information that is current and reflects the latest amendments or updates in ISO 27001.   |
| 7.  | Customization and Specificity     | Assess the ability of the models to tailor their responses to specific organizational contexts or unique security needs.   |
| 8.  | Risk Assessment and Management    | Evaluate how effectively the models address risk assessment and management, which are core components of ISO 27001.  |
| 9.  | Scalability and Flexibility       | Check if the models' outputs are scalable and flexible enough to be adapted for different sizes and types of organizations.  |
| 10. | Ethical Considerations and Bias   | Assess the models for any potential ethical issues or biases, especially in terms of data privacy and security.  |
| 11. | Response Time and Efficiency      | Consider how quickly and efficiently the models generate responses, as this can be crucial in operational settings.  |
| 12. | Innovation and Creativity         | While compliance is often about adhering to standards, the ability of the model to offer innovative or improved solutions within the framework of ISO 27001 can also be a valuable trait.    |

Таблиця 2.4 – Критерії оцінювання від Bard

| № з/п | Критерій         | Опис/метод оцінювання  |
|-------|------------------|--|
| 1.    | Relevancy        | Compare the generated requirement to the relevant ISO27001 control or objective. Assess whether the requirement directly addresses the intended security goal and is not redundant or extraneous to the context.   |
| 2.    | Accuracy         | Verify the accuracy of facts, terminology, and consistency with ISO27001 principles. Ensure the requirement is factually accurate, uses proper terminology, and aligns with established ISO27001 guidelines and best practices.  |
| 3.    | Completeness     | Assess whether the generated requirement comprehensively addresses all relevant aspects of the ISO27001 control or objective. Ensure the requirement provides detailed guidance and covers all necessary considerations for effective implementation                         |
| 4.    | Clarity          | Review the language used in the generated requirement for clarity, conciseness, and avoidance of ambiguity or jargon. Ensure the requirement is easily understandable by the intended audience, including information security professionals and non-technical stakeholders. |
| 5.    | Implementability | Consider the resources, expertise, and technology required to implement the generated recommendation. Assess whether the requirement is feasible to implement within the organization's constraints and does not demand unrealistic or impractical measures.                 |

|     |                  |  |
|-----|------------------|--|
| 6.  | Traceability     | Establish a clear connection between the generated requirement and the specific ISO27001 element it addresses. Ensure the requirement is directly traceable to the relevant ISO27001 control or objective, facilitating effective implementation and demonstration of compliance.                      |
| 7.  | Consistency      | Align the generated requirement with the overall security posture and existing security controls. Ensure the requirement is consistent with the organization's established security practices and does not introduce contradictions or conflicts.  |
| 8.  | Effectiveness    | Evaluate the potential impact of the generated requirement on addressing the intended information security risks. Assess whether the requirement effectively mitigates vulnerabilities, enhances security controls, and contributes to overall risk reduction.   |
| 9.  | Efficiency       | Measure the time taken for the GAI model to produce the generated requirements. Assess the computational resources utilized by the model and evaluate its efficiency in generating requirements in a timely manner.  |
| 10. | Generalizability | Test the GAI model's ability to effectively generate requirements for a variety of information security scenarios and apply it to diverse environments. Assess whether the model can produce relevant and implementable requirements across different industries, organizations, and security domains. |



Таблиця 2.5 – Критерії оцінювання від Claude

| № з/п | Критерій                 | Опис/метод оцінювання   |
|-------|--------------------------|---|
| 1.    | Comprehensiveness        | Assess how complete and thorough the policies, procedures, guidelines etc. provided by each model are. Does it cover all necessary controls and address key information security domains? |
| 2.    | Accuracy                 | Fact check the responses. Are the recommendations technically accurate and aligned with good practices for implementing ISO 27001 controls?   |
| 3.    | Relevance                | Evaluate if the model outputs specifically answer the question asked or pertain to the topic at hand, rather than providing generic or tangential information.                            |
| 4.    | Level of Detail          | Check if appropriate levels of detail are provided - not so high-level the output lacks specific guidance but not overly detailed.  |
| 5.    | Customizability          | Assess if the model's responses can be sufficiently tailored to your specific organizational context and security needs.  |
| 6.    | Compliance Depth         | Analyze how deeply and closely the model's outputs map to ISO 27001 requirements and terminology versus providing more general security advice.   |
| 7.    | Implementation Viability | Evaluate if the policies, configuration guidelines etc. can actually be pragmatically implemented and operationalized efficiently.  |

Проаналізувавши запропоновані моделями критерії, можна побачити, що під час визначення критеріїв оцінки між усіма трьома моделями виник консенсус –

кожна модель незалежно запропонувала та неявно визначила пріоритети певних критеріїв (зазначивши їх у певному порядку у списку), які б могли оцінити якість та надійність застосування генеративних моделей штучного інтелекту з метою аналізу вимог інформаційної безпеки. Отож, усі моделі визначили, що наступні критерії є найважливішими для оцінки:

- точність (accuracy) – усі три моделі наголосили на важливості точності у своїх відповідях. Точність, у контексті інформаційної безпеки, відображає здатність моделей надавати відповіді, які точно відповідають фактичній інформації, уникаючи неправильного тлумачення кінцевим користувачем чи виникнення неточностей, що можуть ставити під загрозу надійність згенерованого контенту;
- актуальність (relevance) – актуальність виділялась як ключовий критерій, запропонований GPT-4, Bard і Claude. Моделі продемонстрували, що їхні відповіді повинні відповідати конкретним запитам щодо інформаційної безпеки, тобто цей критерій гарантує, що створений контент відповідає заданому домену чи темі, а також враховує рольовий контекст (який транлюється через запитання від менеджера, консультанта та інженера);
- повнота (completeness) – критерій повноти також відображався у всіх трьох моделях, що підкреслює важливість надання ґрунтовних та вичерпних відповідей. Повнота також вказує на необхідність того, щоб створений контент охоплював усі відповідні аспекти даної теми чи запитання інформаційної безпеки, не залишаючи критичних деталей поза увагою;
- чіткість (clarity) – ще один досить важливий критерій, який вимагає забезпечення того, щоб моделі формулювали відповіді у чіткій і зрозумілій формі, яка можа бути легко сприйнята кінцевим користувачем. Чіткість гарантує, що контент легко інтерпетується та не викликає двозначності;

- можливість реалізації (implementability) – даний критерій був визначений з метою перевірки того, наскільки запропоновані політики, процедури та інструкції щодо налаштування є застосовними у реальних випадках, він зосереджений на здійсненості та практичності перетворення отриманих ідей у дієві заходи зихисту в контексті інформаційної безпеки;
- простежуваність (traceability) – цей критерій підкреслює важливість чіткого зв'язку між згенерованим контентом, стандартом ISO 27001 та іншими найкращими безпековими практиками, адже це і є головною метою даного дослідження. Саме простежуваність допоможе підвищити прозорість, дозволяючи зацікавленим сторонам переконатись, що моделі використовують справді коректні джерела для аналізу вимог та генерування відповідей.

Окрім вищезазначених критеріїв, моделі виділили ще декілька, деякі з яких пересікаються, а деякі – є унікальними. Схожість відповідей різних моделей представлена у таблиці 2.6.

Таблиця 2.6 – Порівняння критеріїв оцінювання запропонованих моделями

| <b>GPT-4</b>                      | <b>Bard</b>      | <b>Claude</b>            |
|-----------------------------------|------------------|--------------------------|
| Accuracy and Relevance            | Relevancy        | Relevance                |
|                                   | Accuracy         | Accuracy                 |
| Completeness                      | Completeness     | Comprehensiveness        |
| Consistency                       | Consistency      | –                        |
| Practicality and Implementability | Implementability | Implementation Viability |
| Up-to-Date Information            | Traceability     | Compliance Depth         |

Продовження табл. 2.6

|                                 |                  |                 |
|---------------------------------|------------------|-----------------|
| Customization and Specificity   | –                | Customizability |
| Risk Assessment and Management  | Effectiveness    | –               |
| Scalability and Flexibility     | Generalizability | –               |
| Ethical Considerations and Bias | –                | –               |
| Response Time and Efficiency    | Efficiency       | –               |
| Innovation and Creativity       | –                | –               |

Окрім визначення самих критеріїв, надзвичайно важливим є встановлення шкал для оцінювання. Це необхідно зробити декількох причин. Перш за все, це необхідно з точки зору стандартизації підходу щодо оцінювання відповідей згенерованих моделями ШІ, адже шкали задають стандартизований набір значень для кожного критерію, що в свою чергу гарантує, що процес оцінювання є послідовним і що різні оцінювачі (експерти) можуть і будуть застосовувати критерії однаково. Ще однією причиною є встановлення чіткості, адже шкала пояснює значення та очікування, пов'язані із кожним критерієм. Це допомагає уникнути двозначності та гарантує, що оцінка є зрозумілою для усіх залучених сторін, і що всі точно розуміють, де межа між «добре» і «дуже добре» чи що означає «3» та «4» в рамках певного критерію. Окрім цього зменшується суб'єктивність у процесі оцінювання, оскільки задається певна структура, від якої не можна відхилитись, щоб забезпечити правильне трактування результатів. Не менш важливим є те, що наявність шкали для оцінювання допомагає легко порівняти відповіді різних

моделей за різними параметрами та визначити, яка з них впоралась краще без складних підрахунків. Також такий підхід значно спрощує документування результатів оцінки. Отож, враховуючи вищезазначені причини, можна точно стверджувати, що наявність шкали для оцінювання згенерованого контенту за критеріями є надзвичайно важливим компонентом для підтримки послідовності, прозорості та об'єктивності протягом усього процесу оцінювання. Це сприяє тому, щоб критерії застосовувались стандартизованим чином, забезпечуючи чесну і надійну оцінку.

Моделі GPT-4, Bard та Claude також запропонували свої шкали для оцінювання, зокрема Bard запропонував бінарну шкалу (0-1), яка є доволі простою для розуміння та використання, проте абсолютно не надає гранулярності, що унеможливорює визначення того, наскільки добра кожна з моделей справилась із поставленими запитаннями, лише підкреслить, чи враховує кожна з них певні критерії, чи ні. Натомість Claude пропонує 10-рівневу модель, яка допоможе досягти досить високого рівня гранулярності, проте це може негативно вплинути на суб'єктивність оцінки, оскільки, як правило, чим більше рівнів, тим більший потенціал до суб'єктивної інтерпретації оцінювачами. Окрім цього, така велика кількість рівнів значно ускладнить саму оцінку, адже для визначення точних балів знадобиться більше часу та зусиль. Тому було прийнято рішення зупинитись на найбільш оптимальному варіанті, запропонованим GPT-4 – 5-рівневій шкалі, яка відображає золоту середину між гранулярністю і простотою у застосуванні, при цьому все ще дозволяючи встановити чіткі межі і розуміння між різними рівнями та їхніми відмінностями.

### **2.3.2 Уніфікація та узгодження критерії та шкал оцінювання генеративних моделей штучного інтелекту**

Критерії для оцінювання згенерованих відповідей моделями ШІ безперечно потребують аналізу, оскільки незважаючи на сумісність деяких з них, серед

запропонованих є і такі, що відрізняються. Метою даного кроку є їх інтеграція та вдосконалення в уніфікований список критеріїв для оцінювання, який би також охоплював аспекти, що можуть бути потенційно цікавими для трьох залучених ролей: менеджера, консультанта та інженера.

Вибір критеріїв відіграє досить важливу роль, оскільки від цього буде залежати точність і надійність оцінки. Під час даного етапу необхідно врахувати умови проведення самого дослідження, узгодити критерії із його цілями, переконатись, що залучені сторони матимуть можливість об'єктивно і справедливо оцінити результат роботи генеративних моделей ШІ, а також, що ці критерії будуть мати значення для зацікавлених сторін під час подальших досліджень у цій сфері. Окрім цього, варто пам'ятати, що основний фокус має бути спрямований на те, наскільки добре модель впоралась і врахуванням вимог інформаційної безпеки, представлених у згаданих міжнародних стандартах та регуляториках.

Як зазначалось у розділі 2.3.1, було обрано 5-рівневу шкалу для оцінки за критеріями. Проте, варто детально описати кожен рівень, аби забезпечити достатню стандартизованість та розмежування між кожним рівнем.

Як результат даного кроку, було сформовано фінальний перелік критеріїв та визначено шкали для їх оцінювання, який представлено у таблиці 2.7.

Таблиця 2.7 – Критерії для оцінки відповідей ГШІ

| № з/п | Критерій | Опис   | Шкала   |
|-------|----------|--|---|
| 1.    | Accuracy | Measures the precision and correctness of generated content in | 5: Exceptionally Accurate - Content aligns precisely with ISO 27001 standard and other relevant regulations, demonstrating a high level of precision and correctness. |

## Продовження табл. 2.7.

|    |           |  |   |
|----|-----------|--|---|
|    |           | <p>alignment with ISO 27001 standard and other relevant regulations. Accuracy ensures that information provided by the models is factually correct and adheres to established principles.</p>                      | <p>4: Very Accurate - Minor inaccuracies, if any, that do not significantly impact the overall correctness of the content.</p> <p>3: Moderately Accurate - Some inaccuracies present, requiring minor corrections to enhance precision.</p> <p>2: Inaccurate - Significant inaccuracies impacting the reliability of the content.</p> <p>1: Highly Inaccurate - Content is largely incorrect and not aligned with ISO 27001 standard or other mentioned regulations.</p>  |
| 2. | Relevance | <p>Evaluates the direct applicability of generated content to ISO 27001 controls and objectives, as well as other relevant requirements, ensuring it addresses the intended security goals without redundancy.</p> | <p>5: Highly Relevant - Content is directly aligned with and essential to ISO 27001 controls and objectives and other relevant requirements, offering precise solutions.</p> <p>4: Very Relevant - Relevant content with minor redundancies or slight deviations from the targeted security goals.</p> <p>3: Moderately Relevant - Some relevancy, but significant gaps or deviations impacting the direct applicability.</p> <p>2: Irrelevant - Content lacks direct applicability to ISO 27001 controls and objectives, and other relevant requirements.</p> <p>1: Highly Irrelevant - Content is entirely unrelated to ISO 27001 and other relevant requirements or to the request itself.</p> |

## Продовження табл. 2.7.

|    |               |   |  |
|----|---------------|---|--|
| 3. | Completeness: | Examines the extent to which the models provide thorough and detailed information, covering all necessary controls, procedures, and guidelines within ISO 27001 and other relevant regulations. | <p>5: Highly Comprehensive - Content is exhaustive, covering all necessary controls and providing detailed information within the topic.</p> <p>4: Very Comprehensive - Thorough coverage with minor omissions or areas that need further detailing.</p> <p>3: Moderately Comprehensive - Some gaps or areas lacking sufficient details, impacting overall completeness.</p> <p>2: Incomplete - Significant omissions and lack of detailed information.</p> <p>1: Highly Incomplete - Content is severely lacking, missing critical information.</p> |
| 4. | Clarity       | Evaluates the clarity and ease of understanding of the generated content, ensuring accessibility for both technical and non-technical stakeholders.   | <p>5: Exceptionally Clear - Content is highly clear, concise, and easily understandable by both technical and non-technical audiences.</p> <p>4: Very Clear - Clear content with minor areas that may require clarification for some stakeholders.</p> <p>3: Moderately Clear - Some sections are unclear, requiring additional explanations for better understanding.</p>   |



## Продовження табл. 2.7.

|    |  |  |   |
|----|--|--|---|
|    |  |  | <p>2: Unclear - Content is often difficult to understand, hindering effective communication.</p> <p>1: Highly Unclear - Content is entirely convoluted and not comprehensible to the intended audience.</p>   |
| 5. | Practical Implementability and Feasibility | Determines the feasibility and practicality of implementing the generated guidelines and policies within the organizational context. | <p>5: Highly Feasible - Guidelines are practical, realistic, and can be easily implemented within the organization's constraints.</p> <p>4: Very Feasible - Feasible with minor adjustments or considerations to enhance practical implementation.</p> <p>3: Moderately Feasible - Some aspects are feasible, but significant challenges or impracticalities exist, which are not defined in the response.</p> <p>2: Impractical - Guidelines are challenging to implement and require major adjustments or changes.</p> <p>1: Highly Impractical - Implementation is nearly impossible due to inherent impracticalities.</p> |

## Продовження табл. 2.7.

|    |   |  |  |
|----|---|--|--|
| 6. | Traceability and Compliance Mapping     | Establishes a clear connection between generated requirements and specific ISO 27001 and other relevant requirements and controls, facilitating effective implementation and compliance demonstration. | <p>5: Highly Traceable - Requirements are directly and clearly traceable to ISO 27001 and other regulations, ensuring seamless compliance mapping.</p> <p>4: Very Traceable - Requirements are traceable with minor efforts, requiring minimal clarification.</p> <p>3: Moderately Traceable - Some elements are traceable, but significant gaps or ambiguities impact traceability.</p> <p>2: Poor Traceability - Traceability is challenging, requiring substantial efforts and clarification.</p> <p>1: Highly Poor Traceability - Requirements are nearly impossible to trace to ISO 27001 or other regulations, hindering compliance mapping.</p> |
| 7. | Customization to Organizational Context | Assesses the ability of the models to tailor responses to specific organizational contexts and unique security needs.  | <p>5: Highly Customizable - Responses are easily adaptable to specific organizational contexts (including those defined in the questions), demonstrating a high level of customization.</p> <p>4: Very Customizable - Customizable with minor adjustments, accommodating diverse organizational needs.</p>   |

Продовження табл. 2.7.

|    |                                 |  |  |
|----|---------------------------------|--|--|
|    |                                 |  | <p>3: Moderately Customizable - Some customization is possible, but significant limitations exist.</p> <p>2: Limited Customizability - Customization is challenging, with substantial restrictions.</p> <p>1: Highly Limited Customizability - Responses are not customizable and lack adaptability to organizational contexts.</p>  |
| 8. | Consistency and Standardization | Assesses if the models consistently provide answers across various queries, maintaining standardization in security protocols and avoiding contradictions. | <p>5: Highly Consistent - Responses are consistent across all queries, demonstrating a high level of standardization, there are no confusing facts or statements in the same response.</p> <p>4: Very Consistent - Generally consistent with minor deviations that do not impact overall standardization.</p> <p>3: Moderately Consistent - Some inconsistencies exist, impacting standardization, including some conflicting statements within the same response.</p> <p>2: Inconsistent - Significant inconsistencies that hinder standardization, several conflicting statements are present.</p> <p>1: Highly Inconsistent - Responses vary widely and lack any form of standardization.</p> |

Ще два критерії, які були вартими уваги, але не потрапили у список – час реагування та ефективність (Response Time and Efficiency), а також зручність використання кінцевим користувачем (Ease of use). Причинами для виключення було те, що не усі експерти безпосередньо були залученні до роботи з моделями, а лише будуть оцінювати згенерований контент, тож вони б не могли оцінити наскільки простими та інтуїтивно зрозумілими для використання є моделі, і тим паче оцінити час, за який кожна з моделей згенерувала кожне запитання. Окрім того, враховуючи стрімкий розвиток даної технології, різниця у часі між згенерованими відповідями майже непомітна для кінцевого користувача, а витрачений час напряму залежить від багатьох факторів, таких як стабільність мережевого з'єднання, комплексність запитання, мова запиту, довжина згенерованого тексту та інших. Врахування цих аспектів значно б ускладнило оцінювання, та не допомогло б напряму досягти мети даного дослідження.

Процес визначення критеріїв перетворився на спільну роботу, яка поєднує людське розуміння з унікальними можливостями генеративних моделей ШІ. Як результат даного етапу, було проаналізовано пропозиції кожної моделі щодо самих критеріїв та шкал для оцінювання. Цей спільний підхід дозволив не тільки використати моделі генеративного штучного інтелекту як об'єкти для дослідження, але й дав змогу активно залучати їх як учасників до визначення важливих параметрів оцінювання їхніх можливостей.

## **2.4 Проведення дослідження та аналіз результатів використання генеративних моделей ШІ з метою аналізу вимог інформаційної безпеки**

### **2.4.1 Проведення експерименту: постановка запитань моделям ШІ**

Усі три моделі – GPT-4, Bard та Claude доступні для кінцевого користувача у вигляді інтерактивного чату, де користувач може задавати свої запитання у

довільному форматі та швидко отримувати на них відповіді. Для того, щоб згенеровані відповіді та результати їх оцінки були об'єктивними і справедливими, під час проведення експерименту для кожної моделі були створені однакові умови, про які вже раніше було згадано у розділі 2.2.3 роботи, зокрема було забезпечено, щоб кожна з моделей отримала ідентичні запитання, які погруповані за трьома ролями (менеджер, консультант та інженер), при чому для кожної ролі створюється новий чат, а запитання ставляться у тому ж самому порядку. Чати в межах кожної моделі для кожної ролі також створювались в однаковому порядку: спочатку для запитань менеджера, потім консультанта і інженера відповідно. Також кожна модель має лише одну спробу для генерації відповіді. Тобто, під час проведення експерименту моделям не надавалась можливість покращити свою першу відповідь, регенерувати її навіть у випадку, якщо відповідь була незавершена тощо. Користувачу, який проводив даний експеримент також не дозволялось обирати чи змінювати запропоновану початкову версію.

Окрім цього, важливо також зазначити, що робота з усіма моделями за усіма ролями проводилась в один день з незначними паузами. Жодних змін до версій моделей чи їх наборів даних не відбувалось впродовж всього дослідження. Даний аспект є досить критичним, оскільки за наявності великої паузи між запитаннями в межах одного чату (за час якої розробники могли б оновити модель до нової версії), модель могла б надавати відповідь на запитання в абсолютно інший спосіб. Необхідність у паузах виникала через те, що деякі моделі мали обмеження щодо кількості запитів за певний проміжок часу, що напряму пов'язано з умовами ліцензування чи пропускнуою спроможністю кожної з них. Жодних додаткових викликів чи труднощів під час проведення експерименту (наприклад збій мережевого з'єднання, вихід з ладу обладнання тощо) не виникало.

Відповіді, надані моделями представлені у додатку Б. Незважаючи на забезпечення однакових умов для усіх моделей, підхід кожної з них до генерування відповідей, формування речень та представлення результатів доволі різний. Одна

модель часто до своїх пояснень прикріплює зображення та надає посилання, інша стисло і чітко дає відповідь на запитання, інша гарно оформлює текст і детально розписує кожен аспект, згаданий у запитанні.

#### **2.4.2 Аналіз відповідей моделей ГШІ за визначеними критеріями**

Після того, як усі моделі згенерували відповіді на запитання визначених ролей, результати їхньої роботи були окремо продубльовані та збережені в окремих файлах відповідно до ролі та моделі. Кожна відповідь отримала свій унікальний ідентифікатор для спрощення подальшої обробки результатів. Окрім цього, важливим нюансом є те, що під час перенесення та збереження результатів, вони були обфусковані. Такі кроки були необхідні з декількох причин. Перш за все, варто було забезпечити цілісність та доступність даних дослідження та попередити можливі проблеми та ризики, пов'язані зі збоєм систем, навмисною чи ненавмисною модифікацією чи видаленням даних, необхідністю у створенні облікових записів для доступу до результатів експертами чи обмеженнями моделей щодо поширення результатів через брак такого функціоналу тощо. Ще однією, мабуть найбільш вагомою причиною, є забезпечення об'єктивності оцінювання. Кожен з експертів уже ймовірно мав досвід використання принаймні однієї із досліджуваних моделей і може мати упереджене (позитивне чи негативне) ставлення до якоїсь із них. Саме тому, доцільно було надати обфусковані відповіді без зазначення назв моделей та будь-яких інших підказок, які б допомогли експерту визначити, яка з моделей надала ту чи іншу відповідь (наприклад скріншотів із систем, використання логотипів тощо). Натомість, експертам були надані файли, де лише є ідентифікатор запитання, згідно із таблицею 2.1, та ідентифікатор відповіді у наступному форматі: GA11-E3, де GA11 – це ідентифікатор моделі, E3 – третє запитання від інженера, згідно із таблицею 2.1. Окрім цього, кожному експерту

було надано форму для оцінювання, де вказані ідентифікатори моделей та питань, критерії, шкали для оцінювання та пояснення рівнів шкали для кожного критерію.

Кожен із залучених експертів повинен ознайомитись із результатами роботи генеративних моделей штучного інтелекту, тобто проаналізувати відповіді на запитання від усіх ролей кожної моделі, та надати свою оцінку за визначеними критеріями за 5-бальною шкалою. Також важливо зазначити, група експертів, залучена до оцінювання ефективності застосування ГШІ для аналізу вимог, складається з трьох осіб, які вже мають досвід роботи у сфері інформаційної безпеки та можуть адекватно оцінити, наскільки добре справились моделі із запитаннями різних рівнів деталізації.

### 2.4.3 Результати експертної оцінки

Ознайомившись із відповідями, згенерованими моделями штучного інтелекту GPT-4, Bard і Claude, та проаналізувавши рівень їх відповідності до заздалегідь визначених критеріїв, експерти виставили свої оцінки за 5-бальною шкалою. Наступним етапом було опрацювання результатів оцінювання відповідей моделей ГШІ наданого кожним експертом.

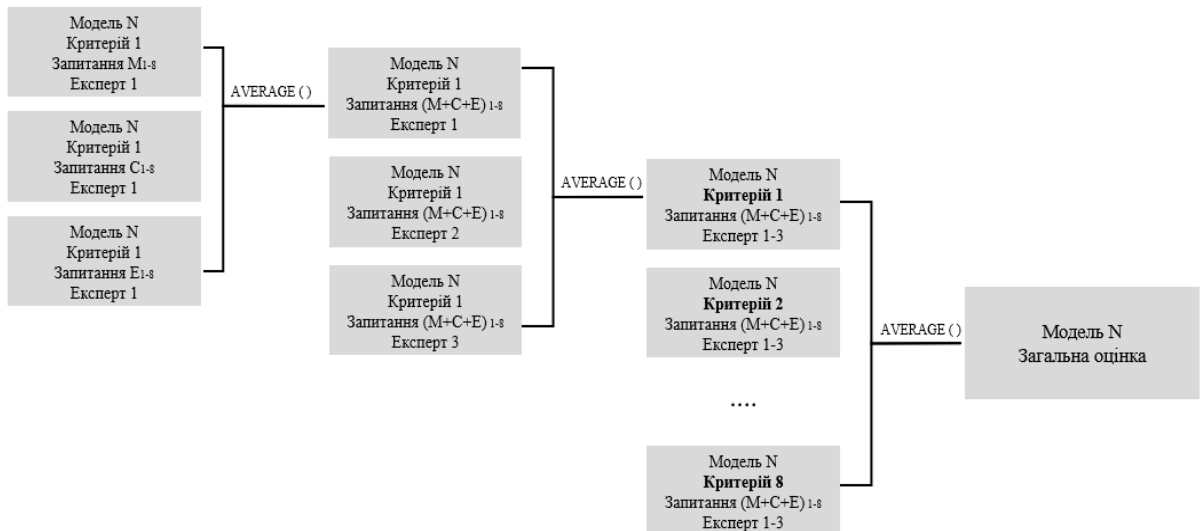


Рисунок 2.1 – Процес оцінювання відповідей ГШІ за критеріями

Під час аналізу результатів оцінювання, було помічено, що в експертів дещо різнилися думки щодо відповідей наданих однією з моделей. Ймовірно причиною такої розбіжності може бути різний досвід експертів у галузі інформаційної безпеки. Проте, щодо більшості запитань експерти зійшлися у своїх поглядах, а іноді оцінки були майже ідентичними, що може свідчити про коректність формулювання критеріїв та умов щодо проведення експерименту.

Для визначення загальної оцінки ефективності застосування моделі було використано обрахунок середнього арифметичного. Перш за все, було зібрано результати оцінювання моделей від кожного експерта. Далі, з використанням формул в Microsoft Excel, було послідовно визначено середню оцінку для кожної моделі від кожного експерта по кожному набору рольових запитань для кожного критерію окремо. Процес підрахунку оцінки представлено на рисунку 2.1.

В результаті даного кроку було визначено, як з моделей впоралась найкраще відповідно до визначених критеріїв, а також обчислено загально оцінку по всіх критеріях для кожної моделі та визначено ту, яка показала найкраще значення. Фінальні оцінки представлені у таблиці 2.8.

Таблиця 2.8 – Результати оцінки моделей ГШІ за критеріями

| <b>Критерій/Модель</b>                            | <b>Bard</b>  | <b>Claude</b> | <b>GPT-4</b> |
|---|--------------|---------------|--------------|
| <b>Accuracy</b>                                   | 4.569        | 4.014         | 4.597        |
| <b>Relevance</b>                                  | 4.597        | 4.167         | 4.528        |
| <b>Completeness</b>                               | 4.139        | 2.583         | 4.250        |
| <b>Clarity</b>                                    | 4.486        | 3.444         | 4.514        |
| <b>Practical Implementability and Feasibility</b> | 4.583        | 3.889         | 4.486        |
| <b>Traceability and Compliance Mapping</b>        | 4.583        | 3.667         | 4.778        |
| <b>Customization to Organizational Context</b>    | 4.389        | 3.569         | 4.292        |
| <b>Consistency and Standardization</b>            | 4.528        | 3.528         | 4.514        |
| <b>Grand Total</b>                                | <b>4.484</b> | <b>3.608</b>  | <b>4.495</b> |



Провівши аналіз даних результатів, можна побачити, що різниця між Bard і GPT-4 складає лише 0,2% і загалом результати є доволі високими відносно 5-ти бальної шкали, що свідчить про явний потенціал та здатність генеративних моделей штучного інтелекту аналізувати вимоги інформаційної безпеки та генерувати корисний контент у даній сфері.

Також, незважаючи на різну архітектуру даних моделей та дати останніх оновлень наборів даних, видно, що різниця між оцінками за кожним окремим критерієм не є надто великою, хоч і чітко можна виділити, яка модель впоралась краще за кожним із них. Проте, варто розуміти, що обчислення методом середнього арифметичного має свої недоліки, які теж можуть впливати на точність і надійність оцінки. Перш за все, даний метод не враховує критичність кожного окремого критерію, для даного методу всі критерії рівні, що може не зовсім відповідати дійсності. Наприклад, бачимо, що GPT-4 гірше впорався із критерієм «Customization of Organization Context», ніж Bard. Проте, якщо б даному критерію було надано більший ваговий коефіцієнт, ніж іншим, підкреслюючи його критичність, то безперечним переможцем у даному експерименті стала б модель Bard. Однак це не єдиний недолік даного методу. Саме тому, аби покращити точність дослідження, варто звернути увагу на рекомендації, представлені у розділі 2.4.4.

Також, отримавши результати оцінювання ефективності моделей відносно визначених критеріїв, було цікаво дізнатись, яка з моделей краще впоралась із запитаннями окремих ролей, що представляли різні рівні деталізації. Процес здійснення такої оцінки представлено на рисунку 2.2.

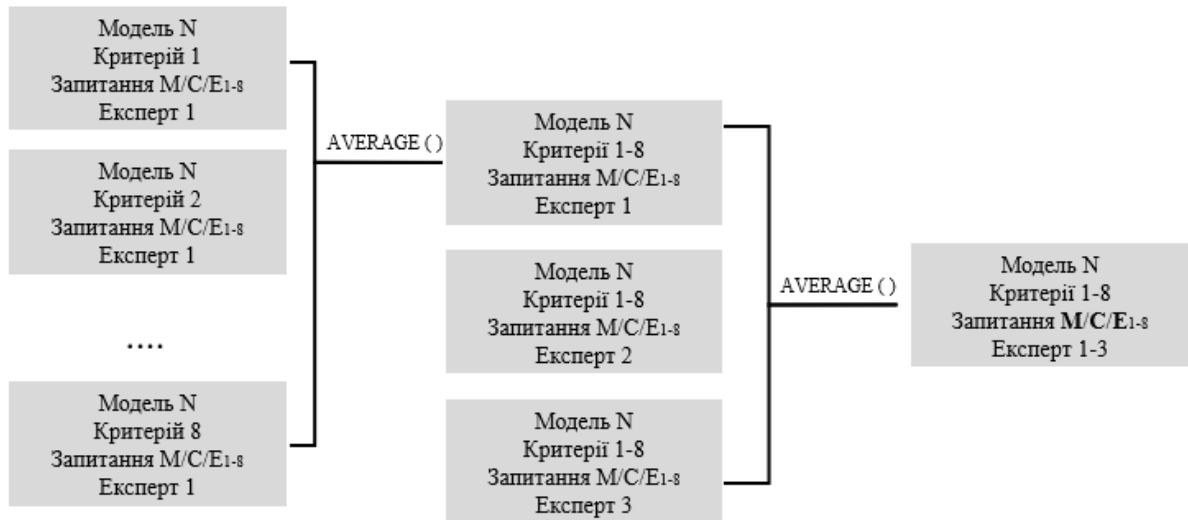


Рис. 2.2 – Процес оцінювання відповідей ГШІ за ролями

Після здійснення обчислень було отримано результати ефективності моделей ГШІ за визначеними ролями, які представлені у таблиця 2.9.

Таблиця 2.9 – Результати оцінки моделей ГШІ за ролями

| Роль/Модель    | Bard  | Claude | GPT-4 |
|----------------|-------|--------|-------|
| Менеджер ІБ    | 4.458 | 3.510  | 4.589 |
| Консультант ІБ | 4.542 | 3.609  | 4.396 |
| Інженер ІБ     | 4.453 | 3.800  | 4.500 |

Отже, відповідно до поданих вище результатів можна побачити, що найкраще покрити запитання щодо процесів, процедур та методологій інформаційної безпеки вдалось Bard, а от технічні запитання та детальні інструкції налаштування систем краще довірити GPT-4. В той же час GPT-4 виявилась більш універсальною моделлю, добре впоравшись із загальними стратегічними питаннями менеджера з невеликим відривом від Bard, яка безсумнівно теж заслуговує на увагу. Щодо Claude, то цій моделі не вдалось себе особливо проявити ні у жодній ролі, ні за якимось із критеріїв.

#### **2.4.4 Рекомендації щодо подальших досліджень у сфері аналізу вимог інформаційної безпеки**

Результати даного дослідження показали, що все ж таки генеративні моделі штучного інтелекту мають потенціал щодо аналізу вимог інформаційної безпеки та добре справляються із розробкою політик, процедур та практичних інструкцій, необхідних для ефективного управління інформаційної безпекою в організації. Тому, для подальших досліджень застосування генеративного штучного інтелекту для аналізу вимог інформаційної безпеки, варто врахувати деякі спостереження та рекомендації.

Перш за все, враховуючи недосконалість методу обчислення за допомогою середнього арифметичного, рекомендується здійснити пріоритизацію критеріїв та надати кожному з них вагові коефіцієнти, щоб підвищити точність оцінювання шляхом відображення важливості критеріїв. Окрім цього, під час підрахунку також варто звернути увагу на досвід та професіоналізм експертів і відобразити це у додаткових коефіцієнтах. Такий зважений підхід гарантуватиме, що критичні критерії матимуть більші значення в загальній оцінці, зменшуючи ризик неточних розрахунків та інших недоліків методу середнього арифметичного.

З метою дослідження застосовності ГШІ для конкретних ролей, варто розробити більш розширений набір запитань, адаптований до обов'язків та операційних задач певної ролі для більш глибокого аналізу ефективності моделей та покрити більше сценаріїв, коли застосування ГШІ могло б спростити виконання завдання для спеціаліста.

Також варто дослідити ефективність моделей у роботі із кількома джерелами вимог інформаційної безпеки одночасно, наприклад розробити запитання, які охоплюють вимоги таких стандартів та регуляторик як ISO/IEC 27001, PCI DSS, GPDR тощо. Цей підхід дозволить оцінити здатність моделей осягати та

синтезувати інформацію із кількох ресурсів одночасно, демонструючи свою універсальність та вміння співставляти подібні вимоги.

Зважаючи на динамічну природу технологій та нормативного законодавства, виникає необхідність у дослідженні ГШІ з точки зору адаптації до змін та оновлення своїх даних, а також створення контенту на основі внесених змін. Таку можливість було б добре оцінити у поєднанні із інтеграцією ГШІ з існуючими системами автоматизації відповідності вимогам. Таким чином вдалось би оцінити наскільки добре моделі можуть сприяти спрощенню підтримки таких систем та розробленого контенту в актуальному стані, забезпечувати постійне вдосконалення, здатність аналізувати зміни та необхідність у внесенні правок до документів організації чи впровадженні додаткових заходів захисту.

## 3 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

### 3.1 Охорона праці

Генеративний штучний інтелект безперечно став шокуючим технологічним відкриттям цього року, надалі захоплюючи свої унікальними можливостями. Проте, більшість користувачів абсолютно не задумуються, який негативний вплив має ця технологія на навколишнє середовище.

Основна проблема полягає у тому, що моделі ГШІ для своєї роботи вимагають величезної кількості енергії. За словами Раві Джайн з Асоціації обчислювальної техніки США (Association for Computing Machinery) обчислювальні вимоги цих моделей є колосальними [18] [19]. Йдеться не лише про кількість комп'ютерів, необхідну для навчання чи використання ГШІ, але і про значну кількість викидів вуглекислого газу в атмосферу, що доповнює і без того значний слід вуглецю, що спричинений використанням цифрових технологій. Зокрема, у США фахівці прогнозують можливе подвоєння чи навіть потроєння споживанні енергії від використання ГШІ в найближче десятиліття. Такий ріст може понести за собою катастрофічні наслідки, оскільки він значно випереджає темпи впровадження відновлюваних джерел енергії.

Кожен етап роботи із технологією ГШІ для створення тексту, зображень, відео та інших типів контенту, вимагають тривалого навчання та аналізу, що потребує величезної кількості електроенергії, яка також необхідна і для використання моделей кінцевими користувачами. Оскільки розміри та складність цих моделей зростають, відповідно зростає і необхідність у додатковій витраті енергії, що призводить до збільшення кількості вуглецевих викидів.

Розробники таких великих моделей як ChatGPT, Bard та Claude для розгортання цих моделей використовують великі хмарні центри обробки даних, які в останні роки зосереджуються на тому, аби зробити їх максимально

відмовостійкими, використовуючи більше джерел відновлюваної енергії. Проте, через глобальне використання таких ресурсів, хмарні обчислення все ще залишають помітний вуглецевий слід, показники якого швидко зростають, адже суспільство все більше покладається на цифрові технології.

За даними дослідження «Energy and policy considerations for deep learning in NLP» [20], опублікованого Університетом Массачусетса, навчання однієї моделі може викидати 626 000 фунтів еквівалента вуглекислого газу, що в п'ять разів перевищує викиди середньостатистичного автомобіля за весь термін використання. Цікаву статистику також демонструє дослідження Університету Корнелл щодо споживання енергії моделями ГШІ під час генерації тексту чи зображень. Відповідно до цього дослідження, для створення лише декількох зображень, ГШІ споживає стільки енергії, скільки необхідно для повної зарядки сучасного смартфона. На жаль, користувачі не задумуються над тим, скільки енергії потрібно для генерації зображення, адже роблять це здебільшого для розваг чи щоб протестувати здібності моделі у сфері графічного дизайну. Дослідники підрахували, що залежно від розміру зображення, результат створення кожного з них може виробляти від 0,1 до 0,5 грама вуглекислого газу. Щодо генерації тексту, то цей процес потребує значно меншої кількості енергії, а отже, нижчий рівень викидів вуглецю (від 0,002 до 0,015 грамів залежно від моделі) [21].

Окрім цього, ГШІ додає свій вклад у забруднення навколишнього середовища через швидку експлуатацію апаратного забезпечення. Йдеться про те, що ГШІ не лише вимагає багато пристроїв для своєї роботи, але й прискорює цикл їх заміни, що призводить до збільшення електронних відходів. Карен Панетта, представниця Інституту інженерів з електротехніки та електроніки (Institute of Electrical and Electronics Engineers (IEEE)), наголошує на недостатніх ресурсах для переробки чипів та комп'ютерних елементів, вкотре нагадуючи про зростаючу проблему електронних відходів.

Проте, бажання організацій та технічних лідерів бути попереду та опановувати нові технології для розширення свого бізнесу, як правило, переважає над думкою про те, який вплив має генеративний штучний інтелект на навколишнє середовище чи виконання операційних задач персоналом. Така ситуація також спричинена тим, що наразі використання ГШІ чітко юридично не врегульовано. Проте, відповідно до вимог локального законодавства, компанії зобов'язані дотримуватись законів щодо охорони праці [23] та навколишнього середовища [24], забезпечуючи відповідальне використання ГШІ та інших цифрових технологій у своїй діяльності. Зокрема, компанії мають запровадити відповідні внутрішні правила, які б регулювали використання ГШІ в межах компанії, враховуючи використання енергозберігаючих приладів та методів обчислення, використання послуг постачальників, які пропонують відновлювані джерела електроенергії, застосування у своїй роботі вже існуючих моделей ГШІ замість створення і навчання нових, проведення тренінгів та навчальних кампаній, які б стимулювали працівників розсудливо використовувати ГШІ для виконання своїх завдань, враховуючи не лише вплив на навколишнє середовище та взаємодію між різними членами команди, але і інші ризики, які стосуються етичних аспектів, інформаційної безпеки та прав інтелектуальної власності.

Щодо даного дослідження, то було забезпечено, щоб воно проводилось відповідно до вимог щодо безпеки та захист здоров'я під час роботи з екранними пристроями [22], а також відповідно до статті 13 Закону України «Про охорону праці»[23]. Зокрема, для проведення дослідження було організовано робоче місце таким чином, щоб усі елементи робочого місця та їх розташування відповідали ергономічним, антропологічним та іншим вимогам, а також характеру виконуваних робіт. Було використано два екрани із матовим покриттям із відрегульованим рівнем яскравості та кутом нахилу для спрощення обробки великих масивів тексту, що є необхідним для виконання дослідження. Окрім цього, враховуючи фізіологічні потреби виконавця, було встановлено підставку під ноутбук, щоб уникнути втоми

рук. Підставка також передбачає додаткове охолодження пристрою, що попереджає утворення надлишкового тепла та знижує ймовірність виходу з ладу пристрою. Після закінчення роботи пристрої були вимкнені та відключені від мережі, аби уникнути можливих аварійних ситуацій, які можуть статись внаслідок перегріву пристрою, короткого замикання, можливого доступу третіх сторін до пристрою чи необережного поводження при виконанні інших задач, що непов'язані напряду із виконанням дослідження. Також, із врахуванням вимог, описаних у Законі України «Про охорону навколишнього природного середовища» [23], для проведення дослідження було використано вже наявні моделі штучного інтелекту, а не новостворені, аби не витратити додаткових обчислювальних та енергетичних ресурсів на розробку та навчання цих моделей, що могло б мати значний негативний вплив на забруднення навколишнього середовища вуглецевими викидами. Окрім цього, мета та завдання дослідження не передбачали генерацію унікальних зображень, що теж могло б вплинути на кількість небезпечних викидів, оскільки моделі генерували лише текст.

### **3.2 Безпека в надзвичайних ситуаціях**

В умовах сьогодення, зокрема під час складних геополітичних конфліктів, забезпечення надійного функціонування цифрових технологій в надзвичайних ситуаціях (НС), в тому числі генеративного штучного інтелекту, стає важливим кроком на шляху до забезпечення цивільного захисту (ЦЗ) населення – одного із найпріоритетніших завдань держави [25].

За останні роки технології стали одночасно і засобом боротьби, і вектором атаки, адже за наявності розуміння принципів роботи певних інформаційних систем, їх вразливостей та слабких налаштувань безпеки, виникає загроза щодо експлуатації цих систем зловмисниками з метою завдання збитків, крадіжки



конфіденційних даних чи унеможливлення використання сервісів. Якравим прикладом є нещодавна кібератака на мережу оператора зв'язку «Київстар», в результаті якої без мобільного зв'язку та інтернету залишились 24 мільйони абонентів [26][27], в той час, коли надзвичайно важливо бути в курсі новин та розуміти, що відбувається, адже країна потерпає від повномасштабного російського вторгнення.

Проте, в епоху, коли роль штучного інтелекту в діяльності організацій по всьому світу стає дедалі важливішою, зростає і необхідність забезпечення того, що інфраструктура, яка лежить в основні цих систем, є такою ж надійною та безпечною, як і самі алгоритми. Завдання забезпечення того, щоб штучний інтелект продовжував працювати в умовах надзвичайних ситуацій виходить за межі програмного забезпечення та стосується фізичних активів, у яких розміщені ці інтелектуальні системи. Основою надійності штучного інтелекту в надзвичайних ситуаціях є відмовостійка та якісна інфраструктура. Зокрема це стосується центрів обробки даних та забезпечення того, що вони розроблені відповідно вимог локального та міжнародного законодавства [28][29][30] та є стійкими до стихійних лих, відключень електроенергії та інших непередбачуваних подій. Потужність такої інфраструктури також має вирішальне значення. Вона повинна бути масштабованою, щоб справлятися із раптовими сплесками потреб в обробці даних, які можуть виникати під час надзвичайних ситуацій. Така характеристика гарантуватиме, що системи штучного інтелекту зможуть продовжувати ефективно функціонування навіть в умовах підвищеного навантаження.

Ще одним критично важливим аспектом для забезпечення безперервності функціонування є впровадження резервних ресурсів. Завдяки наявності кількох територіально розподілених центрів обробки даних і каналів зв'язку, ризик повної відмови системи значно знижується. Таким чином, у випадку, коли один з центрів було пошкоджено внаслідок стихійного лиха чи ракетної атаки, інші центри можуть взяти на себе роботу без перерви в обслуговуванні. Також наявність резервних

ресурсів має поширюватись і на джерела живлення, системи охолодження та мережеві канали.

Варто також пам'ятати і про захист самих моделей ІІІ. Оскільки ІІІ відіграє важливу роль у прийнятті рішень, моделі стають цілями для кібезагроз, саме тому потрібно врахувати кілька рівнів захисту:

- захист від DdoS атак – даний тип атак спрямований на спричинення відмови в обслуговуванні системою, що може мати значний негативний вплив, адже системи стануть недоступними в критичні моменти. Надійні системи проти DDoS та правильне налаштування мережевих фільтрів є надважливими для того, щоб ІІІ, чи системи на основі ІІІ продовжували працювати за будь-яких умов;
- обмеження того, хто може отримати доступ до моделей ІІІ та за яких умов може мати вирішальне значення. Даний захід передбачає сувору автентифікацію та протоколи авторизації, що гарантуватиме, що лише авторизований персонал може взаємодіяти з системами ІІІ;
- захист від зломисного програмного забезпечення – системи ІІІ, як і будь-які інші інформаційні системи, вразливі до зломисного програмного забезпечення. Ефективні антивірусні системи, регулярна оцінка та сканування вразливостей, а також оперативне встановлення оновлення програмного забезпечення та компонентів є критично важливими для захисту систем ІІІ від зломисних атак;
- окрім захисту систем ІІІ від зовнішніх загроз, забезпечення цілісності та конфіденційності даних, які вони обробляють є пріоритетним завданням. Це передбачає впровадження надійних методів шифрування під час зберігання та передачі даних, створення резервних копій даних, регулярні перевірки та дотримання правил захисту даних.

Щоб переконатись, що згадані вище заходи захисту та забезпечення безперервності функціонування працюють належним чином, потрібно проводити регулярні тестування та навчання на випадок надзвичайних ситуацій. Згідно з начальним посібником «Техноекологія та цивільна безпека. Частина «Цивільна безпека»» [31], «одним із основним завдань ЦЗ, які визначені Кодексом цивільного захисту України, є підготовка і перепідготовка керівного складу Цивільного захисту, його органів управління та сил, навчання населення вмінню застосовувати засоби індивідуального захисту і діяти в НС». Ці тренування та тестування повинні моделювати різні сценарії катастроф чи непередбачуваних ситуацій, щоб оцінити стійкість систем ШІ та інфраструктури, що їх підтримує. Тестування також допомагає виявляти вразливі місця та є рушієм постійного вдосконалення.

Отже, забезпечення того, щоб системи штучного інтелекту не вийшли з ладу в надзвичайних ситуаціях – це багаторівневе завдання, яке охоплює широкий діапазон від стійкості та потужності фізичної інфраструктури до передових заходів кібербезпеки. Це вимагає цілісного підходу, який враховує кожен аспект системи. Оскільки компанії все глибше вбудовують штучний інтелект у свої процеси, то реагування на надзвичайні ситуації, імперативи стійкості інфраструктури, безпеки та постійного тестування стають не просто технологічними вимогами, а й обов'язком суспільства.

## ВИСНОВКИ

Дана кваліфікаційна робота описує проведення дослідження щодо застосування потенціалу моделей генеративного штучного інтелекту, зокрема GPT-4, Bard та Claude, для аналізу вимог інформаційної безпеки. Дослідження розпочалось із огляду технології генеративного штучного інтелекту в цілому, ретельному аналізу та вибору моделей ГШІ, що дало основу для подальшого експерименту. Наступний крок передбачав визначення та встановлення ролей – менеджера, консультанта та інженера інформаційної безпеки, які відіграють важливу роль у формулюванні індивідуальних питань, дозволяючи перевірити, наскільки добре можуть впоратись моделі покриваючи різні аспекти інформаційної безпеки. Далі дослідження розгортається завдяки спільним зусиллям у визначенні та вдосконаленні критеріїв для оцінки згенерованих відповідей, поєднуючи критичне мислення людини із надзвичайними можливостями ГШІ. Такий підхід забезпечує створення багатогранного та вичерпного списку критеріїв, які допомогли найбільш повно проаналізувати роботу моделей. Окрім цього, також було визначено 5-рівневу шкалу із детальним описом кожного рівня відповідно до заданого критерію, що допомогло зробити процес оцінки об'єктивним та стандартизованим.

Наступний етап дослідження відображає безпосередньо проведення експерименту. Зокрема було забезпечено, щоб кожна із моделей знаходилась в однакових умовах, які детально описані у даній роботі. Після того, як кожна з моделей згенерувала відповіді на рольові запитання, результати роботи ГШІ було обфусковано та передано для аналізу та оцінки експертам у сфері інформаційної безпеки. Отримавши результати оцінки усіх згенерованих відповідей відповідно до критеріїв, було обраховано загальні оцінки ефективності моделей за визначеними критеріями та за ролями, а також фінальну оцінку. У заключному підрозділі представлено ключові спостереження та рекомендації щодо подальших досліджень.

Дане дослідження являє собою важливий внесок у динамічний та прогресуючий ландшафт інформаційної безпеки. Взаємодія генеративних моделей штучного інтелекту із величезним набором даних, включаючи вимоги інформаційної безпеки, а також зростаючий вектор кіберзагроз та появу нових технологій, закликає дослідників, практиків, спеціалістів з інформаційної безпеки та інших зацікавлених сторін використовувати потенціал генеративного штучного інтелекту для підвищення ефективності активностей пов'язаних із впровадженням, підтримкою та постійним вдосконалення інформаційної безпеки в організаціях.

## ПЕРЕЛІК ПОСИЛАНЬ

1. SOC 2, HIPAA, ISO 27001, PCI, and GDPR Compliance Automation. *Vanta*. URL: <https://www.vanta.com/> (дата звернення: 01.12.2023).
2. ELEKS Compliance Automation Platform. *ELEKS: Enterprise Software Development, Technology Consulting*. URL: <https://eleks.com/compliance-automation-platform/> (дата звернення: 01.12.2023).
3. McGill J. How many AI tools are there?. *Content at Scale*. URL: <https://contentatscale.ai/blog/how-many-ai-tools-are-there/> (дата звернення: 03.12.2023).
4. The EU Artificial Intelligence Act : від 14.06.2023 р. : станом на 9 груд. 2023 р. URL: <https://www.artificial-intelligence-act.com/> (дата звернення: 23.11.2023).
5. EU AI Act: first regulation on artificial intelligence | News | European Parliament. *European Parliament News*. URL: <https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence> (дата звернення: 23.11.2023).
6. Bommasani R., Klyman K., Zhang D. Do Foundation Model Providers Comply with the Draft EU AI Act?. *Stanford CRFM*. URL: <https://crfm.stanford.edu/2023/06/15/eu-ai-act.html> (дата звернення: 24.11.2023).
7. Bateni N., Dara R. Automated generation of privacy policy using deep models. м. Ontario, 28 жовт. 2021 р. URL: <https://ieeexplore.ieee.org/document/9629155> (дата звернення: 01.12.2023).
8. Panukhnyk O. Artificial intelligence in the educational process and scientific research of higher education applicants: responsible boundaries of AI content. *Galic'kij ekonomičnij visnik*. 2023. Т. 83, № 4. С. 202—211. URL: <https://elartu.tntu.edu.ua/handle/lib/42652> (дата звернення: 22.12.2023).
9. Mashliy G., Mosiy O., Pelcher M. Information provided for labor relationship management as compositional social responsibility of enterprises. *Galic'kij*

- ekonomičnij visnik*. 2019. Т. 57, № 2. С. 80—89.  
URL: <https://elartu.tntu.edu.ua/handle/lib/27963> (дата звернення: 22.12.2023).
10. Skibska K. The use of artificial intelligence tools in recruitment. *Galic'kij ekonomičnij visnik*. 2023. Т. 83, № 4. С. 114—121. URL: <https://elartu.tntu.edu.ua/handle/lib/42641> (дата звернення: 22.12.2023).
11. Щигельська Г. О., Джадав Х. Еволюція у сфері живопису, створеного штучним інтелектом. *Збірник тез III Міжнародної науково-практичної конференції молодих учених та студентів „Філософські виміри техніки“*. Тернопіль, 2022. С. 33—35. URL: <https://elartu.tntu.edu.ua/handle/lib/39678> (дата звернення: 30.11.2023).
12. ChatGPT. *OpenAI*. URL: <https://openai.com/chatgpt> (дата звернення: 02.12.2023).
13. Поширені запитання про Bard. *Bard Експеримент*.  
URL: <https://bard.google.com/faq?hl=uk> (дата звернення: 02.12.2023).
14. Meet Claude. *Anthropic*. URL: <https://www.anthropic.com/product> (дата звернення: 02.12.2023).
15. AI21 Studio. *AI21 Labs*. URL: <https://www.ai21.com/studio> (дата звернення: 02.12.2023).
16. BLOOM. *Hugging Face — The AI community building the future*. URL: [https://huggingface.co/docs/transformers/model\\_doc/bloom](https://huggingface.co/docs/transformers/model_doc/bloom) (дата звернення: 02.12.2023).
17. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection Information security management systems - Requirements. На заміну ISO/IEC 27001:2013/Cor.2015 ; чинний від 2022-10-25. Вид. офіц. 2022. 19 с.  
URL: <https://www.iso.org/standard/27001> (дата звернення: 05.12.2023).
18. Pratt M. K. Generative AI's sustainability problems explained | TechTarget. *TechTarget*.  
URL: <https://www.techtarget.com/sustainability/feature/Generative-AIs-sustainability-problems-explained> (дата звернення: 07.12.2023).

19. The development, deployment, and use of generative ai technologies. *Association for Computing Machinery*. URL: <https://www.acm.org/binaries/content/assets/public-policy/ustpc-approved-generative-ai-principles> (дата звернення: 07.12.2023).
20. Strubell E., Ganesh A., McCallum A. Energy and Policy Considerations for Modern Deep Learning Research. *Proceedings of the AAAI Conference on Artificial Intelligence*. 2020. Т. 34, № 09. С. 13693—13696.  
URL: <https://doi.org/10.1609/aaai.v34i09.7123> (дата звернення: 08.12.2023).
21. Luccioni A. S., Jernite Y., Strubell E. Power hungry processing: watts driving the cost of AI deployment?. 2023. С. 5—6.  
URL: <https://doi.org/10.48550/arXiv.2311.16863> (дата звернення: 08.12.2023).
22. Про затвердження Вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями : Наказ М-ва соц. політики України від 14.02.2018 р. № 207. URL: <https://zakon.rada.gov.ua/laws/show/z0508-18#Text> (дата звернення: 07.12.2023).
23. Про охорону праці : Закон України від 14.10.1992 р. № 2694-ХІІ : станом на 1 жовт. 2023 р. URL: <https://zakon.rada.gov.ua/laws/show/2694-12#Text> (дата звернення: 07.12.2023).
24. Про охорону навколишнього природного середовища : Закон України від 25.06.1991 р. № 1264-ХІІ : станом на 8 жовт. 2023 р.  
URL: <https://zakon.rada.gov.ua/laws/show/1264-12#Text> (дата звернення: 07.12.2023).
25. Кодекс цивільного захисту України : Кодекс України від 02.10.2012 р. № 5403-VI : станом на 27 листоп. 2023 р. URL: <https://zakon.rada.gov.ua/laws/show/5403-17#Text> (дата звернення: 07.12.2023).
26. Учасники проєктів Вікімедіа. Кібератака на «Київстар» (2023) — Вікіпедія. *Вікіпедія*. 2023.  
URL: [https://uk.wikipedia.org/wiki/Кібератака\\_на\\_«Київстар»\\_\(2023\)](https://uk.wikipedia.org/wiki/Кібератака_на_«Київстар»_(2023)) (дата звернення: 11.12.2023).



27. "Київстар" не працює. Що сталося і чи можна обійти проблему - BBC News Україна. *BBC News Україна*.  
URL: <https://www.bbc.com/ukrainian/articles/cz92xrkklwro> (дата звернення: 12.12.2023).
28. ISO 22301:2019. ISO 22301:2019 Security and resilience Business continuity management systems - Requirements. На заміну ISO 22301:2012 ; чинний від 2019-10-30. Вид. офіц. 2019. 21 с.  
URL: <https://www.iso.org/standard/75106.html> (дата звернення: 11.12.2023).
29. The NIS 2 Directive : від 14.12.2022 р. URL: <https://www.nis-2-directive.com/> (дата звернення: 11.12.2023).
30. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР : станом на 1 лип. 2022 р.  
URL: <https://zakon.rada.gov.ua/laws/show/80/94-вр#Text> (дата звернення: 22.12.2023).
31. Стручок В. С. Техноекоелогія та цивільна безпека. Частина «Цивільна безпека». Навчальний посібник. Тернопіль : Тернопільський національний технічний університет імені Івана Пулюя, 2022. 150 с.  
URL: <https://elartu.tntu.edu.ua/handle/lib/39424>.

**ДОДАТКИ**

**ДОДАТОК А**

---

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ТЕРНОПЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ  
УНІВЕРСИТЕТ ІМЕНІ ІВАНА ПУЛЮЯ**

**МАТЕРІАЛИ**

**XI НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ**

**«ІНФОРМАЦІЙНІ МОДЕЛІ,  
СИСТЕМИ ТА ТЕХНОЛОГІЇ»**



**13-14 грудня 2023 року**

**ТЕРНОПЛЬ  
2023**

УДК 004.056:342.9

Олена Сміх, Руслан Козак, к.т.н., доцент

Тернопільський національний технічний університет імені Івана Пулюя

## АНАЛІЗ МОЖЛИВОСТЕЙ ПЛАТФОРМ GAI ДЛЯ ГЕНЕРУВАННЯ ВИМОГ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Olena Smikh, Ruslan Kozak Ph.D., Assoc. Prof.

### ANALYSIS OF THE CAPABILITIES OF GAI PLATFORMS FOR GENERATING INFORMATION SECURITY REQUIREMENTS

Інтеграція генеративного штучного інтелекту (ГШІ) (Generative Artificial Intelligence, GAI) у процес розробки програмного забезпечення привносить не лише інновації, але й дає можливість революціонізувати визначення та формулювання вимог безпеки.

Перший у світі проект регламенту щодо застосування ШІ було запропоновано у ЄС у червні 2023 року, який отримав назву EU Artificial Intelligence Act (AIA) [1]. Проект регламенту розподіляє ШІ на три різні категорії залежно від ризику, що його ШІ може становити для людей: неприйнятний ризик, високий ризик і обмежений ризик.

Відповідність моделей GAI до EU AIA було проаналізовано в [2]. Зокрема, двадцять дві вимоги акту були прокласифіковані, і з них було обрано 12 вимог, які розділені між 4 різними категоріями. Понад 90% серед доступних GAI платформ базуються на популярних моделях [3], зокрема, на GPT 3.5.

У дослідженні для з'ясування типів, особливостей та ризиків застосування ГШІ проаналізовано такі GAI платформи: ChatGPT, Bard, Claude, AI21 Studio, BLOOM. Методику проведення порівняльного аналізу згідно критеріїв, запропонованих в [2], та структуру результатів дослідження представлено у вигляді наступних таблиць:

| № | Платформа       | Готовність до застосування | Дата оновлення наборів даних | Відповідність до EU Artificial Intelligence Act (AIA) |             |       |            | Загальна оцінка |
|---|-----------------|----------------------------|------------------------------|---|-------------|-------|------------|-----------------|
|   |                 |                            |                              | Data  | Compute     | Model | Deployment |                 |
|   | Платформа       | ChatGPT                    | Bard                         | Claude  | AI21 Studio | BLOOM |            |                 |
|   | Загальна оцінка | 29                         | 32                           | 10  | 11          | 39    |            |                 |

Оцінки для кожної із 4 категорій щодо відповідності до AIA були визначені на основі результатів аналізу GAI платформ. З метою вибору платформи GAI для генерації вимог інформаційної безпеки до програмного забезпечення, аналіз здійснено не лише на основі технічних характеристик платформ, але й з врахуванням ризиків, етичних аспектів та вимог правового регулювання.

#### Література

1. Regulating generative AI. Towards Data Science. [Електронний ресурс]/ Sweenor, D – 4 серпня 2023 – Режим доступу до ресурсу: <https://towardsdatascience.com/regulating-generative-ai-e8b22525d71a>
2. EU AI Act. [Електронний ресурс]/ Center for Responsible AI at Stanford University – 15 червня 2023 – Режим доступу до ресурсу: <https://crfm.stanford.edu/2023/06/15/eu-ai-act.html>
3. Announcing AI21 Studio and Jurassic-1. [Електронний ресурс]/ AI21 Labs – 7 червня 2023 – Режим доступу до ресурсу: <https://www.ai21.com/blog/announcing-ai21-studio-and-jurassic-1>

## ДОДАТОК Б

Таблиця Б.1 – Відповідність ідентифікаторів моделей до їх назв

| Ідентифікатор | Назва моделі |
|---------------|--------------|
| GAI1          | Bard         |
| GAI2          | Claude       |
| GAI3          | ChatGPT      |

### Generated responses by GAI1 Model for Manager role

**M1:** Could you please advise which security frameworks should EU-based software development company with 500 employees follow?

**GAI1-M1:**

Choosing the right security framework for your EU-based software development company with 500 employees depends on several factors, including:

1. Industry and Compliance Requirements:

- **General Data Protection Regulation (GDPR):** If your company handles personal data of EU citizens, you must comply with GDPR. Frameworks like ISO 27001 and NIST Cybersecurity Framework can help you achieve compliance.
- **eIDAS Regulation:** If you offer trust services like e-signatures or electronic identification, you might need to comply with eIDAS. The ENISA Trusted Cloud Services Scheme (TCSS) may be relevant.
- **Industry-specific regulations:** Certain industries have specific security requirements. For instance, healthcare companies need to comply with HIPAA, and financial institutions need to comply with PCI DSS.

2. Company size and resources:

- **Scalability:** Choose a framework that can grow with your company.
- **Resource constraints:** Smaller companies might benefit from lighter frameworks like CIS Controls or NIST Cybersecurity Framework.

3. Existing security posture:

- **Conduct a risk assessment:** Identify your security vulnerabilities and prioritize risks based on their potential impact.
- **Align your framework with your risk assessment:** Choose a framework that addresses your identified risks.

#### 4. Certification goals:

- If you seek third-party certification: Choose a framework that is recognized and accredited by relevant bodies.

Here are some recommended security frameworks for EU-based software development companies:

1. ISO 27001: A comprehensive framework for information security management systems (ISMS). It provides a systematic approach to identifying, managing, and mitigating security risks.
2. NIST Cybersecurity Framework: A US government framework that provides a flexible and prioritized approach to managing cybersecurity risks. It is readily adaptable to different industries and company sizes.
3. CIS Controls: A prioritized set of actions for mitigating the most prevalent cyber threats. It is a good starting point for smaller companies or those with limited resources.
4. ENISA Trusted Cloud Services Scheme (TCSS): A European scheme for certifying cloud service providers that comply with specific security standards.
5. OWASP Top 10: A list of the top 10 web application security risks. It provides guidance on how to prevent these risks in your software development lifecycle.

In addition to implementing a framework, consider these best practices:

- Security awareness training: Educate your employees about cybersecurity threats and best practices.
- Secure coding practices: Develop secure software by following established coding standards and guidelines.
- Vulnerability scanning and penetration testing: Regularly identify and address vulnerabilities in your software and systems.
- Incident response planning: Plan and prepare for how to respond to security incidents.

Additional resources:

- ENISA - Advancing Software Security in the EU:  
<https://www.enisa.europa.eu/publications/advancing-software-security-through-the-eu-certification-framework>
- CBI - The European market potential for software development services:  
<https://www.cbi.eu/market-information/outsourcing-itobpo/software-development-services/market-potential>

Remember, choosing the right security framework is an ongoing process. Regularly review your needs and adapt your approach as necessary.

**M2:** How organizational structure of EU-based software development company with 500 employees should look like to manage security risks effectively?

**GAI1-M2:**

There's no one-size-fits-all answer to the ideal organizational structure for an EU-based software development company with 500 employees for managing security risks effectively. However, considering your company size and the importance of data protection in the EU, here are some possible options:

## 1. Centralized Security Team:

- Pros: Strong central control over security policies, procedures, and resources. Efficient utilization of expertise and resources. Easier to maintain consistency and compliance.
- Cons: Potential bottleneck for decision-making. Risk of disconnect from development teams and specific project needs. Increased workload for the central team.

## 2. Hybrid Model:

- Combines a centralized security team with dedicated security specialists embedded within development teams.
- Pros: Balances central control with team-specific focus. Faster response to risks and improved understanding of team needs. Stronger collaboration between security and development teams.
- Cons: Requires careful coordination and communication between central and embedded teams. Potential for inconsistencies in implementation across teams. Increased complexity in managing resources and expertise.

## 3. Decentralized Security Champions:

- Empowers development teams to manage their own security with guidance from dedicated security champions.
- Pros: Faster decision-making and ownership within teams. Promotes security awareness and responsibility among developers.
- Cons: Requires thorough training and resources for champions. Risk of inconsistent security practices across teams. Potential lack of expertise in highly specialized security areas.

Additional factors to consider:

- Company culture: Choose a structure that aligns with your existing culture and fosters collaboration between security and development teams.
- Industry and technology: Specific security needs of your industry and the complexity of your technology might influence the required level of expertise and centralized control.
- Growth plans: Consider scalability as your company grows. Will the chosen structure adapt efficiently to increasing staff and complexity?

Regardless of the chosen structure, ensure to implement these elements for effective security risk management:

- Clear roles and responsibilities: Define who owns different security aspects within the structure.
- Regular communication and collaboration: Foster open communication between security and development teams.
- Security awareness training: Train all employees on security best practices and relevant regulations.
- Continuous monitoring and improvement: Regularly assess your security posture and adapt your structure as needed.

Ultimately, the best organizational structure will depend on your specific needs and priorities. Consider experimenting with different approaches and analyzing their effectiveness to find the optimal fit for your EU-based software development company.

Remember, it's crucial to involve a qualified security professional in designing and implementing your chosen organizational structure to ensure it adheres to relevant regulations and effectively manages security risks.

**M3:** Please develop Access Control Policy based on ISO 27001 to ensure the security and privacy of company systems and data.

### **GAI1-M3:**

#### Access Control Policy

##### 1. Purpose

This Access Control Policy (ACP) outlines the principles and procedures for managing access to company systems and data, ensuring their security and privacy. It aligns with the ISO 27001 standard and aims to:

- Grant authorized users access to the resources they need to perform their job duties.
- Prevent unauthorized access to systems and data.
- Protect sensitive and confidential information.
- Maintain accountability for all access activities.

##### 2. Scope

This policy applies to all personnel of the company, including employees, contractors, consultants, and temporary workers. It covers all company systems and data, regardless of their location or format.

##### 3. Definitions

- Access Control: A set of rules that determine who can access which resources and under what conditions.
- Authentication: The process of verifying the identity of a user.
- Authorization: The process of granting a user permission to access a specific resource.

- Confidential Information: Information that is not publicly known and must be protected from unauthorized disclosure.
- Sensitive Information: Information that could cause harm to the company or its stakeholders if it were to be disclosed.
- System: Any hardware, software, firmware, or combination thereof that processes or stores data.

#### 4. Access Control Principles

- Least privilege: Users should only be granted the minimum level of access required to perform their job duties.
- Need-to-know: Access to sensitive information should be restricted to those who have a legitimate business need to know.
- Separation of duties: Critical tasks should be separated to prevent any single individual from having complete control over a process.
- Accountability: All access activities should be logged and monitored to identify and address any suspicious behavior.

#### 5. Access Control Procedures

- User accounts: All users must have a unique identifier and password to access company systems.
- Password requirements: Passwords must be complex and changed regularly.
- Multi-factor authentication: Multi-factor authentication should be used for accessing sensitive systems and data.
- Access control lists: Access control lists (ACLs) should be used to define who can access specific resources and what actions they can perform.
- Data encryption: Sensitive data should be encrypted at rest and in transit.
- Data access logs: Data access logs should be maintained and monitored for suspicious activity.
- Regular reviews: Access privileges should be reviewed regularly to ensure they are still valid.
- Access termination: Access to company systems and data should be terminated when a user leaves the company.

#### 6. Roles and Responsibilities

- IT Security Officer: Responsible for overseeing the implementation and enforcement of this policy.
- System administrators: Responsible for managing user accounts and access controls for the systems they administer.
- Data owners: Responsible for classifying data and ensuring that it is protected appropriately.



- All employees: Responsible for protecting their own credentials and reporting any suspected security incidents.

## 7. Training and Awareness

All employees will receive training on this policy and their roles and responsibilities in protecting company systems and data.

## 8. Non-compliance

Non-compliance with this policy will result in disciplinary action, up to and including termination of employment.

## 9. Review and Updates

This policy will be reviewed and updated regularly to reflect changes in the organization's security needs and best practices.

## 10. References

- ISO 27001:2022 Information technology — Security techniques — Information security management systems — Requirements
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations

Note: This is a sample Access Control Policy based on ISO 27001 and may need to be adapted to meet the specific needs of your organization. You should consult with a qualified security professional to ensure that your policy is effective and meets all applicable legal and regulatory requirements.

**M4:** Please develop Encryption Policy that adheres to the encryption requirements of ISO 27001 to protect sensitive data.

### **GAI1-M4:**

#### Encryption Policy

##### 1. Purpose

This Encryption Policy outlines the principles and procedures for the use of encryption to protect sensitive data, adhering to the encryption requirements of ISO 27001. This policy aims to:

- Ensure the confidentiality and integrity of sensitive data at rest and in transit.
- Prevent unauthorized access to sensitive data.
- Minimize the risk of data breaches and other security incidents.
- Comply with all applicable legal and regulatory requirements.

##### 2. Scope

This policy applies to all company personnel, including employees, contractors, consultants, and temporary workers. It covers all sensitive data stored, processed, or transmitted on company systems and devices, regardless of their location or format.

### 3. Definitions

- Encryption: The process of transforming plaintext data into ciphertext using an algorithm and a key.
- Cryptography: The science and practice of secure communication in the presence of adversaries.
- Data at rest: Data that is stored on a storage device, such as a hard drive or a USB drive.
- Data in transit: Data that is being transmitted over a network.
- Sensitive data: Data that is confidential, personally identifiable, or otherwise sensitive in nature.
- Encryption key: A secret piece of information used to encrypt and decrypt data.

### 4. Encryption Requirements

- All sensitive data must be encrypted at rest using a FIPS-validated encryption algorithm and a minimum key length of 256 bits.
- All sensitive data in transit must be encrypted using a FIPS-validated encryption algorithm and a secure transport protocol, such as TLS/SSL.
- Encryption keys must be stored and managed securely.
- All employees must be trained on the proper use of encryption.

### 5. Encryption Implementation

- The IT Security team will be responsible for implementing and maintaining the encryption infrastructure.
- The Data Classification Policy will be used to identify sensitive data.
- Encryption solutions will be chosen based on the type of data being protected and the security requirements.
- Encryption keys will be stored in a secure key management system.
- Regular testing and assessments will be conducted to ensure the effectiveness of the encryption controls.

### 6. Roles and Responsibilities

- IT Security Officer: Responsible for overseeing the implementation and enforcement of this policy.
- System administrators: Responsible for implementing and maintaining encryption controls on the systems they administer.
- Data owners: Responsible for classifying data and ensuring that it is encrypted appropriately.

- All employees: Responsible for protecting their encryption keys and reporting any suspected security incidents.

## 7. Training and Awareness

All employees will receive training on this policy and their roles and responsibilities in protecting sensitive data using encryption.

## 8. Monitoring and Auditing

The encryption controls will be monitored and audited regularly to ensure that they are effective and that they are being implemented correctly.

## 9. Non-compliance

Non-compliance with this policy will result in disciplinary action, up to and including termination of employment.

## 10. Review and Updates

This policy will be reviewed and updated annually to reflect changes in the organization's security needs and best practices.

## 11. References

- ISO 27001:2022 Information technology — Security techniques — Information security management systems — Requirements
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations
- National Institute of Standards and Technology (NIST) Special Publication 800-63B: Digital Identity Guidelines

Note: This is a sample Encryption Policy that adheres to the encryption requirements of ISO 27001 and may need to be adapted to meet the specific needs of your organization. You should consult with a qualified security professional to ensure that your policy is effective and meets all applicable legal and regulatory requirements.

**M5:** Please develop an Information Security Risk Management Policy in accordance with ISO 27001 aimed at effective security risk identification, management, and treatment.

### **GAI1-M5:**

#### Information Security Risk Management Policy

##### 1. Purpose

This Information Security Risk Management Policy (ISRM Policy) outlines the principles and procedures for identifying, assessing, and managing information security risks in accordance with ISO 27001. This policy aims to:

- Effectively identify and assess information security risks.

- Implement appropriate controls to mitigate identified risks.
- Continuously monitor and improve the effectiveness of the information security risk management process.
- Ensure compliance with relevant legal and regulatory requirements.

## 2. Scope

This policy applies to all company personnel, including employees, contractors, consultants, and temporary workers. It covers all information assets and systems owned, operated, or used by the company, regardless of their location or format.

## 3. Definitions

- Information security risk: The potential for a threat to exploit a vulnerability and cause harm to information assets.
- Threat: A potential source of harm to information assets.
- Vulnerability: A weakness in an information asset or system that can be exploited by a threat.
- Risk assessment: The process of identifying, analyzing, and evaluating information security risks.
- Risk treatment: The process of selecting and implementing controls to mitigate identified risks.
- Information asset: Any information that has value to the organization.
- Information security control: A safeguard or countermeasure that is put in place to protect information assets from threats and vulnerabilities.

## 4. Risk Management Framework

The company will adopt a risk management framework that is consistent with ISO 27001 and includes the following steps:

- Risk identification: Identifying potential threats and vulnerabilities that could impact information assets.
- Risk assessment: Analyzing the likelihood and impact of identified risks.
- Risk treatment: Selecting and implementing appropriate controls to mitigate identified risks.
- Risk monitoring: Continuously monitoring the effectiveness of risk controls and updating the risk management process as needed.

## 5. Risk Management Procedures

- Risk assessments will be conducted regularly at least annually or whenever there are significant changes to the organization's environment or information systems.
- Risk assessments will be conducted by a team of qualified individuals with expertise in information security risk management.
- Risks will be prioritized based on their likelihood and impact.

- Appropriate controls will be selected and implemented to mitigate identified risks.
- The effectiveness of risk controls will be monitored and reviewed regularly.
- Information security incidents will be investigated and reported to the appropriate authorities.
- Lessons learned from information security incidents will be used to improve the effectiveness of the information security risk management process.

## 6. Roles and Responsibilities

- IT Security Officer: Responsible for overseeing the implementation and enforcement of this policy.
- Risk Management Team: Responsible for conducting risk assessments and implementing risk treatment plans.
- System administrators: Responsible for implementing and maintaining controls on the systems they administer.
- Data owners: Responsible for classifying data and ensuring that appropriate controls are in place to protect it.
- All employees: Responsible for reporting potential information security risks and complying with security policies and procedures.

## 7. Training and Awareness

All employees will receive training on information security risks and their responsibilities in protecting information assets.

## 8. Non-compliance

Non-compliance with this policy will result in disciplinary action, up to and including termination of employment.

## 9. Review and Updates

This policy will be reviewed and updated annually to reflect changes in the organization's security needs and best practices.

## 10. References

- ISO 27001:2022 Information technology — Security techniques — Information security management systems — Requirements
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations
- National Institute of Standards and Technology (NIST) Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments  
(<http://www.jsebs.org/jsebs/index.php/jsebs/article/view/210>)

Note: This is a sample Information Security Risk Management Policy that is in accordance with ISO 27001 and may need to be adapted to meet the specific needs of your organization. You should consult

with a qualified security professional to ensure that your policy is effective and meets all applicable legal and regulatory requirements.

**M6:** Please develop Secure Software Development Lifecycle Policy as per ISO 27001 requirements ensuring the security of software throughout the development lifecycle.

### **GAI1-M6:**

#### Secure Software Development Lifecycle Policy (SSDLC Policy)

##### 1. Purpose

This Secure Software Development Lifecycle (SSDLC) Policy outlines the principles and procedures for developing secure software, ensuring compliance with ISO 27001 requirements. This policy aims to:

- Integrate security throughout the entire software development lifecycle (SDLC).
- Identify and address security vulnerabilities early in the development process.
- Develop secure and reliable software that meets all relevant security requirements.
- Continuously improve the effectiveness of the secure software development process.

##### 2. Scope

This policy applies to all software developed or acquired by the company. It covers all stages of the SDLC, from planning and design to deployment and maintenance.

##### 3. Definitions

- Secure software development lifecycle (SSDLC): A framework for developing software that incorporates security considerations throughout the entire process.
- Security requirement: A specific security need that the software must meet.
- Security vulnerability: A weakness in software that could be exploited by an attacker.
- Security control: A safeguard or countermeasure that is put in place to protect software from vulnerabilities.
- Threat: A potential source of harm to software.

##### 4. SSDLC Phases and Activities

The following phases and activities are included in the company's SSDLC:

###### 1. Planning and Design:

- Identify security requirements.
- Define security architecture.
- Develop security test plans.

## 2. Development:

- Implement secure coding practices.
- Conduct static code analysis.
- Perform vulnerability scanning.
- Conduct penetration testing.

## 3. Testing and Integration:

- Perform functional testing.
- Perform security testing.
- Integrate security controls.

## 4. Deployment and Maintenance:

- Deploy software securely.
- Monitor and update software for security vulnerabilities.
- Respond to security incidents.

## 5. Security Requirements Management

- All security requirements will be documented and maintained in a central repository.
- Security requirements will be reviewed and updated regularly.
- Security requirements will be communicated to all developers and stakeholders.

## 6. Secure Coding Practices

- Developers will use secure coding practices to prevent common vulnerabilities.
- Developers will use secure coding libraries and frameworks.
- Developers will receive training on secure coding practices.

## 7. Vulnerability Management

- The company will use vulnerability scanning and penetration testing tools to identify vulnerabilities in software.
- The company will prioritize and fix vulnerabilities based on their severity and impact.
- The company will track and report on the status of vulnerability remediation efforts.

## 8. Security Incident Response

- The company will have a plan for responding to security incidents.
- The plan will include procedures for identifying, containing, and recovering from security incidents.
- The company will train employees on the security incident response plan.

## 9. Training and Awareness

- All developers and stakeholders will receive training on the SSDLC policy and secure coding practices.
- The training will be tailored to the specific roles and responsibilities of participants.

## 10. Non-compliance

Non-compliance with this policy will result in disciplinary action, up to and including termination of employment.

## 11. Review and Updates

This policy will be reviewed and updated annually to reflect changes in the organization's security needs and best practices.

## 12. References

- ISO 27001:2022 Information technology — Security techniques — Information security management systems — Requirements
- National Institute of Standards and Technology (NIST) Special Publication 800-64B: Developing Secure Software
- Open Web Application Security Project (OWASP) Top 10

Note: This is a sample SSDLC Policy that is in accordance with ISO 27001 requirements and may need to be adapted to meet the specific needs of your organization. You should consult with a qualified security professional to ensure that your policy is effective and meets all applicable legal and regulatory requirements.

**M7:** Could you please develop Security Awareness and Training Policy in accordance with ISO 27001 to raise awareness about information security among employees?

### **GAI1-M7:**

#### Security Awareness and Training Policy

##### 1. Purpose

This Security Awareness and Training Policy outlines the principles and procedures for raising awareness about information security among employees, aligning with ISO 27001 requirements. This policy aims to:

- Educate employees about information security threats and vulnerabilities.
- Promote a culture of security awareness within the company.
- Empower employees to protect information assets.
- Reduce the risk of information security incidents.

##### 2. Scope



This policy applies to all employees of the company, including full-time, part-time, and temporary employees.

### 3. Definitions

- Information security: The protection of information from unauthorized access, use, disclosure, disruption, modification, or destruction.
- Information security awareness: The understanding of information security risks and the ability to take appropriate measures to protect information assets.
- Information security training: The process of providing employees with the knowledge and skills they need to protect information assets.
- Information asset: Any information that has value to the organization.

### 4. Security Awareness and Training Program

The company will develop and implement a comprehensive security awareness and training program that includes the following components:

- New employee training: All new employees will receive security awareness training as part of their onboarding process.
- Annual security awareness training: All employees will receive annual security awareness training that covers current threats and best practices.
- Role-based training: Specific training will be provided to employees based on their roles and responsibilities.
- Phishing simulations: The company will conduct regular phishing simulations to test employees' ability to identify and avoid phishing attacks.
- Security awareness campaigns: The company will conduct regular security awareness campaigns to promote a culture of security.

### 5. Content of Security Awareness and Training

Security awareness and training will cover the following topics:

- General information security concepts
- Company's security policies and procedures
- Identification of information security threats and vulnerabilities
- Best practices for protecting information assets
- Reporting information security incidents

### 6. Roles and Responsibilities

- IT Security Officer: Responsible for overseeing the implementation and enforcement of this policy.

- Human Resources Department: Responsible for coordinating security awareness and training for new employees.
- Management: Responsible for promoting a culture of security awareness within their departments.
- All employees: Responsible for participating in security awareness and training programs and following the company's security policies and procedures.

## 7. Evaluation and Improvement

The effectiveness of the security awareness and training program will be evaluated regularly. The program will be updated as needed to reflect changes in the organization's security needs and best practices.

## 8. Non-compliance

Non-compliance with this policy will result in disciplinary action, up to and including termination of employment.

## 9. References

- ISO 27001:2022 Information technology — Security techniques — Information security management systems — Requirements
- National Institute of Standards and Technology (NIST) Special Publication 800-50 Revision 1: The Security Awareness Training and Education Program

Note: This is a sample Security Awareness and Training Policy that is in accordance with ISO 27001 requirements and may need to be adapted to meet the specific needs of your organization. You should consult with a qualified security professional to ensure that your policy is effective and meets all applicable legal and regulatory requirements.

**M8:** What regulations should be followed in case our EU-based company provides software development services for client in California, who requires us to work with personal data?

### **GAI1-M8:**

When your EU-based software development company provides services for a client in California and handles personal data, you need to comply with both EU and California regulations:

EU Regulations:

- General Data Protection Regulation (GDPR): Applies to the processing of personal data of individuals located in the EU, regardless of the data controller's location. This means you must comply with GDPR even if your company is located outside the EU.
- EU-US Privacy Shield: Although currently invalidated by the Court of Justice of the European Union (CJEU), it still serves as a reference point for data transfers between the EU and the US. You may need to consider alternative legal bases for data transfers, such as Standard Contractual Clauses (SCCs).

### California Regulations:

- California Consumer Privacy Act (CCPA): Grants California residents certain rights over their personal data, including access, deletion, and portability.
- California Privacy Rights Act (CPRA): Amends and expands the CCPA, giving consumers more control over their data and creating additional requirements for businesses.

Here are some key requirements to consider:

- Data minimization: Only collect and process the minimum amount of personal data necessary for the intended purpose.
- Transparency and notice: Provide clear and concise information about your data practices to individuals whose data you collect.
- Individual rights: Respect individuals' rights to access, correct, delete, and restrict the processing of their personal data.
- Data security: Implement appropriate security measures to protect personal data from unauthorized access, use, disclosure, alteration, or destruction.
- Data breach notification: Notify individuals and relevant authorities in case of a data breach.
- Cross-border data transfers: Ensure that any transfer of personal data from the EU to California complies with relevant legal requirements.

Additional resources:

- European Commission - General Data Protection Regulation (GDPR): <https://gdpr.eu/>
- California Attorney General - California Privacy Rights Act (CPRA): <https://oag.ca.gov/privacy/ccpa>
- International Association of Privacy Professionals (IAPP): <https://iapp.org/>

It's important to consult with a qualified legal expert to ensure your company complies with all applicable regulations and protects the privacy of individuals' data.

## Generated responses by GAI1 Model for Consultant role

**C1:** Which security policies should be developed for EU-based software development company with 500 employees based on ISO27001?

### **GAI1-C1:**

Security Policy Recommendations for an EU-Based Software Development Company with 500 Employees based on ISO 27001

#### 1. Introduction and Scope

This document establishes the security policy for [Company Name], an EU-based software development company with 500 employees. This policy outlines the company's commitment to protecting its information assets, including sensitive data, intellectual property, and critical infrastructure.

## 2. Policy Objectives

This policy aims to achieve the following objectives:

- **Confidentiality:** Ensure that information assets are only accessible to authorized individuals and systems.
- **Integrity:** Protect information assets from unauthorized modification or destruction.
- **Availability:** Ensure that information assets are available to authorized users when needed.
- **Compliance:** Comply with all applicable data protection regulations, including EU General Data Protection Regulation (GDPR).

## 3. Security Roles and Responsibilities

- **Management:** Management is responsible for providing leadership and support for the information security program.
- **IT Security Officer:** The IT Security Officer is responsible for developing, implementing, and maintaining the information security program.
- **Information Asset Owners:** Information asset owners are responsible for identifying, classifying, and protecting their information assets.
- **Employees:** All employees are responsible for following the company's security policies and procedures.

## 4. Security Policies and Procedures

- **Access Control:** Implement access control measures to restrict access to information assets based on the principle of least privilege.
- **Data Security:** Classify information assets based on their sensitivity and implement appropriate security controls to protect them.
- **Password Management:** Implement strong password policies and procedures.
- **Incident Management:** Establish an incident response plan to identify, contain, and recover from security incidents.
- **Risk Management:** Identify, assess, and mitigate information security risks.
- **Third-Party Security:** Implement security controls to manage risks associated with third-party vendors.
- **Compliance:** Ensure compliance with all applicable data protection regulations.

## 5. Security Awareness and Training

- Provide all employees with security awareness and training on a regular basis.
- Tailor training to specific roles and responsibilities.

#### 6. Continuous Improvement

- Regularly review and update the information security program to ensure its effectiveness.
- Conduct periodic risk assessments and security audits.

#### 7. ISO 27001 Alignment

This policy is designed to be aligned with the ISO 27001 standard for information security management systems. Implementing an ISO 27001-compliant information security program will help the company to achieve its security objectives and demonstrate its commitment to information security.

#### 8. Communication and Reporting

- Communicate the information security policy to all employees.
- Report security incidents to the IT Security Officer and management.

#### 9. Enforcement

- The company will enforce this policy through disciplinary action.
- Violations of the policy will be investigated and may result in disciplinary action, up to and including termination of employment.

#### Additional Considerations for Ukraine

Due to the current conflict in Ukraine, the company should take additional security measures to protect its information assets from cyberattacks and other threats. These measures may include:

- Implementing additional security controls to protect sensitive data, such as encryption and multi-factor authentication.
- Increasing the frequency of security backups and ensuring that backups are stored in a secure location.
- Monitoring systems and networks for suspicious activity.
- Developing a plan for business continuity and disaster recovery.

By implementing these recommendations, the company can develop a comprehensive and effective security program that meets the requirements of ISO 27001 and protects its information assets from a range of threats.

Please note: This is a general recommendation and may need to be adapted based on the specific needs of the company. It is important to consult with a qualified information security expert to develop a tailored security program.

**C2:** Could you please develop Statement of Applicability for ISO27001 for EU-based software development company with 500 employees?

**GAI1-C2:**

## Statement of Applicability (SoA) for ISO 27001

Company Name: [Company Name] Address: [Company Address] Date: 2023-12-09

**1. Introduction**

This Statement of Applicability (SoA) defines the scope of the information security management system (ISMS) implemented by [Company Name] based on the ISO 27001 standard. This document identifies the controls and processes included in the ISMS and excludes those deemed not relevant to the company's context and risk profile.

**2. Scope of the ISMS**

The ISMS applies to all information assets owned, processed, or stored by [Company Name], including:

- Information Technology (IT) Systems: Servers, workstations, network devices, cloud services, and applications.
- Software Assets: Source code, documentation, and intellectual property.
- Data: Financial records, customer data, employee data, and other sensitive information.

The ISMS excludes the following:

- Personal data of employees: This data is managed and protected under the EU General Data Protection Regulation (GDPR) and other relevant regulations.
- Physical security of buildings and facilities: This aspect is managed by a separate system and procedures.

**3. Relevant ISO 27001 Annex A Controls**

The following Annex A controls from ISO 27001 are implemented as part of the ISMS:

- A.5.1.1 Security policy: Establishes the organization's commitment to information security.
- A.5.2.1 Asset management: Identifies, classifies, and protects information assets.
- A.5.2.2 Information access control: Restricts access to information assets based on the principle of least privilege.
- A.5.2.3 Cryptographic controls: Protects sensitive information using encryption.
- A.5.3.1 Security awareness and training: Educates employees on information security risks and procedures.
- A.5.3.2 Incident management: Identifies, contains, and recovers from security incidents.
- A.5.3.3 Business continuity and disaster recovery: Ensures the continuity of critical business processes in the event of a disaster.
- A.6.1.2 Identification of risks and opportunities: Assesses risks and opportunities relating to information security.

- A.6.1.3 Risk assessment: Analyzes risks and determines appropriate risk treatment methods.
- A.6.1.4 Risk treatment: Implements controls to mitigate identified risks.
- A.8.1.3 Legal and regulatory requirements: Complies with all applicable data protection regulations.
- A.9.1 Monitoring, measurement, analysis, and evaluation: Monitors the performance of the ISMS and identifies areas for improvement.
- A.9.3 Internal audit: Conducts internal audits to assess the effectiveness of the ISMS.
- A.10.1 Continual improvement: Continuously improves the ISMS.

#### 4. Justification for Exclusions

The following controls from Annex A are not implemented as part of the ISMS:

- A.7.2.1 Secure coding practices: These practices are addressed through the company's software development lifecycle (SDLC) processes.
- A.12.1 Compliance obligations: Compliance with specific regulations is addressed through separate policies and procedures.

These exclusions are justified due to the following reasons:

- The controls are addressed through other existing and effective measures.
- The controls are not relevant to the company's context and risk profile.

#### 5. Review and Approval

This SoA will be reviewed and updated periodically to reflect changes in the company's business and risk profile. The SoA is approved by the senior management of [Company Name].

#### 6. Signatures

Approved by:

- Name: [Name of CEO or Managing Director]
- Title: CEO or Managing Director
- Date: 2023-12-09

Prepared by:

- Name: [Name of Information Security Officer]
- Title: Information Security Officer
- Date: 2023-12-09

Note:

This SoA is a template and should be adapted to reflect the specific circumstances of the company. It is important to consult with a qualified information security expert to develop a tailored SoA.

**C3:** Develop a procedure on how to implement access controls in accordance with ISO27001 within the EU-based software development company.

### **GAI1-C3:**

#### Procedure for Implementing Access Controls in Accordance with ISO 27001

##### 1. Purpose

This procedure outlines the steps for implementing access controls in accordance with ISO 27001 within the EU-based software development company. Effective access controls are essential for protecting sensitive information and ensuring compliance with relevant regulations, including the General Data Protection Regulation (GDPR).

##### 2. Scope

This procedure applies to all employees, contractors, and other third-party users who access the company's information systems and resources.

##### 3. Roles and Responsibilities

- **Information Security Officer (ISO):** Responsible for developing and maintaining the access control policy, reviewing and approving access requests, and conducting periodic access reviews.
- **IT Department:** Responsible for implementing and managing access controls, including user provisioning, deprovisioning, and password management.
- **Information Asset Owners (IAOs):** Responsible for identifying and classifying information assets, determining appropriate access levels, and recommending access control measures.
- **System Administrators:** Responsible for configuring access controls on specific systems and applications.
- **All Users:** Responsible for using their access privileges responsibly and protecting their credentials.

##### 4. Steps

###### 4.1. Identify and Classify Information Assets

- Conduct an information asset inventory to identify all sensitive information assets.
- Classify information assets based on their sensitivity level, using a predefined classification scheme (e.g., confidential, internal use only).

###### 4.2. Define Access Levels

- Define different access levels based on the principle of least privilege, granting users only the minimum access required to perform their job duties.
- Examples of access levels: Read-only, Read/Write, Full Access.



#### 4.3. Implement Access Control Mechanisms

- Implement appropriate access control mechanisms based on the sensitivity level of the information asset and the user's access level.
- Examples of access control mechanisms: User authentication, password management, access control lists (ACLs), role-based access control (RBAC), multi-factor authentication (MFA).

#### 4.4. Manage User Access Requests

- Establish a process for requesting and approving user access.
- The process should include:
  - User submitting a formal access request.
  - IAO reviewing the request and recommending appropriate access level.
  - ISO approving or denying the request.
  - IT Department provisioning or deprovisioning access.

#### 4.5. Conduct Periodic Access Reviews

- Regularly review user access privileges to ensure they remain appropriate and necessary.
- Reviews should happen at least annually or whenever there is a change in job duties or role.

#### 4.6. Monitor and Audit Access Activity

- Monitor and audit access activity to detect and investigate unauthorized access attempts and suspicious activity.
- Logs should be reviewed regularly by authorized personnel.

#### 4.7. Train Users

- Provide all users with regular training on access control policies and procedures.
- Training should cover topics such as:
  - Importance of access controls.
  - User responsibilities for protecting their credentials.
  - How to report suspicious activity.

#### 4.8. Reporting and Escalation

- Establish a process for reporting and escalating security incidents related to access controls.
- Incidents should be reported immediately to the ISO and IT Department.

#### 5. Documentation

- Document all access control policies, procedures, and processes.
- Documentation should be readily available to all users.

## 6. Continuous Improvement

- Regularly review and update access control policies and procedures to ensure they remain effective and compliant with ISO 27001 and relevant regulations.

## 7. Compliance with EU Regulations

- Implement additional access controls and procedures to comply with relevant EU regulations, such as the GDPR.
- Ensure that user access is limited to personal data only as necessary for their job function.
- Implement procedures for responding to data subject requests, such as access requests and erasure requests.

## 8. References

- ISO 27001: Information technology - Security techniques - Information security management systems - Requirements.
- General Data Protection Regulation (GDPR)

Note: This is a sample procedure and may need to be adapted based on the specific needs of the company. It is important to consult with a qualified information security expert to develop a tailored access control program.

**C4:** Could you please create a detailed guideline on what should be done in order to implement Encryption policy in accordance with ISO27001 within EU-based software development company?

### **GAII-C4:**

#### Detailed Guideline for Implementing Encryption Policy in Accordance with ISO 27001

##### 1. Introduction

This guideline provides detailed instructions for implementing an encryption policy within an EU-based software development company in accordance with the ISO 27001 Information Security Management System (ISMS) standard.

##### 2. Objectives

- Protect sensitive information from unauthorized access, disclosure, modification, or destruction.
- Ensure compliance with relevant regulations, including the EU General Data Protection Regulation (GDPR).
- Enhance trust and confidence among stakeholders by demonstrating a commitment to data security.

##### 3. Scope

This policy applies to all encryption activities within the company, including:

- Encryption of data at rest and in transit.

- Use of cryptographic keys and key management practices.
- Secure disposal of cryptographic materials.
- Encryption of communications channels.
- Encryption of software applications and components.

#### 4. Roles and Responsibilities

- Information Security Officer (ISO): Oversees the development, implementation, and maintenance of the encryption policy.
- IT Security Team: Responsible for implementing and managing encryption solutions.
- Information Asset Owners (IAOs): Identify sensitive information assets and recommend appropriate encryption controls.
- System Administrators: Configure and maintain encryption systems.
- All Users: Utilize encryption solutions according to the policy guidelines.

#### 5. Policy Contents

##### 5.1. Encryption Standards and Algorithms

- Define the approved encryption standards and algorithms to be used within the company.
- Consider factors like:
  - Security strength of the algorithms.
  - Compatibility with existing systems and applications.
  - Compliance with industry standards and regulations.

##### 5.2. Encryption Key Management

- Establish procedures for the secure generation, storage, distribution, and destruction of cryptographic keys.
- Implement key management best practices, including:
  - Separation of duties for key management functions.
  - Use of Hardware Security Modules (HSMs) for key storage.
  - Regular key rotation and backups.

##### 5.3. Data at Rest and in Transit Encryption

- Define the types of data that must be encrypted at rest and in transit.
- Implement appropriate encryption solutions for different types of data.
- For example:
  - Full disk encryption for laptops and desktops.

- Database encryption for sensitive data stored in databases.
- Secure sockets layer (SSL) or Transport Layer Security (TLS) encryption for web applications.

#### 5.4. Secure Disposal of Cryptographic Materials

- Establish procedures for the secure disposal of cryptographic materials, including:
  - Overwriting or degaussing magnetic media.
  - Shredding or burning paper documents.
  - Securely erasing data from electronic devices.

#### 5.5. Encryption of Communications Channels

- All communications channels transmitting sensitive information should be encrypted.
- Examples of technologies to be considered:
  - Virtual Private Networks (VPNs) for secure remote access.
  - Secure email messaging services.

#### 5.6. Encryption of Software Applications and Components

- Implement encryption for sensitive parts of software applications and components to protect them from unauthorized access and modification.
- Techniques include:
  - Code signing and verification.
  - Secure development practices.

#### 5.7. User Training and Awareness

- Provide regular training and awareness programs to all employees on the importance of encryption and how to use encryption solutions effectively.

#### 5.8. Monitoring and Auditing

- Regularly monitor and audit encryption systems and activities to ensure they meet policy requirements.
- Address any identified weaknesses or vulnerabilities promptly.

#### 5.9. Continuous Improvement

- Review and update the encryption policy regularly to reflect changes in technology, threats, and regulations.
- Conduct periodic risk assessments to identify new encryption needs.

### 6. Compliance with EU Regulations

- Ensure compliance with relevant EU regulations, such as the GDPR, which require appropriate data protection measures, including encryption.
- Pay particular attention to the encryption of personal data and the use of encryption for data transfers outside the European Union.

## 7. References

- ISO 27001: Information technology - Security techniques - Information security management systems - Requirements.
- General Data Protection Regulation (GDPR)
- National Institute of Standards and Technology (NIST) Special Publication 800-53: Revision 5, Recommendation for Security Controls for Federal Information Systems and Organizations

## 8. Conclusion

Implementing a comprehensive encryption policy is essential for protecting sensitive information, ensuring compliance with relevant regulations, and building trust among stakeholders. By following this guideline and tailoring it to the specific needs of your company, you can establish a robust encryption program that meets the requirements of ISO 27001 and safeguards your valuable data assets.

**C5:** Please develop a detailed procedure on how to assess risks in accordance with ISO27001 at EU-based software development company, what scales should be used to define risk levels and provide several examples of how risk register should look like?

### **GAI1-C5:**

Detailed Procedure for Risk Assessment in Accordance with ISO 27001:

#### 1. Introduction:

This procedure outlines the steps for conducting a risk assessment in accordance with ISO 27001 within an EU-based software development company. Risk assessment is a critical component of the Information Security Management System (ISMS) and helps identify, analyze, and prioritize potential threats and vulnerabilities that could impact information assets.

#### 2. Objectives:

- Identify and assess information security risks.
- Determine the likelihood and potential impact of each risk.
- Develop risk treatment plans to mitigate identified risks.
- Ensure compliance with ISO 27001 and relevant regulations.

#### 3. Scope:

This procedure applies to all information assets of the company, including:

- IT systems and applications
- Data
- Software assets
- Intellectual property
- Physical assets

#### 4. Roles and Responsibilities:

- Information Security Officer (ISO): Oversees the risk assessment process and ensures it complies with ISO 27001.
- Risk Assessment Team: Conducts the risk assessment and prepares the risk register.
- Information Asset Owners (IAOs): Identify and classify information assets and provide input on potential risks.
- Management: Reviews and approves risk assessment findings and risk treatment plans.

#### 5. Steps:

##### 5.1. Identify Information Assets:

- Conduct an inventory of all information assets within the company.
- Identify the owner(s) and sensitivity level of each asset.

##### 5.2. Identify Threats and Vulnerabilities:

- Brainstorm potential threats and vulnerabilities that could impact identified information assets.
- Consider internal and external threats, such as:
  - Cyberattacks
  - Physical security breaches
  - System outages
  - Data breaches
  - Human error

##### 5.3. Analyze Risks:

- For each identified threat and vulnerability, assess the likelihood of occurrence and potential impact on information assets.
- Use a risk assessment matrix to determine the overall risk level (e.g., high, medium, low).

##### 5.4. Risk Register:

- Document the identified risks, likelihood, impact, and overall risk level in a risk register.
- The risk register should include:

- Description of the risk
- Threat source
- Vulnerability
- Likelihood score
- Impact score
- Overall risk level
- Recommended risk treatment actions
- Responsible person(s)
- Target completion date

#### 5.5. Risk Treatment:

- Develop and implement risk treatment plans to mitigate identified risks.
- Potential risk treatment options include:
  - Avoidance
  - Prevention
  - Reduction
  - Transfer
  - Acceptance

#### 5.6. Review and Update:

- Regularly review and update the risk assessment process and risk register to reflect changes in the organization's environment, threats, and vulnerabilities.

#### 6. Scales for Defining Risk Levels:

##### Likelihood:

- 5 – Almost certain to occur
- 4 – Likely to occur
- 3 – Possible to occur
- 2 – Unlikely to occur
- 1 – Rare

##### Impact:

- 5 – Catastrophic impact
- 4 – Major impact

- 3 – Moderate impact
- 2 – Minor impact
- 1 – Negligible impact

Overall Risk Level:

- High – Risk score of 16 to 25
- Medium – Risk score of 9 to 15
- Low – Risk score of 1 to 8

## 7. Risk Register Examples:

Example 1:

| Risk Description                     | Threat Source     | Vulnerability  | Likelihood | Impact | Overall Risk Level | Recommended Treatment  | Responsible Person | Target Completion Date |
|--------------------------------------|-------------------|--|------------|--------|--------------------|--|--------------------|------------------------|
| Unauthorized access to customer data | Malicious hackers | Weak password policy and lack of multi-factor authentication | 4          | 5      | 20                 | Implement strong password policy and multi-factor authentication | IT Security Team   | 3 months               |

Example 2:

| Risk Description                  | Threat Source | Vulnerability                    | Likelihood | Impact | Overall Risk Level | Recommended Treatment  | Responsible Person | Target Completion Date |
|-----------------------------------|---------------|----------------------------------|------------|--------|--------------------|--|--------------------|------------------------|
| Data loss due to hardware failure | System outage | Outdated hardware infrastructure | 3          | 3      | 9                  | Upgrade hardware infrastructure and implement backup and recovery procedures | IT Operations Team | 6 months               |

Note: These examples are for illustrative purposes only. The specific scales and risk register format may vary depending on the organization's needs and industry best practices.

## 8. Compliance with EU Regulations:



- Ensure the risk assessment process considers relevant EU regulations, such as the General Data Protection Regulation (GDPR).
- Identify and address risks associated with personal data processing and comply with GDPR data protection principles

**C6:** How to ensure the implementation of secure SDLC controls on the projects conforming to ISO27001 at EU-based software development company?

**GAI1-C6:**

Ensuring Secure SDLC Controls in ISO 27001 Compliant Projects

Introduction:

Implementing secure SDLC controls is crucial for developing secure and trustworthy software in an EU-based company complying with ISO 27001. These controls help identify and address security vulnerabilities throughout the software development lifecycle, reducing risks and ensuring data protection.

1. Integrating Secure SDLC with ISMS:

- Align the SDLC with the overall ISMS framework.
- Define roles and responsibilities for security within the SDLC.
- Integrate security practices into all SDLC phases, including requirements gathering, design, development, testing, deployment, and maintenance.
- Document and share secure SDLC policies and procedures with all stakeholders.

2. Implementing Specific Secure SDLC Controls:

a) Secure Requirements and Design:

- Conduct threat modeling to identify potential threats and vulnerabilities early on.
- Define security requirements and incorporate them into the design process.
- Utilize secure coding practices, such as input validation and secure data handling.

b) Secure Development and Testing:

- Implement static and dynamic application security testing (SAST and DAST) to identify and address vulnerabilities.
- Conduct code reviews to ensure secure coding practices are followed.
- Utilize secure development tools and libraries.

c) Secure Deployment and Maintenance:

- Implement secure deployment procedures and configuration management practices.
- Monitor for security vulnerabilities and incidents after deployment.

- Perform regular security audits and penetration testing.
- Maintain software updates and patches promptly.

### 3. Additional Controls:

- **Training and Awareness:** Train developers and other stakeholders on secure coding practices and security awareness.
- **Vulnerability Management:** Implement a vulnerability management program to identify, prioritize, and remediate vulnerabilities.
- **Incident Response:** Develop and implement an incident response plan to address security incidents effectively.
- **Secure Configuration Management:** Ensure secure configuration of systems and applications throughout the SDLC.
- **Third-Party Risk Management:** Implement controls to manage risks associated with third-party vendors and their software components.

### 4. Tools and Technologies:

- Utilize automated tools for vulnerability scanning, code analysis, and secure coding practices.
- Integrate security tools with the SDLC workflow.
- Consider using secure development platforms and cloud-based services.

### 5. Compliance with EU Regulations:

- Ensure SDLC controls address specific requirements of relevant EU regulations, such as the GDPR.
- Implement mechanisms for data access control, data integrity, and data protection.
- Conduct data protection impact assessments for high-risk projects.

### 6. Continuous Improvement:

- Regularly review and update SDLC controls based on lessons learned, evolving threats, and changes in technology.
- Conduct periodic audits and assessments to ensure the effectiveness of SDLC controls.
- Foster a culture of security within the organization, encouraging continuous learning and improvement.

By implementing these recommendations and adapting them to your specific company needs, you can ensure the implementation of secure SDLC controls and develop software that complies with ISO 27001 and protects sensitive data effectively.

**C7:** Could you please develop Information Security Awareness Program conforming to ISO27001, including regular training sessions on security policies, procedures, and best practices?

## **GAI1-C7:**

### Information Security Awareness Program for ISO 27001 Compliance

#### 1. Introduction

This document outlines an Information Security Awareness Program (ISAP) for an EU-based software development company aiming to comply with ISO 27001. This program aims to educate and train employees on information security principles, policies, procedures, and best practices to protect sensitive information and mitigate security risks.

#### 2. Objectives

- Increase employee awareness of information security risks and threats.
- Promote a culture of security within the organization.
- Equip employees with knowledge and skills to protect information assets effectively.
- Reduce the occurrence of security incidents and breaches.
- Ensure compliance with ISO 27001 and relevant EU regulations.

#### 3. Target Audience

This program targets all employees of the company, including:

- Developers
- IT staff
- Management
- Administrative personnel
- Third-party contractors

#### 4. Program Components

##### 4.1. Awareness Training:

- **Initial Training:** All new employees will receive comprehensive information security awareness training during onboarding.
- **Ongoing Training:** Regular training sessions will be conducted throughout the year to refresh knowledge and address emerging threats.
- **Training Topics:** Training sessions will cover topics such as:
  - ISO 27001 overview and information security principles.
  - Company information security policies and procedures.
  - Identification and classification of information assets.
  - Password security and best practices for managing credentials.
  - Social engineering and phishing attacks awareness.

- Data protection principles and GDPR compliance.
- Secure use of company resources and technology.
- Incident reporting procedures.

#### 4.2. Communication and Resources:

- Regularly communicate information security updates and reminders through various channels (e.g., newsletters, intranet, posters).
- Provide access to information security resources and reference materials (e.g., policies, FAQs, training videos).
- Encourage open communication and reporting of security concerns.

#### 4.3. Security Awareness Events and Activities:

- Organize security awareness campaigns and events to promote engagement and participation.
- Conduct phishing simulations and other practical exercises to test employee knowledge and response skills.
- Reward employees for demonstrating exemplary information security practices.

#### 4.4. Measurement and Evaluation:

- Regularly assess the effectiveness of the ISAP through surveys, quizzes, and feedback mechanisms.
- Analyze data and identify areas for improvement.
- Update the program content and delivery methods based on the evaluation results.

### 5. Training Sessions on Security Policies and Procedures

- Security Policy Training:
  - Overview of the company's information security policy.
  - Explanation of key security principles and goals.
  - Employee roles and responsibilities in information security.
  - Consequences of non-compliance with the policy.
- Procedures Training:
  - Training on specific security procedures, such as:
    - Password management.
    - Data access control.
    - Incident reporting.
    - Secure use of company devices and networks.

- Practical demonstrations and hands-on exercises.

## 6. Best Practices Training

- Training on best practices for protecting information assets, including:
  - Secure coding practices.
  - Data encryption and secure storage.
  - Physical security of devices and equipment.
  - Mobile security and BYOD policies.
  - Social engineering awareness and prevention techniques.
  - Secure online communication practices.

## 7. Compliance with EU Regulations

- Training on relevant EU regulations, such as the GDPR.
- Explain data protection principles and employee responsibilities.
- Provide guidance on handling personal data securely and complying with data subject rights.

## 8. Continuous Improvement

- Regularly review and update the ISAP to reflect changes in the organization's environment, threats, and regulations.
- Incorporate feedback from employees and stakeholders.
- Utilize new technologies and resources to enhance the program's effectiveness.

## 9. Conclusion

An effective Information Security Awareness Program plays a vital role in achieving and maintaining ISO 27001 compliance. By educating employees and promoting a culture of security, the company can significantly reduce risks, protect sensitive information, and build trust among stakeholders. This program should be adapted and tailored to the specific needs and context of the organization to ensure its success.

**C8:** Are there any privacy risks or concerns that should be taken into account while developing software under CCPA regulation?

### **GAI1-C8:**

#### Privacy Risks and Concerns while Developing Software under CCPA Regulation

Developing software under the California Consumer Privacy Act (CCPA) requires careful consideration of several privacy risks and concerns to ensure compliance and protect user data. Here are some key areas to be mindful of:

##### 1. Collection and Use of Personal Information:

- **Transparency:** Clearly inform users about what personal information is collected, the purpose of collection, and how it will be used.
- **Consent:** Obtain valid and informed consent from users before collecting or selling their personal information.
- **Minimization:** Collect only the minimum amount of personal information necessary for legitimate business purposes.
- **Data Retention:** Implement data retention policies to store personal information only for as long as necessary.

## 2. Access, Deletion, and Opt-Out Rights:

- Provide users with the right to access, correct, delete, and request portability of their personal information.
- Implement mechanisms for users to easily opt-out of the sale of their personal information.
- Respond to user requests promptly and securely.

## 3. Data Security:

- Implement strong security measures to protect personal information from unauthorized access, use, disclosure, modification, or destruction.
- Utilize encryption, access controls, and other appropriate safeguards.
- Regularly assess and update security practices to address evolving threats.

## 4. Third-Party Vendors:

- Carefully vet and select third-party vendors that process personal information on your behalf.
- Enter into contracts with vendors that include strong data security and privacy provisions.
- Monitor and audit vendors' compliance with data privacy regulations.

## 5. Transparency and Documentation:

- Maintain comprehensive records of all personal information collected, used, and disclosed.
- Document data collection, use, storage, and deletion practices.
- Make relevant information readily available to users through privacy policies and other notices.

## 6. Sensitive Data:

- Exercise particular caution when dealing with sensitive data categories such as social security numbers, financial information, and health data.
- Implement additional safeguards to protect this type of data.
- Obtain explicit consent before collecting and using sensitive data.

## 7. Compliance with other Regulations:

- Ensure compliance with other applicable data privacy regulations, such as the General Data Protection Regulation (GDPR) if your software is used by users outside of California.
- Stay updated on evolving privacy regulations and adapt your practices accordingly.

Additional Considerations:

- Conduct regular privacy impact assessments to identify and mitigate potential risks.
- Train employees on data privacy principles and practices.
- Implement a data breach response plan to address security incidents effectively.
- Consider engaging with privacy professionals and legal counsel to ensure compliance and best practices.

By addressing these risks and concerns during software development, you can minimize privacy violations, build trust with users, and ensure compliance with the CCPA. Remember that compliance is an ongoing process, and it is crucial to continuously monitor and adapt your practices to keep pace with evolving regulations and technologies.

## Generated responses by GAI1 Model for Engineer role

**E1:** Which technologies you can advise for EU-based software development company with 500 employees to build on?

**GAI1-E1:**

Technologies to Consider for an EU-based software development company with 500 employees:

Emerging Technologies:

- **Artificial intelligence (AI) and machine learning (ML):** These technologies are rapidly changing various industries, and companies that invest in AI/ML development can gain a significant competitive advantage.
- **Blockchain:** While still in its early stages, blockchain technology has the potential to revolutionize many industries, including finance, supply chain management, and healthcare. Investing in blockchain development can position your company well for the future.
- **Internet of Things (IoT):** The number of connected devices is expected to explode in the coming years, creating new opportunities for software development companies. Building expertise in IoT development can help your company tap into this growing market.
- **Quantum computing:** While still in its early stages, quantum computing has the potential to solve complex problems that are impossible for traditional computers. Investing in quantum computing research and development can give your company a head start in this emerging field.

Established Technologies:

- **Cloud computing:** Cloud computing offers a scalable and cost-effective way to develop and deploy software applications. By leveraging cloud services, your company can reduce its upfront costs and focus on core business activities.
- **Big data analytics:** With the growing volume of data available, companies need tools to analyze and extract insights from this data. Investing in big data analytics solutions can help your company make better decisions and improve its operations.
- **Cybersecurity:** As cyber threats continue to evolve, it is essential for software development companies to invest in robust cybersecurity solutions. This will help protect your company's data and systems from cyberattacks.
- **DevOps:** DevOps is a set of practices that combine software development and operations to improve agility and speed up delivery cycles. By adopting DevOps principles, your company can shorten time to market and improve software quality.
- **Low-code/no-code platforms:** These platforms are making it easier for businesses to develop their own software applications without the need for coding expertise. This can help your company reduce development costs and bring products to market faster.

#### Specific Technologies:

- **Programming languages:** Depending on your company's focus areas, you may want to consider building expertise in specific programming languages such as Python, JavaScript, Java, Go, or Kotlin.
- **Frameworks and libraries:** Frameworks and libraries can significantly reduce development time and costs. Popular choices include React, Angular, Spring, and TensorFlow.
- **Databases:** Choosing the right database technology is essential for storing and managing data. Popular options include MySQL, PostgreSQL, MongoDB, and Cassandra.
- **Testing tools:** Automated testing tools can help ensure the quality and reliability of your software. Popular choices include Selenium, Cypress, and Jest.
- **Version control systems:** Version control systems help track changes to your code and collaborate with other developers. Popular choices include Git and SVN.

#### Additional Considerations:

- **Market trends:** It is important to consider current and future market trends when making technology choices. Invest in technologies that are expected to grow and avoid those that are becoming outdated.
- **Company culture:** The best technology choices for your company will depend on your specific culture and needs. Consider factors such as your team's skills and experience, your budget, and your risk tolerance.
- **Scalability:** Choose technologies that can scale with your company's growth. This will help you avoid having to rewrite your code or switch to a new technology stack down the road.

#### Resources for further research:



- Stack Overflow: <https://stackoverflow.com/>
- GitHub: <https://github.com/github>
- TechCrunch: <https://techcrunch.com/>
- Gartner: <https://www.gartner.com/en>

By carefully considering these factors and conducting thorough research, you can make informed decisions about which technologies your EU-based software development company should build on to stay ahead of the competition and achieve its business goals.

**E2:** How should secure infrastructure of EU-based software development company with 500 employees look like on diagram?

### **GAI1-E2:**

Secure Infrastructure Diagram for an EU-based Software Development Company (500 employees)

Here's a high-level diagram representing the secure infrastructure of an EU-based software development company with 500 employees:

Infrastructure Layers:

#### 1. Network Layer:

- Internet Connectivity: High-bandwidth internet connection with redundancy and failover options.
- DMZ: Demilitarized Zone for hosting publicly accessible services like web servers.
- Internal Network: Secure network for core infrastructure and development resources.
- Firewalls: State-of-the-art firewalls to filter inbound and outbound traffic.
- VPNs: Secure VPN tunnels for remote access to the internal network.

#### 2. Development Layer:

- Version Control System: Securely stores and manages code (e.g., Git, SVN).
- CI/CD Pipeline: Automates building, testing, and deployment of software (e.g., Jenkins, GitHub Actions).
- Development Tools: Secure IDEs, code editors, testing frameworks, etc.
- Collaboration Tools: Secure platforms for communication and document sharing (e.g., Slack, Microsoft Teams).

#### 3. Production Layer:

- Web Servers: Secure web servers to host and deliver applications (e.g., Apache, Nginx).
- Application Servers: Servers running the core application code (e.g., Tomcat, WildFly).
- Databases: Securely store and manage application data (e.g., MySQL, PostgreSQL).
- Load Balancers: Distribute traffic across servers for scalability and resilience.

- **Monitoring and Logging:** Tools for monitoring system health and application performance (e.g., Prometheus, Grafana).

#### 4. Security Layer:

- **Intrusion Detection/Prevention Systems (IDS/IPS):** Detect and block malicious activity.
- **Anti-Malware and Antivirus:** Protect against malware and viruses.
- **Endpoint Security:** Secure laptops, desktops, and mobile devices.
- **Data Loss Prevention (DLP):** Prevent unauthorized data leaks.
- **Security Information and Event Management (SIEM):** Collect and analyze security logs for comprehensive threat detection.

#### 5. Backup and Disaster Recovery:

- **Data Backups:** Regular backups of data to secure locations (e.g., cloud storage, offsite tapes).
- **Disaster Recovery Plan:** Procedures for recovering from critical system failures or disasters.

#### Additional Components:

- **Identity and Access Management (IAM):** Manage user access and permissions to resources.
- **Multi-Factor Authentication (MFA):** Add an extra layer of security to user logins.
- **Encryption:** Encrypt data at rest and in transit.
- **Security Awareness Training:** Educate employees on cybersecurity best practices.

#### Diagram Representation:

The diagram would visually represent these layers with boxes and arrows connecting them. Different colors could be used to differentiate layers or security zones. An example layout could be:

- **Top Section:** Internet, DMZ, Firewalls
- **Middle Section:** Development Layer, Production Layer
- **Bottom Section:** Security Layer, Backup and Disaster Recovery

Remember: This is a generic representation, and the specific components and connections will vary depending on the company's specific needs and industry regulations. It's crucial to tailor the infrastructure to your specific requirements and continuously evaluate and update it based on evolving threats and security best practices.

I hope this information helps you visualize and build a secure infrastructure for your EU-based software development company!

**E3:** Develop a detailed instruction on how to configure access controls in Microsoft Azure in accordance with ISO 27001.

**GAI1-E3:**

## Configuring Access Controls in Microsoft Azure in Accordance with ISO 27001

### Introduction:

ISO 27001 is an international standard that outlines best practices for information security management systems (ISMS). It requires organizations to implement appropriate access controls to protect their information assets. Microsoft Azure offers a variety of features and services that can be used to configure access controls in accordance with ISO 27001.

### Azure Services for Access Control:

Several Azure services play a crucial role in implementing access controls:

- Azure Active Directory (AAD): Centralized identity and access management service for controlling access to Azure resources.
- Azure Role-Based Access Control (RBAC): Assigns specific roles and permissions to users and groups within AAD.
- Azure Resource Manager (ARM): Manages and deploys resources in Azure, including assigning access controls.
- Azure Policy: Defines rules and compliance standards for Azure resources.

### Steps for Configuring Access Controls:

1. Identify Information Assets:
  - List all critical information assets stored or processed in Azure.
  - Classify information assets based on sensitivity and impact of unauthorized access.
2. Define Access Levels:
  - Determine the minimum access level required for each user or group to perform their tasks.
  - Implement the principle of least privilege (granting only minimal access).
3. Configure Azure AD:
  - Create AAD users and groups for different roles and departments.
  - Implement multi-factor authentication (MFA) for increased security.
4. Configure Azure RBAC:
  - Assign roles with specific permissions to users or groups for Azure resources.
  - Use built-in roles or create custom roles for granular control.
  - Follow the principle of separation of duties by assigning different roles to different people.
5. Configure Conditional Access:

- Define policies that restrict access based on conditions (e.g., device type, location, IP address).
  - Implement access reviews to regularly review and update access permissions.
6. Implement Azure Policy:
- Create policies to enforce access control standards and best practices.
  - Monitor compliance with policies and address any violations promptly.
7. Monitor and Audit:
- Implement logging and auditing for all access activities.
  - Regularly review logs to detect suspicious activity and potential security breaches.
8. Document and Maintain:
- Document access control policies and procedures clearly.
  - Regularly review and update access controls to adapt to changing needs.

#### Additional Recommendations:

- Utilize Azure Security Center: Leverage the security insights and recommendations provided by Security Center to strengthen your access control posture.
- Implement Secure Score: Track your overall security posture and identify areas for improvement in access controls.
- Utilize Azure Key Vault: Store and manage sensitive information like passwords and encryption keys securely in Key Vault.
- Integrate with other security solutions: Integrate your Azure access controls with existing security tools for a holistic security approach.

#### Resources:

- Microsoft Azure Security Documentation: <https://learn.microsoft.com/en-us/azure/security/>
- ISO 27001 Information Security Management: <https://www.itgovernanceusa.com/iso27001>
- Azure Policy Samples for ISO 27001: <https://learn.microsoft.com/en-us/compliance/regulatory/offering-iso-27001>

#### Conclusion:

By following these steps and implementing best practices, you can configure access controls in Microsoft Azure in accordance with ISO 27001 and significantly improve the security posture of your organization. Remember to continuously monitor, review, and update your access controls to ensure they remain effective and adaptable to evolving threats and business needs.

**E4:** Could you please create a procedure for IT technician on how to manage cryptographic keys in accordance with ISO 27001 and how to configure encryption on Windows devices?

**GAI1-E4:**

Procedure for IT Technicians: Managing Cryptographic Keys and Configuring Encryption on Windows Devices (ISO 27001 Compliance)

1. Introduction:

This procedure outlines the steps for IT technicians to manage cryptographic keys and configure encryption on Windows devices in accordance with ISO 27001 standards.

2. Scope:

This procedure applies to all IT technicians responsible for configuring and managing cryptographic keys and encryption on Windows devices within the organization.

3. References:

- ISO/IEC 27001:2013 - Information Technology - Security Techniques - Information Security Management Systems – Requirements (<https://www.scribd.com/document/392846254/201624258-ISO-27001-pdf>)
- Microsoft Windows Documentation for BitLocker Drive Encryption
- Organization's Information Security Policy

4. Responsibilities:

IT Technicians:

- Implement and maintain the organization's cryptographic key management policy.
- Configure and manage cryptographic keys for Windows devices.
- Configure BitLocker Drive Encryption on Windows devices.
- Backup and restore cryptographic keys securely.
- Monitor and audit access to cryptographic keys and encrypted data.
- Report any suspicious activity or security incidents related to cryptographic keys or encryption.

5. Procedures:

5.1. Cryptographic Key Management:

- Key Generation: Generate cryptographic keys using FIPS 140-2 compliant hardware security modules (HSMs) or software libraries.
- Key Storage: Store cryptographic keys in secure locations with restricted access, such as dedicated HSMs, cloud key management services, or encrypted storage solutions.
- Key Rotation: Regularly rotate cryptographic keys to mitigate the risk of compromise.
- Key Destruction: Destroy cryptographic keys securely when they are no longer needed.

- Access Control: Implement strong access controls to restrict access to cryptographic keys based on the principle of least privilege.
- Logging and Auditing: Implement logging and auditing mechanisms to track all activities related to cryptographic keys and encryption.

#### 5.2. BitLocker Drive Encryption:

- Configuration: Enable BitLocker Drive Encryption on all Windows devices according to the organization's security policy.
- Encryption Algorithm: Use a strong encryption algorithm, such as AES-256, for maximum protection.
- Recovery Key Management: Store BitLocker recovery keys securely and separately from the encrypted devices.
- Pre-Boot Authentication: Implement pre-boot authentication to require a password or other authentication method before the operating system boots.
- Removable Storage Encryption: Enable encryption of removable storage devices to protect data at rest and in transit.

#### 5.3. Monitoring and Auditing:

- Regularly monitor logs and audit trails for suspicious activity related to cryptographic keys and encryption.
- Investigate any anomalies or security incidents promptly and take necessary corrective actions.
- Report any security incidents or potential vulnerabilities to the IT security team.

#### 6. Training:

- Provide IT technicians with appropriate training on cryptographic key management, BitLocker Drive Encryption, and ISO 27001 compliance requirements.
- Update training materials regularly to reflect changes in technology, security threats, and industry best practices.

#### 7. Documentation:

- Document all procedures related to cryptographic key management and BitLocker Drive Encryption configuration.
- Maintain accurate and up-to-date records of all cryptographic keys and encryption configurations.

#### 8. Review and Improvement:

- Regularly review and update the cryptographic key management and BitLocker Drive Encryption procedures to ensure they remain effective and compliant with ISO 27001 standards.

- Conduct periodic audits to assess the effectiveness of cryptographic key management and encryption controls.

#### 9. Non-compliance:

- Any violation of this procedure or the organization's security policy will be subject to disciplinary action, up to and including termination of employment.

#### 10. Contact Information:

- For any questions or concerns related to cryptographic key management or BitLocker Drive Encryption, please contact the IT security team.

Note: This procedure is a general guideline and may need to be adapted to the specific requirements of your organization and the applicable industry standards.

**E5:** Could you please advise what security controls should be configured in order to prevent the risk of data leakage in Microsoft 365?

#### **GAI1-E5:**

#### Security Controls for Preventing Data Leakage in Microsoft 365

Data leakage in Microsoft 365 can have severe consequences for organizations, including regulatory fines, reputational damage, and financial losses. Several security controls can be implemented to mitigate this risk:

#### Data Loss Prevention (DLP):

- Use Microsoft Purview Data Loss Prevention (DLP) to identify, classify, and protect sensitive data.
- Define DLP policies to prevent data from being shared or transferred outside the organization.
- Implement DLP policies for email, SharePoint Online, OneDrive for Business, and other Microsoft 365 services.
- Use DLP sensitivity labels to classify and protect sensitive documents and emails.

#### Access Controls:

- Implement Azure Active Directory (AD) and Multi-Factor Authentication (MFA) to control user access to Microsoft 365 resources.
- Grant least privilege access to minimize the number of users with access to sensitive data.
- Implement Azure AD Conditional Access to restrict access based on device type, location, and other factors.
- Regularly review and update user access permissions.

#### Device Management:

- Enroll all devices used to access Microsoft 365 in Microsoft Endpoint Manager (MEM/Intune).

- Configure mobile app management (MAM) to control how data is accessed and used on mobile devices.
- Require encryption of all devices used to access Microsoft 365.
- Implement remote wipe functionality to remove corporate data from lost or stolen devices.

#### Encryption:

- Enable encryption for all data stored in Microsoft 365, including email, files, and SharePoint Online sites.
- Use Azure Information Protection (AIP) to encrypt and protect sensitive documents and emails.
- Encrypt removable storage devices used to transfer data to and from Microsoft 365.

#### Auditing and Logging:

- Enable audit logging for all Microsoft 365 services to track user activity and data access.
- Regularly review audit logs to identify suspicious activity and potential data leakage incidents.
- Implement security alerts to notify administrators of potential security threats.

#### Additional Controls:

- Implement email filtering and anti-malware protection to prevent phishing attacks and malware infections.
- Secure your network infrastructure and implement firewalls to restrict unauthorized access.
- Regularly update Microsoft 365 applications and services to address security vulnerabilities.
- Educate your employees on data security best practices and how to identify and report suspicious activity.
- Conduct regular security assessments and penetration testing to identify and address security weaknesses.

Implementing these security controls can significantly reduce the risk of data leakage in Microsoft 365 and protect your organization's sensitive data.

Note: This is not an exhaustive list, and the specific controls you implement will depend on your organization's specific security requirements and risk tolerance.

It is also important to consider the following factors when configuring security controls:

- User experience: Security controls should be balanced with user productivity and needs.
- Cost: Some security controls require additional investment in software or licenses.
- Ease of implementation: Choose controls that are easy to manage and maintain.
- Legal and regulatory requirements: Your organization may need to comply with specific data privacy regulations.



It is recommended to consult with a security expert to help you assess your specific needs and implement appropriate security controls in Microsoft 365.

**E6:** Could you please provide the detailed technical configuration that needs to be done to secure the GitHub environment in accordance with ISO 27001?

**GAI1-E6:**

Securing Your GitHub Environment for ISO 27001 Compliance

Achieving ISO 27001 compliance within your GitHub environment requires implementing a comprehensive security framework across various aspects, including access control, data protection, vulnerability management, and incident response.

Here's a detailed breakdown of technical configurations:

1. Access Control:

- **Strong Authentication:** Enforce multi-factor authentication (MFA) for all users.
- **Least Privilege:** Grant access only on a need-to-know basis, based on user roles and responsibilities.
- **Role-based Access Control (RBAC):** Utilize GitHub's built-in RBAC system to manage user and group permissions for repositories, organizations, and teams.
- **Access Reviews:** Conduct regular access reviews to identify and revoke stale or unused permissions.

2. Data Protection:

- **Repository Encryption:** Enable repository encryption at rest and in transit using the strongest available cipher (AES-256).
- **Personal Access Tokens (PATs):** Manage PATs securely, including revoking inactive tokens, enforcing strong password requirements, and limiting their scope.
- **Secrets Management:** Utilize GitHub's Secrets functionality to securely store sensitive data like API keys and environment variables.
- **Branch Protection Rules:** Implement branch protection rules to prevent accidental or malicious changes to critical code.

3. Vulnerability Management:

- **Code Scanning:** Enable GitHub's code scanning feature to identify security vulnerabilities in your code.
- **Dependency Updates:** Automate security updates for dependencies to patch vulnerabilities promptly.
- **Regular Vulnerability Scans:** Conduct regular vulnerability scanning of your GitHub repositories and related infrastructure.

- Automated Patch Management: Implement automated patch management for vulnerabilities identified through scans.

#### 4. Incident Response:

- Incident Response Plan: Develop and document a comprehensive incident response plan for handling security incidents within your GitHub environment.
- Security Monitoring: Implement tools and processes for monitoring security events and alerts within your GitHub organization.
- Threat Intelligence: Utilize threat intelligence feeds to stay informed about emerging threats and vulnerabilities.
- Incident Reporting: Establish clear procedures for reporting and escalating security incidents within the organization.

#### Additional Technical Configurations:

- Security Policies: Define and enforce clear security policies outlining acceptable use, password complexity, and data handling procedures.
- Code Reviews: Implement mandatory code reviews for all code changes before merging them into the main branch.
- Automated Security Testing: Integrate automated security testing tools into your CI/CD pipeline to identify vulnerabilities early in the development process.
- Logging and Audit Trails: Enable comprehensive logging and audit trails for all user activity and security events.
- Security Awareness Training: Provide regular security awareness training for all users to educate them about cybersecurity best practices.

#### Compliance Tools and Resources:

- ControlMap: automates audit preparation and evidence collection for ISO 27001 compliance.
- Vanta: provides a platform for managing and documenting compliance policies and controls.
- GitHub Security Lab: offers tools and resources for securing your GitHub environment.
- ISO 27001 Documentation: provides official guidance on the standard's requirements.

Remember: This configuration guide serves as a general framework. The specific configuration steps will vary depending on your organization's security posture, risk tolerance, and compliance requirements. It's crucial to continuously monitor and adapt your security controls as threats evolve and best practices change.

By implementing these technical configurations and continuously evaluating your security posture, you can achieve a secure GitHub environment that meets the stringent requirements of ISO 27001.

**E7:** Could you prepare a training script for privileged Windows user covering related risks and recommendations?

### **GAI1-E7:**

#### Training Script for Privileged Windows Users

##### Introduction:

This training session will provide an overview of the risks and responsibilities associated with being a privileged Windows user. We will discuss best practices for securing your account and protecting sensitive data.

##### Target Audience:

This training is intended for all privileged Windows users, including administrators, domain controllers, and service accounts.

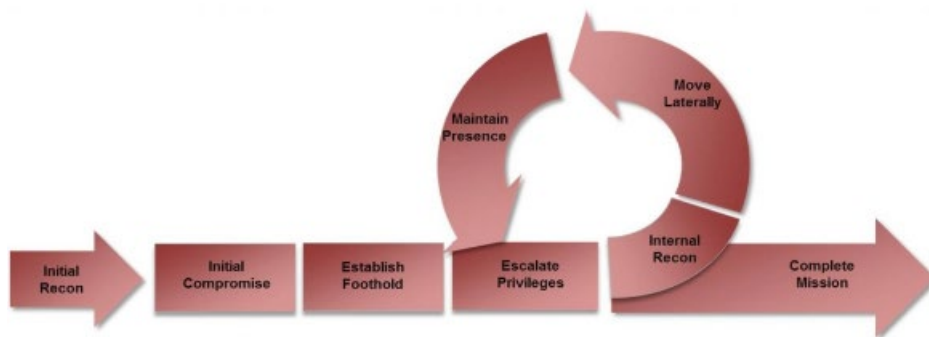
##### Training Objectives:

- Understand the risks associated with being a privileged user.
- Learn best practices for securing your account and protecting sensitive data.
- Identify common security threats and vulnerabilities.
- Implement strategies to mitigate security risks.

##### Training Agenda:

#### 1. Introduction to Privileged Access:

- What is a privileged user?
- Why are privileged users targeted by attackers?
- The impact of a compromised privileged account.



Source: Mandiant Consulting, see <https://www.fireeye.com/services.html>.

#### 2. Risks and Responsibilities:

- Risks of privilege misuse:
  - Data breaches

- System outages
- Financial losses
- Reputational damage
- Responsibilities of privileged users:
  - Securing your account and credentials
  - Protecting sensitive data
  - Following security policies and procedures

### 3. Best Practices for Securing Your Account:

- Use strong passwords and multi-factor authentication.
- Avoid using the same password for multiple accounts.
- Be aware of phishing attacks and social engineering scams.
- Don't open attachments or click on links from unknown senders.
- Keep your software up to date.
- Report suspicious activity to the IT security team.

### 4. Protecting Sensitive Data:

- Encrypt sensitive data at rest and in transit.
- Use access controls to restrict access to sensitive data.
- Regularly back up your data.
- Be mindful of what data you share online.

### 5. Common Security Threats and Vulnerabilities:

- Malware
- Phishing attacks
- Password brute-force attacks
- Zero-day attacks
- Insider threats

### 6. Strategies for Mitigating Security Risks:

- Implement security awareness and training programs.
- Conduct regular security assessments and vulnerability scans.
- Patch software vulnerabilities promptly.
- Implement security controls such as firewalls and intrusion detection systems.

- Have a plan for responding to security incidents.

#### 7. Resources:

- National Institute of Standards and Technology (NIST): <https://www.nist.gov/cybersecurity>
- SANS Institute: <https://www.sans.org/>
- Microsoft Security Response Center: <https://www.microsoft.com/en-us/msrc>

#### 8. Questions and Answers:

#### 9. Conclusion:

By following these best practices and being aware of the risks, you can help to keep your organization's data safe and secure.

#### Additional Resources:

- Microsoft Security Baseline for Windows 10: <https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-framework/windows-security-baselines>
- Center for Internet Security (CIS) Critical Security Controls: <https://www.cisecurity.org/>

**E8:** How to ensure that configuration of Microsoft 365 aligns with the requirements of CCPA?

#### **GAI1-E8:**

#### Ensuring Microsoft 365 Configuration Aligns with CCPA Requirements

The California Consumer Privacy Act (CCPA) grants California residents specific rights regarding their personal information, including the right to access, delete, and opt-out of the sale of their data. Organizations using Microsoft 365 must ensure their configuration complies with these requirements.

Here's how to ensure Microsoft 365 aligns with CCPA:

#### 1. Identify Personal Data:

- Determine what personal data your organization stores in Microsoft 365.
- Consider data in services like Exchange Online, OneDrive, SharePoint Online, and Teams.
- Utilize tools like Microsoft Purview Data Loss Prevention (DLP) to identify and classify sensitive data.

#### 2. Implement Access Controls:

- Leverage Azure Active Directory (AD) and multi-factor authentication (MFA) to control access to data.
- Grant access based on the principle of least privilege, minimizing unnecessary access.
- Implement Azure AD Conditional Access to restrict access based on location, device, and other factors.

- Regularly review and update user access permissions.

### 3. Enable Data Subject Rights Requests (DSRs):

- Configure Microsoft 365 to facilitate DSRs.
- This includes providing users with access to their data, deleting data upon request, and offering opt-out mechanisms.
- Consider utilizing tools like Microsoft Customer Lockbox for enhanced DSR management.

### 4. Implement Data Protection:

- Encrypt data at rest and in transit using encryption technologies like AES-256.
- Utilize Microsoft Purview Information Protection (AIP) to classify and protect sensitive data.
- Implement data retention policies to minimize unnecessary data storage.

### 5. Logging and Auditing:

- Enable audit logging for all Microsoft 365 services to track user activity and data access.
- Regularly review audit logs to identify suspicious activity and potential data breaches.
- Implement security alerts to notify administrators of potential threats.

### 6. Training and Awareness:

- Provide training for employees on CCPA requirements and data protection best practices.
- Raise awareness about protecting personal data and handling DSRs.
- Encourage employees to report suspicious activity.

### 7. Vendor Management:

- Ensure vendors with access to Microsoft 365 data comply with CCPA requirements.
- Implement contractual agreements to ensure data protection and adherence to CCPA regulations.

### 8. Regular Assessments:

- Conduct regular audits to assess compliance with CCPA requirements.
- Identify and address any gaps in compliance.
- Stay updated on evolving CCPA regulations and adapt your configuration accordingly.

### Additional Resources:

- Microsoft CCPA Documentation: <https://privacy.microsoft.com/en-us/ccpa>
- California Attorney General's CCPA website: <https://oag.ca.gov/privacy/ccpa/regs>
- International Association of Privacy Professionals (IAPP): <https://iapp.org/>

Image:



[https://tr.m.wikipedia.org/wiki/Dosya:Microsoft\\_365\\_logo.png](https://tr.m.wikipedia.org/wiki/Dosya:Microsoft_365_logo.png)

By following these steps and best practices, organizations can ensure their Microsoft 365 configuration aligns with the requirements of CCPA. This helps protect consumer privacy and minimizes the risk of non-compliance penalties.

### **Generated responses by GAI2 Model for Manager role**

**M1:** Could you please advise which security frameworks should EU-based software development company with 500 employees follow?

**GAI2-M1:**

Here are some recommended security frameworks an EU-based software company with 500 employees should consider following:

- ISO 27001 - This provides best practices for an information security management system. It helps companies manage and secure data properly. Key areas it covers includes access control, cryptography, communications security, and more.
- NIST Cybersecurity Framework - This provides guidelines around identifying, protecting, detecting, responding to, and recovering from cyberattacks. It's risk-based and flexible to adapt to different organizations.
- PCI DSS - The Payment Card Industry Data Security Standard is a must if the company handles any credit card data. It ensures cardholder data is properly managed and secured.
- GDPR - The EU's General Data Protection Regulation sets strict rules around collecting and managing Personally Identifiable Information. Fines for non-compliance can be substantial.
- OWASP Top 10 - The Open Web Application Security Project outlines the top 10 critical web application vulnerabilities. Following OWASP guidance can help secure web apps.
- CSA CCM - The Cloud Security Alliance's Cloud Control Matrix covers fundamental security principles across 16 domains for cloud infrastructure and applications.

Some good first steps would be achieving ISO 27001 and PCI DSS compliance, if applicable, and ensuring development teams are following guidance from OWASP and the NIST Cybersecurity Framework around application security and overall security best practices. Let me know if any

additional details would be helpful! **M2:** How organizational structure of EU-based software development company with 500 employees should look like to manage security risks effectively?

### **GAI2-M2:**

Here is one recommended way to structure an EU-based software company with 500 employees to have robust security risk management:

#### Senior Leadership

- CEO
- CFO
- CISO (Chief Information Security Officer)

#### Technology

- Engineering
- IT/Infrastructure

#### Information Security Department

- Governance, Risk and Compliance (GRC) Team
  - Develop security policies, standards
  - Perform risk assessments
  - Ensure regulatory compliance
- Application and Infrastructure Security
  - Provide architecture guidance
  - Code reviews, testing
  - Monitor networks, endpoints
  - Vulnerability management
- Identity and Access Management
  - Control access
  - Provisioning/deprovisioning
- Security Operations Center
  - Monitor alerts
  - Incident response
  - Forensics and threat hunting



## Other Departments

- Legal, Finance, HR

Having a dedicated CISO overseeing information security strategy as well as adequate staffing for key functions like GRC, security engineering, and SOC enables effective policy setting, user access controls, continuous monitoring, and swift incident response.

Cross-departmental collaboration also ensures security is ingrained at design and development stages. Please let me know if you need any other specifics around optimal information security organizational structures.

**M3:** Please develop Access Control Policy based on ISO 27001 to ensure the security and privacy of company systems and data.

### **GAI2-M3:**

Here is an outline for an Access Control Policy based on ISO 27001 guidelines that could be implemented for an EU-based software company to ensure security and privacy of systems and data:

#### Scope

This policy applies to all information systems, networks, and data used by employees, contractors, partners, and any other personnel that have access to company resources.

#### Policy Statements

- A role-based access control model will be used to limit access to only authorized users based on job role and responsibilities. The principle of "least privilege" will be followed.
- Authentication for network/system access will be enforced through secure passwords, multi-factor authentication, certificates, or other accepted methods.
- Employees will have access revoked immediately upon termination or change of employment.
- Logical access to data will be limited based on classification levels and staff roles. Restrictions in place to prevent unauthorized viewing, copying, or editing of sensitive data.
- Physical access to facilities, data centers, and other restricted areas will require valid credentials and audit logging.
- Annual user access reviews will be performed by data/system owners to ensure all those with access still require it for their job functions. Any unnecessary access to be revoked.
- Exceptions to this policy must be approved via formal access management process that involves appropriate risk assessment.

## Responsibilities

- CISO and Security team: Regular review of access logs/unauthorized access attempts, policy/control updates, identity & access management
- Managers: Submitting access requests/modifications/terminations for team members
- All Staff: Maintaining confidentiality of access credentials, promptly reporting suspicious activities

By following this standardized access control approach aligned with ISO 27001 guidelines, the confidentiality, integrity, and availability of company resources can be better protected from both internal and external threats.

**M4:** Please develop Encryption Policy that adheres to the encryption requirements of ISO 27001 to protect sensitive data.

### **GAI2-M4:**

Here is an outline of an Encryption Policy aligned to ISO 27001 encryption requirements that could be implemented at an EU-based software company:

#### Scope

This policy mandates standards for encryption of sensitive company data at rest and in transit to ensure confidentiality and privacy. It applies to all departments handling sensitive data.

#### Policy Statements

- Encryption protocols such as AES-256 or above must be implemented for storing sensitive data at rest and SSL/TLS for data in transit.
- Strong encryption passwords, keys, and certificates must be protected from unauthorized access, disclosure, and misuse.
- Sensitive data includes customer information, employee records, financial data, intellectual property, system credentials and must be classified appropriately.
- A secure key management process shall document storage, rotation, destruction, access control, authorized users etc.
- Encrypted data transported physically via removable media must adhere to secure transit guidelines.
- Periodic assessments by Security team required for new threat detection, encryption algorithm strength.

## Responsibilities

- CISO & Security team: Facilitate implementation of encryption controls as per data classification guidelines
- IT Systems team: Install and configure cipher suites, VPNs, manage keys/credentials
- Department heads: Conduct risk assessments of sensitive data, enable encryption

By aligning with ISO 27001 encryption standards, this policy aims to ensure encryption strength is maintained in the organization and evolving data security needs are addressed effectively as the threat landscape changes.

Please let me know if you need any clarification or have additional questions as I develop this policy further. I can provide implementation specifics on encryption protocols, key management, classified data types etc. based on your environment.

**M5:** Please develop an Information Security Risk Management Policy in accordance with ISO 27001 aimed at effective security risk identification, management, and treatment.

**GAI2-M5:**

Here is an outline for an Information Security Risk Management Policy based on ISO 27001 guidelines with the aim of effectively governing risk identification, assessment and treatment:

Scope

Applies to information security risk management processes followed across the organization to identify, analyze, evaluate and treat risks to systems and data.

Policy Statements

- Information security risks to the confidentiality, integrity and availability of data and systems will be assessed on an annual basis via risk assessment exercises.
- Identified risks will be quantitatively evaluated based on likelihood of occurrence and potential impact in terms of financial, reputational and productivity losses.
- Unacceptable high risks will be documented in risk registers and risk owners assigned. Treatment via application of controls, acceptance or avoidance determined in consultation with management.
- Residual risks after treatment to be continually monitored. Quarterly reviews conducted for high risks and half-yearly for moderate ones.
- Cyber insurance covering data breach, network outage, cyber extortion etc. will be acquired with annual evaluation of coverage.

- Training on information security risk awareness and procedures to be provided to all employees.

#### Responsibilities

- CISO: Direct information security risk assessments, maintain risk registers, advise on risk treatment
- Security team: Perform risk monitoring, recommend technical controls and guidance
- Managers: Provide inputs for risk evaluation, consult on risk treatment, enable security initiatives
- Employees: Attend risk management trainings, report risks/incidents promptly

Adoption of this standardized information security risk management policy in alignment with ISO 27001 will enable the organization to effectively identify, analyze and treat risks on an ongoing basis to ensure robust security.

Let me know if you need any other specifics to be included in this policy based on your organizational context. I can provide more guidance on risk assessment methodologies, metrics frameworks, controls etc.

**M6:** Please develop Secure Software Development Lifecycle Policy as per ISO 27001 requirements ensuring the security of software throughout the development lifecycle.

#### **GAI2-M6:**

Here is an outline for a Secure Software Development Lifecycle (SSDLC) policy in accordance with ISO 27001 standards to build security into all stages of software development:

#### Scope

This policy applies to all software development projects undertaken across the organization including in-house, outsourced, collaborations, and open source contributions.

#### Policy Statements

- Risk assessments must be carried out at project inception phase to define security requirements and identify controls.
- Security architecture, threat modeling and design reviews must be done during design phase addressing risks identified earlier.
- Static, dynamic analysis and penetration testing will be conducted on source code and software builds to identify and remediate vulnerabilities.

- Software security checklists must be completed to validate controls before User Acceptance Testing.
- Security configuration baselines adhering to company standards and checklists must be established.
- Production readiness reviews covering end-to-end security verification must be passed prior to deployment.
- Issue tracking for vulnerabilities and security updates during development until decommissioning.

Responsibilities:

- CISO: Provide SSDLC frameworks, standards, review processes
- Security Team: Conduct risk assessments, secure code reviews, penetration tests
- Development & Testing teams: Attend SSDLC training, complete checklists, comply to policy

By instituting this SSDLC policy mandated by ISO 27001, security can be intrinsically built into software development methodology reducing risk and enabling quicker remediation.

Please let me know if you need any clarification or specifics around the secure coding standards, preferred SAST/DAST tools, development & testing methodology followed etc. I can provide more tailored recommendations based for your technical environment and teams.

**M7:** Could you please develop Security Awareness and Training Policy in accordance with ISO 27001 to raise awareness about information security among employees?

**GAI2-M7:**

Here is an outline for a Security Awareness and Training Policy aligned with ISO 27001 to educate employees on maintaining information security:

Scope

This policy applies to all permanent and temporary employees, vendors, and contractors who access company systems or handle sensitive information.

Policy Statements

- All new hires must complete Information Security training during onboarding before systems access granted. Refresher courses yearly.
- Topic-specific security training to be provided when assuming new roles or responsibilities.
- Training will cover data privacy policies, password best practices, identifying threats like phishing, reporting incidents etc.

- Additional online security courses, mock simulations to heighten awareness of emerging threats like ransomware, business email compromise, social engineering etc.
- Alerts and advisories regarding high priority threats communicated across organization immediately as applicable.
- Security tips to be disseminated via newsletters, blogs or email reminders periodically to maintain heightened consciousness of vulnerabilities.
- Assessment surveys will measure understanding gained from the various awareness initiatives.

### Responsibilities

- CISO: Drive strategic development of security culture
- HR/Learning & Development: Support design/delivery of security education programs
- All staff: Responsible for completing mandatory trainings as assigned on time

This policy will enable robust security education through continuous skill-building that raises competency levels across organization to combat ever-evolving threats.

Please let me know if you need any specifics around training modalities, tools for implementation, measurement criteria etc. I would be happy to provide more tailored recommendations.

**M8:** What regulations should be followed in case our EU-based company provides software development services for client in California, who requires us to work with personal data?

### **GAI2-M8:**

If your EU-based software company is providing development services and handling personal data for a client located in California, here are some key regulations you would need to comply with:

1. GDPR - As an EU-based company, you are required to comply with the EU's General Data Protection Regulation around collection, processing, security and privacy of personal data of any EU residents.
2. CCPA - Since your client is based in California, their data is subject to the California Consumer Privacy Act, which sets requirements around disclosure, deletion rights, opt-out of sale of personal data for any California residents.
3. Privacy Shield/Standard Contractual Clauses - As you are transferring personal data to the US from the EU, you would need approved legal data transfer mechanisms in place such as the EU-US Privacy Shield framework or the Standard Contractual Clauses.

4. Data Security Controls - Specific data security controls required under GDPR like pseudonymization, encryption, access controls, audits etc. would need to be implemented when processing this data.

Additionally, aspects like transparency requirements, appointment of a Data Protection Officer, Privacy Impact Assessments may be necessary depending on specifics of data processing activities and risk analysis.

I'd be happy to provide more details on specific obligations under CCPA, GDPR or Privacy Shield for your scenario of client data processing. The key is ensuring EU data protection principles are upheld while also satisfying CCPA mandates. Please let me know if you need any further guidance!

### **Generated responses by GAI2 Model for Consultant role**

**C1:** Which security policies should be developed for EU-based software development company with 500 employees based on ISO27001?

**GAI2-C1:**

Here are some key security policies I would recommend an EU-based software company with 500 employees develop based on the ISO 27001 standard:

1. Information Security Policy - Outlines the company's approach and commitment to information security at a high level. Should define security goals, governance, compliance requirements, etc.
2. Access Control Policy - Covers guidelines for access rights, account creation/deletion, password policies, review procedures, remote access, etc. Important for ensuring only authorized user access.
3. Cryptography Policy - Defines standards and proper use of encryption to protect sensitive data in transit and at rest. Should cover things like algorithm types, key management, etc.
4. Acceptable Use Policy - Establishes what is considered acceptable use of company IT systems and data. Helps prevent misuse.
5. BYOD (Bring Your Own Device) Policy - Governs employee use of personal mobile devices to process company information. Important for security.
6. Data Classification Policy - Categories data by levels of sensitivity and defines corresponding security controls for each level. Helps match protections to data.
7. Vendor Security Policy - Covers minimum security requirements for vendors/third parties that access, store, or process company data. Manages third-party risk.

8. Incident Response Plan - Outlines responsibilities and plans for responding to security incidents like data breaches, malware, loss of data, etc. Important for minimizing damage.

The specifics of each policy would need to be tailored to the company's technology environment and compliance needs. But those are some of the essentials I would advise to start with. Let me know if you need any clarification or have additional questions!

**C2:** Could you please develop Statement of Applicability for ISO27001 for EU-based software development company with 500 employees?

**GAI2-C2:**

Here is an example Statement of Applicability (SOA) for an EU-based software company with 500 employees applying the ISO 27001 standard:

1. Introduction

This Statement of Applicability is for [Company Name], an EU-based software company headquartered in [Location] with development centers in [List Locations]. [Company] develops and markets [types of software] to [describe customers]. The company has approximately 500 employees globally.

This SOA has been developed according to Annex A of ISO 27001 and outlines the information security controls from ISO 27001 that are applicable and relevant to [Company]'s ISMS (Information Security Management System).

2. Scope of SOA

This SOA applies to [Company]'s entire information security management system processes and infrastructure supporting the development and delivery of the company's software products and services. This includes internal IT systems as well as cloud environments used to host services and data. Locations in scope involve offices and data centers in [list locations].

3. Applicable Controls

[Company] has adopted controls from all 14 sections of Annex A of ISO 27001. Due to regulatory requirements and customer contacts, all controls are applicable. However, the following controls are not relevant due to the nature of [Company]'s business operations and will be excluded or modified as documented below.

For example:

A.11.2.6 Security of network services: SNMP disabled due to lack of usage

A.12.1.3 Capacity management modified due to cloud infrastructure

4. Justification for Exclusion/Modification of Controls



[Provide justification and details for excluding or modifying any controls listed above]

## 5. Release and Approval

This SOA will be reviewed on an annual basis and updated as needed based on changes to [Company]'s IT environment, customer requirements, and regulatory obligations related to information security.

Approved by [Name, Title, and Date]

Let me know if you need any clarification or have additional questions as you establish your ISO 27001 ISMS!

**C3:** Develop a procedure on how to implement access controls in accordance with ISO27001 within the EU-based software development company.

### **GAI2-C3:**

Here is an example procedure for implementing access controls in alignment with ISO 27001 at an EU-based software development company:

#### 1. Perform Asset Classification

- Classify information assets (ex: code, customer data) based on confidentiality, integrity, availability requirements.

#### 2. Define Roles & Responsibilities Matrix

- Document system/application roles and map required access permissions to each one.
- Example roles: developer, tester, database admin, security auditor.

#### 3. Establish Access Policy

- Create detailed policy covering account creation/deletion, access reviews, revocation of access, password standards, multi-factor authentication (MFA), acceptable use, etc.

#### 4. Implement Technical Controls

- For on-premises infrastructure: Configure firewall rules, ACLs, VPNs, VLAN segmentation.
- For cloud infrastructure: Utilize IAM roles, security groups, VPC endpoints. Enable logging/monitoring.
- Enable MFA using time-based OTP tokens for all admin accounts and remote sessions.

#### 5. Manage Identities & Credentials

- Establish user provisioning / de-provisioning process aligned with access matrix.
- Disable inactive accounts after set timeframe.

- Enforce strong, complex passwords changed every 90 days.

#### 6. Perform Access Reviews

- Review entitlements and permissions quarterly to identify/remove unnecessary access.

#### 7. Maintain Audit Logs

- Enable thorough logging for tracking of all authentication, authorization and system events.

#### 8. Continually Improve

- Incorporate lessons learned from access violations, control failures and incident response into improved controls.

Document all procedures, review annually, and update as needed per evolving security best practices.

Let me know if you need any clarification or have additional questions!

**C4:** Could you please create a detailed guideline on what should be done in order to implement Encryption policy in accordance with ISO27001 within EU-based software development company?

#### **GAI2-C4:**

Here is a detailed guideline for implementing an Encryption Policy in accordance with ISO 27001 at an EU-based software development company:

1. Establish an encryption policy document covering the use of encryption protocols, algorithms, key management procedures, and protection of encrypted data and encryption keys. Align with industry standards and regulations like the EU GDPR.

2. Define what types of data should be encrypted based on data classification levels:

- Identify sensitive data like customer PII, financial information, intellectual property etc. that must be encrypted at rest and in transit.

3. Select approved encryption algorithms per data type:

- For data at rest, use AES-256 or above where possible. For data in transit, require TLS 1.2+ using modern cipher suites.

4. Implement encryption controls systematically:

- For databases, enable TDE or file/column-level encryption capabilities.

- For files/folders, leverage file system or application encryption tools.

- For cloud services, enable encryption functions at the IaaS/PaaS/SaaS level when available.

5. Establish cryptographic key management procedures:

- Define sound key generation, distribution, storage, rotation and revocation practices.
  - Use hardware security modules (HSMs) for storing high value keys.
6. Assign dedicated encryption management responsibilities:
- Appoint admins to oversee encryption technologies deployment per policy.
  - Maintain encryption documentation and procedures.
7. Continually review and update encryption policy per evolving regulatory and industry best practice requirements related to emerging threats and new technologies or products.

Let me know if you need any clarification or have additional questions on implementing robust encryption controls!

**C5:** Please develop a detailed procedure on how to assess risks in accordance with ISO27001 at EU-based software development company, what scales should be used to define risk levels and provide several examples of how risk register should look like?

**GAI2-C5:**

Here is a detailed procedure for conducting risk assessments in accordance with ISO 27001 at an EU-based software development company, along with recommended risk scales and risk register examples:

**Risk Assessment Procedure:**

1. Establish context - Define scope, key company assets, risk criteria.
2. Identify risks - Conduct workshops, surveys to find where vulnerabilities may lead to compromise of confidentiality, integrity, availability. Consider cyber threats, employees, 3rd parties, physical disasters, errors etc.
3. Analyze risks - Estimate likelihood, impact levels using the 5x5 or 3x3 qualitative risk matrix below. Calculate risk score. Focus on high probability, high impact risks first.

**Likelihood Ratings (5x5 matrix):**

1 - Rare; 2 - Unlikely; 3 - Possible; 4 - Likely; 5 - Almost certain

**Impact Ratings:**

1 – Insignificant; 2 – Minor; 3 – Moderate; 4 – Major; 5 – Catastrophic

4. Evaluate risks - Determine risk treatment based on scores:
  - High risks (15-25) require direct action
  - Moderate risks (5-12) may be acceptable with monitoring
  - Low risks (1-4) may not need intervention

5. Treat risks – Select strategy to tolerate, transfer, terminate risk or take actions to reduce likelihood or impact through technical safeguards, policies, training etc.

6. Monitor & review – Review assessment at least annually per ISO 27001.

Risk Register Examples:

Risk ID | Asset | Risk Description | Threat Source | Annualized Rate | Existing Controls | Impact | Likelihood | Risk Score | Risk Treatment

1 | Customer Data | Sensitive data theft | Hackers | 75% | Network firewalls and IDS | 4 | 5 | 20 | Implement 2-factor authentication

2 | Auth Systems | Account takeover | Phishing | 60% | Password policy | 3 | 4 | 12 | Enhance employee security training

Let me know if you have any other questions!

**C6:** How to ensure the implementation of secure SDLC controls on the projects conforming to ISO27001 at EU-based software development company?

#### **GAI2-C6:**

Here are some recommended steps to ensure implementation of secure SDLC controls in alignment with ISO 27001 for projects at an EU-based software development company:

1. Establish a formal secure development policy that aligns to ISO 27001 requirements. Outline all required security activities that must be performed across design, coding, testing, release, and support.

2. Integrate security requirements into the core project lifecycles and project management frameworks used across the organization. Require sign-offs to ensure policy conformance at key milestones like requirements, design, implementation, testing, etc.

3. Provide tailored, practical secure coding guidelines and training for developers specific to the programming languages used. Include guidance on input validation, output encoding, error handling, encryption, authentication, access control etc. per ISO 27001 application development controls.

4. Incorporate security testing tools and processes into the standardized QA approach, including:

- Static Application Security Testing (SAST)
- Dynamic Application Security Testing (DAST)
- Vulnerability scanning
- Penetration testing

Utilize results to drive remediation before production deployment.

5. Maintain detailed logs allowing review that all expected ISO 27001 software development controls have been properly implemented per the secure SDLC policy for a given project release.

6. Periodically audit a sample of recent major application releases from across the organization to verify that defined secure SDLC controls were applied as expected.

Let me know if you have any other questions!

**C7:** Could you please develop Information Security Awareness Program conforming to ISO27001, including regular training sessions on security policies, procedures, and best practices?

**GAI2-C7:**

Here is an outline of an Information Security Awareness Program for an EU-based software company that conforms to ISO 27001 standards:

1. Build Awareness Governance Plan:

- Appoint security awareness committee to oversee program design, execution, and continual improvement
- Define roles & responsibilities between Security Team, HR, and other stakeholder groups
- Set annual goals including target training metrics and high-level topics to cover

2. Conduct Training Needs Assessment:

- Identify highest risk behaviors and skill gaps through surveys, interviews, and policy/incident analysis
- Prioritize topics, teams, and techniques to address with greatest needs

3. Design Ongoing Training Curriculum:

- Security Fundamentals - New hire onboarding on policies, tools, employee responsibilities
- Computer Security Basics - Malware, phishing, passwords, clean desk, info handling
- Compliance Training - GDPR, data privacy, intellectual property handling
- Role-Specific Training - Developers/engineers, HR, executives, etc.
- Simulated Phishing Drills & Assessments

4. Plan Training Delivery:

- Monthly emails, posters, intranet updates on relevant security topics
- Interactive online courses with knowledge checks
- Periodic in-person/video training workshops providing opportunity for hands-on practice and Q&A

5. Track Program Effectiveness:

- Administer surveys and quizzes to gauge comprehension
- Monitor phishing click rates and policy violation rates

- Fine-tune program accordingly toward fostering the most compliant security behaviors

Let me know if you have any other questions!

**C8:** Are there any privacy risks or concerns that should be taken into account while developing software under CCPA regulation?

**GAI2-C8:**

Yes, there are several important privacy risks and requirements to consider when developing software that handles personal data subject to the CCPA:

1. Data Minimization - Only collect the minimum amount of personal information required for the specific business purpose. Limit collection and retention to what is truly necessary.
2. Disclosures & Consent - Clearly notify users about what types of personal data is being collected and allow them to consent, opt-out or request deletion of their information. Honor all consumer rights requests.
3. Data Protection - Take reasonable security measures like encryption, access controls, logging, monitoring and audits to protect the confidentiality and integrity of the personal data.
4. Supplier Management - When utilizing third-party processors or services that may handle personal data, ensure thorough vetting, security assessments and contractual controls are in place to maintain compliance.
5. Purpose Limitation - Only use the collected personal information for purposes directly related to fulfillment of the services outlined to users at time of collection and nothing further without renewed consent.
6. Accountability & Auditing - Maintain detailed audit logs related to personal data handling, processing and sharing to demonstrate compliance across all operations with ability to identify, investigate and resolve privacy incidents rapidly.

Building these kinds of privacy protections into the software from the ground up can help minimize compliance gaps with CCPA while protecting consumer data rights. Please let me know if you have any other questions!

### **Generated responses by GAI2 Model for Engineer role**

**E1:** Which technologies you can advise for EU-based software development company with 500 employees to build on?

**GAI2-E1:**

Here are some good technologies an EU-based software company with 500 employees could utilize and build on:

## Cloud Platforms:

- AWS - Amazon Web Services is a very robust and globally-distributed public cloud. Provides massive scale and many services. Good for dynamic workloads.
- Azure - Microsoft's public cloud platform. Tight integration with existing Microsoft tools. Strong in AI/ML services.

## App Development Frameworks:

- React - A leading JavaScript framework for building dynamic web apps and UI components. Maintained by Facebook.
- Angular - A TypeScript-based web app framework developed by Google. Opinionated and full-featured.
- Spring Boot - Popular Java framework for building scalable backend services and APIs.

## Application Infrastructure:

- Docker - Container platform to streamline deployments across environments. Great for microservices.
- Kubernetes - Open-source orchestration platform for deploying and managing containers. Provides scaling, resilience.

## Databases:

- PostgreSQL - Powerful open-source SQL database with a strong reputation.
- MongoDB - Leading NoSQL document database. Handles massive volumes of data.
- Redis - In-memory data store, useful for caching/messaging.

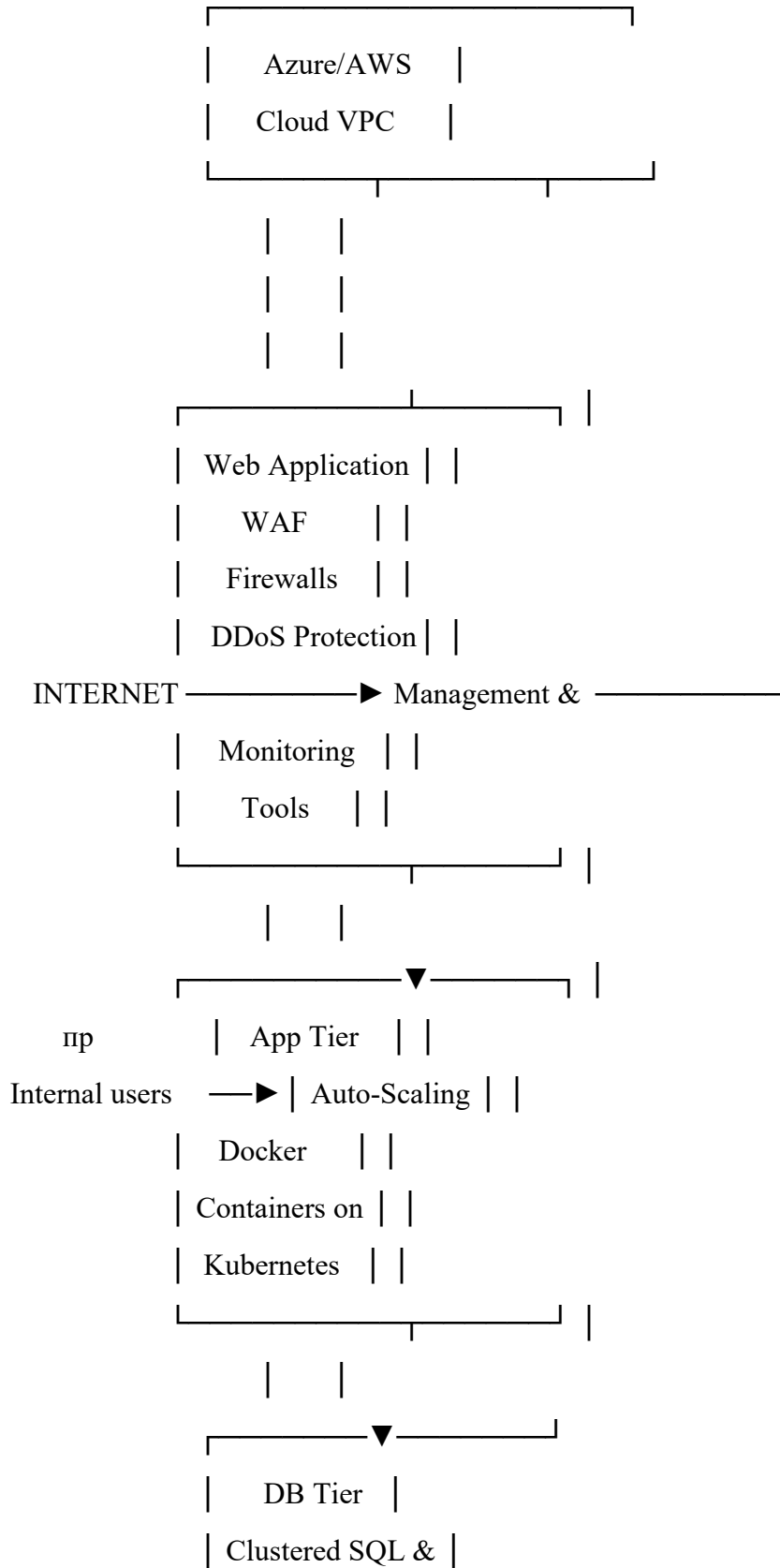
Overall, I'd suggest leveraging managed cloud platforms as appropriate to minimize overhead of self-hosted infrastructure. Focus development on robust frameworks suited for enterprise scale. Use containers/Kubernetes for modular architecture. Evaluate database options based on specific app patterns and data schemas.

Let me know if any additional detail would be helpful! There are of course many directions this could go depending on the specific applications.

**E2:** How should secure infrastructure of EU-based software development company with 500 employees look like on diagram?

**GAI2-E2:**

Here is a diagram for how a secure infrastructure environment should be modeled at a EU-based software company with 500 employees:





|                  |
|------------------|
| NoSQL on IaaS    |
| PaaS VNet        |
| Encryption &     |
| Auditing enabled |

### Key Security Elements:

- Multi-cloud (Azure + AWS) for high-availability
- VPCs to segregate environments
- Web application firewalls + DDoS protection
- Microservices in auto-scaling containers
- Database encryption and auditing
- Intra-env TLS encryption between tiers
- Central security monitoring and management

Please let me know if you have any other questions!

**E3:** Develop a detailed instruction on how to configure access controls in Microsoft Azure in accordance with ISO 27001.

### **GAI2-E3:**

Here is a detailed step-by-step guide on configuring access controls in Microsoft Azure to comply with ISO 27001 security controls standards:

#### 1. Enable Azure Role Based Access Control (RBAC)

- RBAC allows fine-grained control by assigning granular roles to groups and applications. Configure custom roles with specific permissions tailored for security and compliance needs.

#### 2. Define RBAC policy with principle of least privilege

- Only assign the minimal necessary permissions. Limit admin/owner roles. Perform regular access reviews.

#### 3. Configure Azure conditional access policies

- Set policies to enforce contextual requirements like multi-factor authentication (MFA) for sensitive operations. Require trusted locations and devices. Mandate app protection policies.

#### 4. Log and audit access control changes

- Enable Azure AD access reviews. Stream activity logs to Log Analytics. Alert on critical events. Use Azure Monitor dashboards for visibility. Send logs to external SIEM as needed.

#### 5. Restrict external network access to VMs/services

- Set up Network Security Groups (NSGs). Whitelist trusted IP ranges. Disable public access where not required. Enforce service endpoints and VNet integration for maximum security.

#### 6. Leverage Azure Key Vault for secrets management

- Grant access to keys and secrets only on as-needed basis. Integrate with applications and auto-rotation policies. Monitor access attempts.

#### 7. Implement JIT VM access

- Use Azure Bastion or similar to enable just-in-time and audited RDP/SSH connectivity rather than open ports.

#### 8. Validate controls with Azure Security Center

- Use Security Center compliance dashboards to continuously assess ISO 27001 control status across the environment. Remediate findings related to access controls.

Let me know if you need any clarification or have additional questions! Please advise if you would like details on any specific access control scenarios.

**E4:** Could you please create a procedure for IT technician on how to manage cryptographic keys in accordance with ISO 27001 and how to configure encryption on Windows devices?

#### **GAI2-E4:**

Here is a step-by-step procedure for an IT technician on managing cryptographic keys in alignment with ISO 27001 controls and configuring encryption on Windows devices:

#### Managing Cryptographic Keys:

1. Establish a key management process with access granted on a need-to-know basis. Keys should only be accessible to personnel requiring them to perform job functions.
2. Generate keys using secure algorithms and key lengths aligned to latest NIST standards (e.g. RSA 2048+ bit or ECC 256+ bit keys).
3. Store keys securely in a Hardware Security Module (HSM) or managed service like Azure Key Vault for highest assurance. Restrict permissions to add or retrieve keys.
4. Log key access attempts and create alerts for unauthorized requests. Perform privileged access reviews every 90 days.
5. Set automated rotation policies for keys. Destroy old keys completely after a new version is in place.
6. Enforce secure protocols like TLS when transmitting keys over networks. Sign and encrypt keys for storage.

## Configuring Windows Encryption

1. Enable BitLocker drive encryption for internal hard disks and removable media with AES 256-bit XTS-AES encryption.
2. Mandate strong passphrases meeting complexity requirements to secure encryption keys.
3. For portable devices, utilize Windows device encryption with instant device wipe after 10 failed sign-in attempts.
4. Set Windows firewall rules to only allow connections from trusted sources and block risky inbound ports.
5. Enable Always Encrypted feature for protecting sensitive application and database data.

Please let me know if you need any clarification or have additional questions! I can provide more specifics on implementing encryption controls across common Windows environments.

**E5:** Could you please advise what security controls should be configured in order to prevent the risk of data leakage in Microsoft 365?

### **GAI2-E5:**

Here are key security controls I recommend configuring in Microsoft 365 to help prevent data leakage risks:

1. Enable Data Loss Prevention (DLP) policies to detect and automatically protect sensitive information across Office 365
  - Configure rules and conditions based on data types, key identifiers, sharing restrictions
2. Restrict permissions for sharing data externally and mandate data classification
  - Limit ability to share outside organization without reviewing. Classify data to dictate appropriate protections
3. Turn on Exchange Online Advanced Threat Protection
  - Provides additional analysis to detect malicious attachments and links in emails to stop data exfiltration attempts
4. Configure alerts in the Microsoft 365 Security Center
  - Set up alerts for suspicious downloading, after-hours logins, mass deletions, etc. Tune anomaly detection policies over time
5. Review Office 365 Secure Score and implement identified recommendations
  - Improves overall security posture against data leakage. Address weaknesses like multi-factor authentication gaps.

6. Adopt third-party data loss prevention tools if higher sensitivity

- Extends capabilities for identifying confidential data patterns, enforcing contextual access rules and data rights management

7. Frequently audit user permissions and monitor admin actions

- Rotate privileged credentials. Ensure access reviews and minimize standing access to sensitive data.

8. Provide ongoing staff training around data handling

- Help users understand policies and their responsibility in preventing data compromise.

Please let me know if you have any other specific questions! Happy to provide additional guidance to secure your Office 365 environment.

**E6:** Could you please provide the detailed technical configuration that needs to be done to secure the GitHub environment in accordance with ISO 27001?

**GAI2-E6:**

Here are the key technical controls I would recommend to help secure GitHub to align with ISO 27001 information security policy:

GitHub Configuration

1. Enable 2-factor authentication (2FA) for all GitHub user accounts to prevent unauthorized access
2. Configure conditional access policies to require trusted IP ranges, strong device attestation, and limited failed login attempts
3. Use role-based access control permissions and manage membership strictly to enforce least privilege
4. Turn on GitHub Advanced Security vulnerability scanning for repositories to detect code issues
5. Force HTTPS connections and enable TLS v1.2+ encryption in transit for web traffic
6. Create audit log alerts and SIEM integration to monitor critical security events
7. Enable Branch Protection rules to mandate code reviews and status checks before merging
8. Configure Dependabot for automatic pull requests to update vulnerable libraries
9. Use GitHub Actions workflows to embed security testing in the DevOps CI/CD pipeline
10. Adopt Signed Commits to ensure cryptographic verification of Git changes

Together these controls significantly increase identification and protection against threats in order to comply with ISO 27001 security objectives. Please let me know if you need any clarification or assistance with technical implementation details on any specific GitHub security hardening.

**E7:** Could you prepare a training script for privileged Windows user covering related risks and recommendations?

**GAI2-E7:**

Here is a training script covering security risks and recommendations for privileged Windows users:

## Introduction

As a privileged user on this Windows environment, you have elevated access to perform administration, install programs, and configure critical systems and servers. This comes both powers and responsibilities related to security. I want to provide an overview of key risks you should be aware of, along with best practices you should follow to help keep our systems protected.

## Key Risks

- Credential theft – Your admin credentials are highly valuable to attackers. Phishing attacks or malware could compromise your login details to gain unauthorized access.
- Exploiting misconfigurations – Any vulnerabilities or misconfigured systems you introduce could provide openings for malicious actors to gain entry and escalate privileges.
- Falling victim to social engineering – Attackers may attempt to manipulate you through persuasive techniques to hand over access or make harmful changes they shouldn't have rights to do themselves.

## Recommendations

- Maintain dedicated admin accounts – Use separate standard user accounts for common daily work like email and web browsing to limit exposure of admin rights.
- Leverage multi-factor authentication (MFA) – Enroll admin accounts in MFA using a hardware token or authenticator app to prevent password compromise.
- Be extremely cautious of unsolicited links/attachments – Never provide credentials or other sensitive data without verifying legitimacy first.
- Minimize standing privileges – Review and revoke any persistent elevated access no longer required after specific tasks complete.
- Report suspicious security events – Promptly flag phishing attempts, anomalies, or other potential indications of compromise to infosec staff.

By remaining continuously vigilant and following security best practices in your privileged role, you can help protect us from compromise. Please reach out with any other questions!

**E8:** How to ensure that configuration of Microsoft 365 aligns with the requirements of CCPA?

**GAI2-E8:**

Here are best practices for configuring Microsoft 365 to align with key requirements within the California Consumer Privacy Act (CCPA) regulations:

## 1. Classify stored data appropriately and restrict access permissions

- Identify covered information like names, emails, locations etc. and limit access only to those with need-to-know.

2. Enable data loss prevention (DLP) policies in Microsoft 365
  - Configure rules to detect exposed PII and automatically take remediating actions like encrypting or blocking sharing.
3. Turn on auditing/logging across services and retain event data
  - Activate unified audit logs, alert on policy changes. Retain audit records for minimum 1 year per CCPA compliance needs.
4. Train Microsoft 365 administrators on managing consumer privacy data
  - Admins must understand regulatory responsibilities in order to effectively apply appropriate controls.
5. Configure GDPR data subject requests in the Microsoft compliance center
  - Customers can utilize same request process for CCPA data access or deletion requirements.
6. Adopt Azure Information Protection labeling and encryption
  - Classify documents with sensitivity labels. Encrypt data both at rest and in transit.
7. Utilize Office 365 Advanced eDiscovery for identifying covered data
  - Helps search, classify, and filter consumer information dispersed across network.

Please let me know if you have any additional questions! Want to ensure we properly govern access to covered data within our Microsoft 365 environment as required under CCPA regulations.

### **Generated responses by GAI3 Model for Manager role**

**M1:** Could you please advise which security frameworks should EU-based software development company with 500 employees follow?

**GAI3-M1:**

For a European Union-based software development company with 500 employees, adhering to robust security frameworks is crucial to ensure the protection of data, compliance with regulations, and maintaining trust with clients and users. Here are some key security frameworks and standards that are relevant:

1. General Data Protection Regulation (GDPR): This is the primary regulation in the EU for data protection and privacy. GDPR imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. It focuses on the lawful processing of personal data, consent, data subjects' rights, and data protection measures.
2. ISO/IEC 27001: This is an international standard on how to manage information security. It includes details on how to set up and manage an information security management system (ISMS). This is particularly relevant for software companies as it helps protect confidential data, ensure the integrity of business data, and improve the resilience of IT systems.
3. NIST Cybersecurity Framework: While it's a U.S. standard, the NIST framework is globally recognized. It provides a policy framework of computer security guidance for how private

sector organizations in the United States can assess and improve their ability to prevent, detect, and respond to cyber attacks. It's widely applicable for its comprehensive approach to risk management.

4. **Payment Card Industry Data Security Standard (PCI DSS):** If the company handles card payments, this standard is crucial. It applies to any organization that stores, processes, or transmits cardholder data, ensuring secure environments.
5. **Cyber Essentials (UK):** While it's a UK standard, it's often considered by EU companies as well. It focuses on basic cyber hygiene and offers a sound foundation of basic IT security controls.
6. **EU Cybersecurity Act:** This act strengthens the EU's cybersecurity, establishing a European cybersecurity certification framework for products, services, and processes.
7. **Cloud Security Alliance (CSA) Security, Trust & Assurance Registry (STAR):** For companies utilizing cloud services, CSA STAR can be very relevant. It's a free, publicly accessible registry documenting the security and privacy controls provided by popular cloud computing offerings.

In addition to these, it's also important for the company to stay informed about local data protection laws in specific EU countries where they operate, as there can be additional national regulations. Continuous training and awareness programs for employees, regular security audits, and a proactive approach to cybersecurity are also essential practices.

**M2:** How organizational structure of EU-based software development company with 500 employees should look like to manage security risks effectively?

### **GAI3-M2:**

Designing an effective organizational structure for an EU-based software development company with 500 employees, particularly with a focus on managing security risks, involves integrating security roles and responsibilities throughout the organization. A well-structured organization not only aligns with the business objectives but also ensures that security is a shared responsibility. Here's a suggested structure:

#### **Executive Level**

- **Chief Executive Officer (CEO):** Sets the overall strategic direction of the company.
- **Chief Information Security Officer (CISO):** A key role, reporting directly to the CEO or COO, responsible for overseeing and reporting on the company's security posture.
- **Chief Technology Officer (CTO):** Oversees the technological direction of the company, including software development practices.
- **Chief Operating Officer (COO):** Manages operational aspects, aligning them with security practices.
- **Chief Financial Officer (CFO):** Responsible for financial planning and risk management, including cybersecurity-related financial risks.

- **Chief Compliance Officer (CCO):** Oversees compliance with laws and regulations, an essential role given the GDPR and other regulatory requirements.

### Middle Management

- **IT and Security Department:**
  - Led by the CISO.
  - Divisions for Network Security, Application Security, Incident Response, and Compliance.
  - Works closely with IT Infrastructure and Software Development teams.
- **Software Development Department:**
  - Headed by a Senior Development Manager.
  - Teams divided by product lines or services, incorporating security-focused roles like Security Champions within each team.
- **Project Management Office (PMO):**
  - Led by a PMO Director.
  - Ensures that security risk management is integrated into project management practices.

### Operational Teams

- **Development Teams:**
  - Include Security Champions who liaise with the IT and Security Department.
  - Follow secure coding practices and are trained in security awareness.
- **Quality Assurance (QA) and Testing:**
  - Integrates security testing into the software development lifecycle (SDLC).
- **IT Infrastructure:**
  - Manages network and system security.
  - Collaborates with the Security Department for implementing security controls.
- **Human Resources (HR):**
  - Manages security training and awareness programs.
  - Ensures background checks and security policies are part of the hiring process.
- **Customer Support and Relations:**
  - Trained in handling data securely and recognizing potential security threats.

### Cross-Functional Teams

- **Risk Management Committee:**
  - Includes representatives from different departments.
  - Focuses on identifying, assessing, and mitigating security risks across the organization.
- **Incident Response Team:**
  - A specialized, cross-functional team ready to respond to security incidents.

### Additional Considerations

- **Regular Training and Awareness Programs:** Across all levels of the organization.
- **Communication Channels:** For reporting security concerns and incidents.
- **Regular Audits and Assessments:** To evaluate the effectiveness of security measures.
- **Scalability and Flexibility:** The structure should adapt to the changing cybersecurity landscape and business growth.

This structure aims to embed security into every layer of the organization, ensuring that security risk management is not just confined to a single department but is a shared responsibility. Regular reviews



and updates to the structure might be necessary to keep pace with technological advancements and evolving security threats.

**M3:** Please develop Access Control Policy based on ISO 27001 to ensure the security and privacy of company systems and data.

**GAI3-M3:**

Creating an Access Control Policy based on ISO 27001 standards is a crucial step for ensuring the security and privacy of company systems and data. ISO 27001 is an international standard for information security management systems (ISMS) and provides a systematic approach to managing sensitive company information so that it remains secure.

Here's an outline for an Access Control Policy:

Access Control Policy

1. Purpose:

To establish a framework for controlling access to information systems and ensuring that such access is authorized and managed effectively in line with ISO 27001 standards.

2. Scope:

This policy applies to all employees, contractors, and third parties who have access to [Company Name]'s information systems and data.

3. Policy Statements:

3.1 User Access Management:

3.1.1 User Registration: Formal user registration and de-registration process for granting and revoking access to all information systems and services.

3.1.2 Privilege Management: Allocation of privileges must be restricted and controlled based on the user's job role and responsibilities.

3.1.3 User Password Management: Strong password controls must be implemented and adhered to.

3.2 User Responsibilities:

3.2.1 Password Use: Users are responsible for keeping their passwords confidential.

3.2.2 Unattended User Equipment: Users must lock or log off when systems are unattended.

3.2.3 Information Access Restriction: Access to information and application system functions must be restricted in accordance with the access control policy.

3.3 System and Application Access Control:

3.3.1 Secure Log-on Procedures: Access to systems and applications must be controlled by a secure log-on process.

3.3.2 System Utilities Access: Restrictions must be placed on the use of system utilities that could override system and application controls.

3.3.3 Session Time-out: Automatic session time-out must be implemented on inactive sessions.

3.4 Network Access Control:

3.4.1 Policy on Use of Network Services: Users must only use services that they have been specifically authorized to use.

3.4.2 User Authentication for External Connections: Appropriate authentication methods must be used for users connecting from external locations.

3.4.3 Equipment Security: Measures must be taken to protect data and information system security when using mobile computing and teleworking facilities.

4. Compliance:

Non-compliance with this policy can result in disciplinary action and could have legal consequences.

5. Policy Review and Modification:

This policy will be reviewed annually and updated as necessary to ensure compliance with relevant laws and regulations.

6. Approval and Implementation:

This policy is approved by [Top Management/CEO/Board]. All relevant stakeholders are required to implement this policy in their respective areas.

Additional Points:

Training and Awareness: Regular training and awareness programs for employees regarding the importance of access control and adherence to the policy.

Audit and Monitoring: Regular audits and monitoring to ensure compliance with the policy.

Incident Response: A clear incident response plan in case of unauthorized access or breaches.

This Access Control Policy is a starting point and should be customized to the specific needs and context of the organization. Regular reviews and updates are essential to adapt to new threats, technologies, and business changes.

**M4:** Please develop Encryption Policy that adheres to the encryption requirements of ISO 27001 to protect sensitive data.

**GAI3-M4:**

Creating an Encryption Policy that aligns with ISO 27001 standards is essential for safeguarding sensitive data through appropriate cryptographic measures. ISO 27001 provides a framework for

information security management, and encryption plays a key role in protecting the confidentiality, integrity, and availability of data. Here's an outline for an Encryption Policy:

## Encryption Policy

### 1. Purpose:

To establish guidelines for using encryption to protect the confidentiality, integrity, and availability of sensitive data in line with ISO 27001 standards.

### 2. Scope:

This policy applies to all employees, contractors, and third parties who handle [Company Name]'s sensitive data across all forms of digital media.

### 3. Policy Statements:

#### 3.1 Encryption Standards:

3.1.1 Approved Algorithms: Only industry-standard cryptographic algorithms (e.g., AES, RSA) that meet or exceed the minimum key lengths recommended by ISO 27001 will be used.

3.1.2 Key Management: Robust key management practices must be followed, including secure generation, storage, exchange, use, and destruction of cryptographic keys.

#### 3.2 Data at Rest:

3.2.1 Storage Encryption: Sensitive data stored on any device or medium must be encrypted, including servers, laptops, and removable media.

3.2.2 Database Encryption: Databases containing sensitive information must use encryption or other cryptographic protection methods.

#### 3.3 Data in Transit:

3.3.1 Transmission Security: Data transmitted across public or untrusted networks must be encrypted using secure protocols such as TLS/SSL.

3.3.2 Email Security: Sensitive information sent via email must be encrypted or secured through secure email gateways.

#### 3.4 End-User Devices:

3.4.1 Device Encryption: Laptops, smartphones, and other mobile devices that store sensitive data must have full disk encryption enabled.

3.4.2 Portable Media: Use of encrypted USB drives or other portable media when transferring sensitive information.

#### 3.5 Cloud Services and Third Parties:

3.5.1 Cloud Storage Encryption: Use of encryption for sensitive data stored in cloud services.

3.5.2 Vendor Compliance: Third-party vendors handling sensitive data must comply with the encryption standards of this policy.

#### 4. Compliance:

Violation of this policy can result in disciplinary action and may have legal or regulatory consequences.

#### 5. Policy Review and Modification:

This policy will be reviewed annually or in response to significant changes in technology or business practices to ensure ongoing relevance and effectiveness.

#### 6. Approval and Implementation:

This policy is approved by [Top Management/CEO/Board] and must be fully implemented by all relevant personnel and departments.

#### Additional Points:

**Training and Awareness:** Regular training for employees on the importance of encryption and correct procedures for encrypting data.

**Incident Response:** Procedures for reporting and responding to suspected incidents involving unencrypted sensitive data.

**Auditing and Monitoring:** Regular audits to ensure compliance with the encryption policy and effectiveness of the encryption measures.

This Encryption Policy serves as a framework and should be tailored to meet the specific operational and data protection needs of the organization. It's important to keep the policy updated in line with emerging threats, technological advances, and changes in regulatory requirements.

**M5:** Please develop an Information Security Risk Management Policy in accordance with ISO 27001 aimed at effective security risk identification, management, and treatment.

#### **GAI3-M5:**

Developing an Information Security Risk Management Policy in accordance with ISO 27001 involves establishing a systematic approach to managing and mitigating risks that can affect the organization's information assets. ISO 27001 emphasizes the importance of assessing and treating risks in a way that's consistent with the organization's overall risk appetite and security goals. Here's an outline for an Information Security Risk Management Policy:

#### Information Security Risk Management Policy

##### 1. Purpose:

To outline the approach for identifying, assessing, managing, and mitigating information security risks in line with ISO 27001 standards, ensuring the protection of organizational assets and the integrity, confidentiality, and availability of information.

## 2. Scope:

This policy applies to all employees, contractors, and third parties involved in the management of information systems and data within [Company Name].

## 3. Policy Statements:

### 3.1 Risk Assessment:

3.1.1 Risk Identification: Regularly identify risks associated with the loss, damage, or unauthorized access to information assets.

3.1.2 Risk Analysis and Evaluation: Analyze and evaluate risks by considering the likelihood and impact of security incidents.

### 3.2 Risk Treatment:

3.2.1 Risk Treatment Options: Implement appropriate risk treatment options, including risk avoidance, mitigation, transfer, or acceptance.

3.2.2 Risk Mitigation: Where risk mitigation is chosen, apply suitable controls to reduce risks to an acceptable level.

### 3.3 Risk Acceptance:

3.3.1 Acceptance Criteria: Establish clear criteria for accepting risks that align with the organization's risk appetite and business objectives.

3.3.2 Documentation: Document all accepted risks and the rationale for acceptance.

### 3.4 Communication and Consultation:

3.4.1 Internal Communication: Ensure effective internal communication regarding risks and risk management strategies.

3.4.2 External Consultation: Engage with external parties where necessary for risk assessment and treatment.

### 3.5 Monitoring and Review:

3.5.1 Ongoing Monitoring: Regularly monitor and review risks, the effectiveness of controls, and changes in the external and internal context.

3.5.2 Continuous Improvement: Adapt and improve the risk management process based on monitoring and review findings.

### 3.6 Compliance:

3.6.1 Legal and Regulatory Compliance: Ensure that risk management practices comply with applicable legal, regulatory, and contractual requirements.

## 4. Roles and Responsibilities:

Define clear roles and responsibilities for risk management activities, including a Risk Manager or Risk Management Team.

### 5. Training and Awareness:

Provide training and raise awareness about risk management policies and procedures among all relevant personnel.

### 6. Policy Review and Modification:

Review and update this policy annually or in response to significant changes in the risk landscape or business operations.

### 7. Approval and Implementation:

This policy is approved by [Top Management/CEO/Board] and must be implemented across the organization.

#### Additional Points:

**Risk Assessment Methodology:** Adopt a formal risk assessment methodology that is consistent and repeatable.

**Asset Inventory:** Maintain an up-to-date inventory of information assets to be included in the risk assessment process.

**Risk Register:** Keep a risk register to track identified risks, their status, and treatment plans.

**Incident Management:** Implement an incident management process to handle security breaches or incidents effectively.

This Information Security Risk Management Policy is a framework that needs to be customized according to the specific context, operations, and risk appetite of the organization. Regular updates and continuous management are crucial for its effectiveness.

**M6:** Please develop Secure Software Development Lifecycle Policy as per ISO 27001 requirements ensuring the security of software throughout the development lifecycle.

#### **GAI3-M6:**

Creating a Secure Software Development Lifecycle (SSDLC) Policy in line with ISO 27001 requirements involves establishing a framework to ensure the integration of security practices throughout the software development process. ISO 27001 emphasizes the need for systematic management of sensitive information, and incorporating security into the software development lifecycle is critical to this end. Here's an outline for a Secure Software Development Lifecycle Policy:

#### Secure Software Development Lifecycle Policy

##### 1. Purpose:

To define the standards and practices for ensuring security is integrated throughout the software development lifecycle (SDLC) in compliance with ISO 27001.

##### 2. Scope:

This policy applies to all software development projects within [Company Name], including those developed in-house or outsourced to third parties.

### 3. Policy Statements:

#### 3.1 Security Requirements:

3.1.1 Requirements Analysis: Identify and document security requirements in the early stages of the SDLC.

3.1.2 Regulatory Compliance: Ensure software compliance with relevant legal, regulatory, and contractual requirements.

#### 3.2 Secure Design:

3.2.1 Security Architecture: Develop a secure architecture for all software projects.

3.2.2 Design Review: Conduct security-focused reviews of software designs.

#### 3.3 Secure Coding:

3.3.1 Coding Standards: Adhere to secure coding standards and guidelines.

3.3.2 Code Review: Perform regular code reviews to identify security vulnerabilities and coding flaws.

#### 3.4 Testing and Validation:

3.4.1 Security Testing: Implement thorough security testing at various stages of the SDLC.

3.4.2 Vulnerability Assessment: Regularly conduct vulnerability assessments and penetration testing.

#### 3.5 Deployment and Maintenance:

3.5.1 Secure Deployment: Ensure secure deployment practices for software releases.

3.5.2 Patch Management: Establish a process for timely application of security patches and updates.

#### 3.6 Training and Awareness:

3.6.1 Developer Training: Provide regular security training and awareness programs for developers and relevant staff.

3.6.2 Knowledge Sharing: Encourage sharing of security knowledge and best practices within the development team.

### 4. Roles and Responsibilities:

Define clear roles and responsibilities for security in the software development process.

### 5. Third-Party Security:

5.1 Vendor Management: Ensure that third-party vendors and partners adhere to this policy and ISO 27001 standards.

5.2 Security in Contracts: Include security requirements and responsibilities in contracts with third parties.

#### 6. Incident Management:

Implement an incident management process to respond to software security incidents effectively.

#### 7. Policy Review and Modification:

This policy will be reviewed and updated annually or in response to significant changes in the technology or threat landscape.

#### 8. Approval and Implementation:

This policy is approved by [Top Management/CEO/Board] and must be fully implemented by all software development teams and relevant departments.

#### Additional Points:

**Risk Management:** Integrate risk management into the SDLC process.

**Continuous Monitoring:** Implement continuous monitoring and feedback mechanisms throughout the SDLC.

**Documentation:** Maintain comprehensive documentation for all stages of the SDLC.

**Compliance Audits:** Regularly audit the software development processes for compliance with this policy.

This Secure Software Development Lifecycle Policy serves as a foundation to embed security into every aspect of software development. It should be tailored to fit the specific context and needs of the organization and reviewed regularly to ensure it remains effective and relevant.

**M7:** Could you please develop Security Awareness and Training Policy in accordance with ISO 27001 to raise awareness about information security among employees?

#### **GAI3-M7:**

Creating a Security Awareness and Training Policy in accordance with ISO 27001 is a vital component in ensuring that all employees understand their roles and responsibilities regarding information security. ISO 27001 emphasizes the importance of continuous education and awareness to maintain a secure information environment. Here's an outline for a Security Awareness and Training Policy:

#### Security Awareness and Training Policy

##### 1. Purpose:

To provide a framework for delivering continuous and effective security awareness, education, and training to all employees to enhance the organization's overall information security posture as per ISO 27001 standards.

##### 2. Scope:



This policy applies to all employees, contractors, and third-party users of [Company Name]'s information systems and services.

### 3. Policy Statements:

#### 3.1 Security Awareness Program:

3.1.1 Regular Awareness Sessions: Conduct regular security awareness sessions to keep staff informed about current security threats and practices.

3.1.2 Orientation Sessions: Include information security awareness in the induction process for all new employees.

#### 3.2 Training:

3.2.1 Mandatory Training: Implement mandatory information security training for all employees, tailored to their specific roles.

3.2.2 Advanced Training: Provide advanced, role-specific training for employees in sensitive positions or with special security responsibilities.

#### 3.3 Continuous Learning:

3.3.1 Regular Updates: Regularly update training content to reflect the latest security threats, trends, and best practices.

3.3.2 E-Learning Modules: Utilize e-learning modules for easy access to training materials and flexibility.

#### 3.4 Communication:

3.4.1 Regular Communication: Disseminate regular communications regarding security tips, incident reports, and policy updates.

3.4.2 Feedback Mechanism: Implement a feedback mechanism for employees to share their insights or concerns about information security.

#### 3.5 Testing and Evaluation:

3.5.1 Knowledge Assessment: Conduct regular assessments to measure the effectiveness of the security training and awareness programs.

3.5.2 Phishing Simulations: Use simulated phishing exercises to assess employee vigilance against email threats.

### 4. Roles and Responsibilities:

Define clear roles and responsibilities for managing, delivering, and participating in security awareness and training programs.

### 5. Compliance:

5.1 Participation Tracking: Maintain records of all training and awareness activities, including employee participation.

5.2 Non-Compliance Consequences: Address non-compliance with this policy as per the organization's disciplinary process.

#### 6. Policy Review and Modification:

Review and update this policy annually or in response to significant changes in the threat landscape or business operations.

#### 7. Approval and Implementation:

This policy is approved by [Top Management/CEO/Board] and must be implemented across the organization.

#### Additional Points:

Customized Content: Tailor training content to be relevant and understandable for different departments and roles.

Security Champions: Establish 'Security Champions' within departments to advocate best practices and assist in disseminating information.

Engaging Formats: Use engaging training formats, such as videos, workshops, and interactive quizzes.

This Security Awareness and Training Policy is designed to embed a culture of security within the organization. It should be regularly reviewed and updated to stay effective and relevant, ensuring that all employees are equipped with the necessary knowledge and skills to protect organizational information assets.

**M8:** What regulations should be followed in case our EU-based company provides software development services for client in California, who requires us to work with personal data?

#### **GAI3-M8:**

For an EU-based company providing software development services to a client in California and handling personal data, there are several key regulations and standards to be aware of and comply with:

1. **General Data Protection Regulation (GDPR):** Since your company is based in the EU, GDPR applies to all your operations, regardless of where your clients are located. GDPR imposes strict rules on data processing, data subjects' rights, and the transfer of personal data outside the EU. Ensure that your data processing activities align with GDPR principles, especially regarding lawful processing, data minimization, and data subject consent.
2. **California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA):** These are California's primary privacy laws. The CCPA, and its successor, the CPRA, grant California residents various rights regarding their personal information, similar to GDPR. These include the right to know about the personal information a business collects about them and how it is used and shared, the right to delete personal information collected, the right to opt-out of the sale of their personal information, and the right to non-discrimination for exercising their CCPA rights.

3. **Contractual Agreements and Data Processing Agreements (DPAs):** Ensure that contracts with your California-based clients include provisions and Data Processing Agreements that address compliance with GDPR, CCPA/CPRA, and any other relevant data protection laws. This should cover aspects like the purpose of data processing, the types of data being processed, and the responsibilities of each party in protecting that data.
4. **ISO/IEC 27001:** While not a regulation, adhering to this international standard for an information security management system (ISMS) can significantly help in meeting regulatory requirements. It provides a framework for data security and privacy that aligns well with the requirements of GDPR and CCPA/CPRA.
5. **Standard Contractual Clauses (SCCs):** For transferring personal data from the EU to California, ensure the use of Standard Contractual Clauses (SCCs), which are legal tools to provide sufficient safeguards for data transfers from the EU to third countries.
6. **Cybersecurity Frameworks:** Consider adopting cybersecurity frameworks like NIST (National Institute of Standards and Technology), which, while American, can provide a robust approach to managing cybersecurity risks.
7. **Employee Training and Awareness:** Regular training for your employees on GDPR, CCPA/CPRA, and general data protection best practices is crucial. This helps in ensuring that your team is aware of their obligations when handling personal data.
8. **Data Breach Notification Laws:** Be aware of both EU and California data breach notification laws. You must understand the requirements for notifying supervisory authorities and data subjects in case of a data breach.

By adhering to these regulations and implementing robust data protection and privacy measures, your company can ensure compliance and maintain the trust of your clients and their customers.

### **Generated responses by GAI3 Model for Consultant role**

**C1:** Which security policies should be developed for EU-based software development company with 500 employees based on ISO27001?

**GAI3-C1:**

For a European Union-based software development company with 500 employees, developing security policies in line with ISO 27001 standards is crucial. ISO 27001 is a global standard for information security management systems (ISMS). Here are some key security policies that should be developed:

1. **Information Security Policy:** This is the overarching policy that sets the tone for information security in the organization. It should include commitments to protect information, adhere to legal requirements, and continually improve the ISMS.
2. **Access Control Policy:** This policy should define how access to various systems and data is granted, managed, and revoked. It should include provisions for user registration and de-registration, user access provisioning, management of privileged access rights, and control of network access.
3. **Data Protection and Privacy Policy:** Considering the EU's GDPR, this policy should address how personal and sensitive data is collected, processed, stored, and disposed of.

4. **Incident Management Policy:** This policy outlines the process for managing information security incidents and improvements.
5. **Asset Management Policy:** It involves identifying information assets and defining appropriate protection responsibilities.
6. **User Security Policy:** This policy should address user responsibilities, including security training and awareness, acceptable use of assets, and adherence to security practices.
7. **Network Security Management:** This includes policies for managing secure operation of networks, including protection from malware and managing network vulnerabilities.
8. **Physical and Environmental Security Policy:** This policy should outline protection of the physical and environmental aspects of the company's premises, including access control and protection from natural disasters or unauthorized access.
9. **Operations Security Policy:** This covers the management and protection of information processing facilities, including change management and backup.
10. **Communication Security Policy:** This involves protecting the confidentiality, integrity, and availability of information in networks and its supporting information processing facilities.
11. **Supplier Relationship Security Policy:** Since software development often involves third-party services and software, this policy should address how to manage supplier relationships, including their access to the company's information assets.
12. **Compliance Policy:** This policy ensures that the organization complies with legislative, regulatory, and contractual requirements regarding data security.
13. **Business Continuity Management:** Addresses how the business will continue in the event of unforeseen interruptions.

Remember, these policies should be tailored to the specific context and needs of your organization, and should be regularly reviewed and updated as necessary. Additionally, employee training and awareness are key to effectively implementing these policies.

**C2:** Could you please develop Statement of Applicability for ISO27001 for EU-based software development company with 500 employees?

### **GAI3-C2:**

Creating a Statement of Applicability (SoA) for an EU-based software development company with 500 employees in accordance with ISO 27001 involves several steps. The SoA is a critical document in the ISO 27001 process as it details which of the ISO 27001 Annex A controls are applicable to the organization and how they are implemented or justified if deemed not applicable. Here's a framework to guide you through this process:

#### **1. Introduction**

- **Company Overview:** Briefly describe your company, including its size, scope, and the nature of its software development activities.

- Purpose of the SoA: State that the SoA is designed to meet the requirements of ISO 27001 and to ensure the confidentiality, integrity, and availability of information.

## 2. Scope of the ISMS

- Define the scope of your Information Security Management System (ISMS). This might include all processes, locations, and data related to software development and corporate operations.

## 3. ISO 27001 Annex A Controls

- Annex A contains 114 controls in 14 categories. For each category, list the controls and state whether they are applicable or not, along with a brief justification. Examples of these controls include:
  - **Information Security Policies (A.5):** State if your company has established and reviewed information security policies.
  - **Organization of Information Security (A.6):** Describe how your organization assigns responsibilities for information security.
  - **Human Resource Security (A.7):** Explain the controls for ensuring employee, contractor, and third-party user security throughout their lifecycle (prior to employment, during, and post-termination).
  - **Asset Management (A.8):** Detail how organizational assets are identified, classified, and handled.
  - **Access Control (A.9):** Describe how access to systems and data is managed and controlled.
  - **Cryptography (A.10):** Explain the use of cryptographic controls.
  - **Physical and Environmental Security (A.11):** Detail physical security controls and environmental protections for your facilities.
  - **Operations Security (A.12):** Describe the management of operational procedures and responsibilities.
  - **Communications Security (A.13):** Explain how information in networks and its supporting information processing facilities is protected.
  - **System Acquisition, Development and Maintenance (A.14):** State controls for ensuring security in development and support processes.
  - **Supplier Relationships (A.15):** Explain how your company manages supplier relationships to ensure that external parties have access to information assets only as required.
  - **Information Security Incident Management (A.16):** Describe the mechanisms for reporting and managing information security events and weaknesses.
  - **Information Security Aspects of Business Continuity Management (A.17):** State how business continuity and information security are incorporated.

- **Compliance (A.18):** Describe the identification and adherence to laws, regulations, and contractual obligations.

#### 4. **Justification for Inclusions and Exclusions**

- For each control that is applicable, briefly describe how it is implemented or how it will be implemented.
- For each control that is not applicable, provide a clear justification for its exclusion.

#### 5. **Review and Approval**

- The SoA should be reviewed and approved by top management to ensure it aligns with business objectives and risk management strategy.

#### 6. **Revision History**

- Maintain a revision history to track changes and updates to the SoA over time.

Remember, the SoA is a living document and should be reviewed and updated regularly to reflect any changes in the organization's ISMS, risk profile, or other relevant circumstances. The implementation of each control should be aligned with the risk assessment and treatment plan of the organization. This is a high-level guide, and the actual SoA should be detailed and specific to your organization's needs and context.

**C3:** Develop a procedure on how to implement access controls in accordance with ISO27001 within the EU-based software development company.

#### **GAI3-C3:**

Implementing access controls in accordance with ISO 27001 within an EU-based software development company involves a systematic approach to managing and controlling access to both physical and logical assets. Here is a procedure that outlines the key steps:

##### **1. Policy Development**

- **Define an Access Control Policy:** Develop a comprehensive access control policy in line with ISO 27001 requirements. This policy should outline the principles for accessing physical locations, systems, and data.

##### **2. Identify Assets and Access Requirements**

- **Asset Inventory:** Create an inventory of all information assets.
- **Access Classification:** Classify each asset based on its sensitivity and criticality.
- **Determine Access Requirements:** For each asset, define who needs access and the level of access required.

##### **3. User Registration and Management**

- **User Registration:** Implement a formal user registration process to grant access rights.

- **Role-Based Access Control (RBAC):** Define roles and associate them with specific access permissions.
- **Review and Update User Access:** Regularly review user access rights and adjust as necessary, particularly when employees change roles or leave the company.

#### 4. Implement Authentication Mechanisms

- **Authentication Protocols:** Use strong authentication methods such as multi-factor authentication (MFA) for accessing sensitive systems and data.
- **Password Management:** Establish and enforce a strong password policy.

#### 5. Physical Access Controls

- **Secure Areas:** Restrict access to physical areas where critical assets are located.
- **Access Control Systems:** Use access cards, biometrics, or other secure methods to control entry to sensitive areas.

#### 6. Logical Access Controls

- **Access Rights Assignment:** Assign access rights based on the principle of least privilege.
- **System Configuration:** Configure systems and networks to enforce access controls.
- **Encryption:** Use encryption to protect sensitive data in transit and at rest.

#### 7. Monitoring and Logging

- **Audit Trails:** Implement logging mechanisms to record access events, both for physical and logical access.
- **Regular Monitoring:** Continuously monitor access control systems for any unauthorized access attempts or breaches.

#### 8. Incident Management

- **Incident Response Plan:** Develop a plan for responding to access control breaches.
- **Incident Reporting:** Establish a process for reporting security incidents related to unauthorized access.

#### 9. Awareness and Training

- **Employee Training:** Conduct regular training sessions to educate employees about access control policies and procedures.
- **Awareness Programs:** Implement ongoing awareness programs to reinforce the importance of access control.

#### 10. Review and Audit

- **Regular Reviews:** Periodically review the access control policies and procedures to ensure they remain effective and compliant with ISO 27001.

- **Internal Audits:** Conduct internal audits to assess the effectiveness of access control measures.

## 11. Continuous Improvement

- **Feedback Mechanism:** Implement a feedback mechanism to gather insights from employees on access control practices.
- **Update Procedures:** Continually improve access control procedures based on audit findings, feedback, and evolving best practices.

## Documentation and Records

- **Documenting Procedures:** Maintain detailed documentation of all access control policies, procedures, and records.
- **Record Keeping:** Keep accurate records of user access levels, authentication protocols, and incident response actions.

Implementing this procedure will help ensure that access to the company's information assets is appropriately managed and controlled, reducing the risk of unauthorized access and ensuring compliance with ISO 27001 standards.

**C4:** Could you please create a detailed guideline on what should be done in order to implement Encryption policy in accordance with ISO27001 within EU-based software development company?

### GAI3-C4:

Implementing an encryption policy in accordance with ISO 27001 within an EU-based software development company involves several key steps. Here's a detailed guideline:

#### 1. Policy Development

- **Draft an Encryption Policy:** Create a comprehensive encryption policy document. This policy should define the purpose, scope, and objectives of encryption in protecting sensitive data. It should align with the overall information security policy of the company.

#### 2. Identify Sensitive Data

- **Data Classification:** Classify data based on sensitivity and confidentiality. Identify which data requires encryption based on its classification.

#### 3. Risk Assessment

- **Conduct Risk Assessment:** Assess risks associated with the data to be encrypted. Consider potential threats and vulnerabilities, and how encryption can mitigate these risks.

#### 4. Encryption Standards and Protocols

- **Select Encryption Standards:** Choose industry-recognized encryption standards (e.g., AES, RSA, TLS) that meet ISO 27001 requirements.
- **Protocols for Different Data States:** Define protocols for data at rest, in transit, and in use.

#### 5. Key Management



- **Key Generation and Storage:** Implement secure methods for cryptographic key generation, storage, and disposal.
- **Access to Keys:** Restrict access to cryptographic keys to authorized personnel only.
- **Key Lifecycle Management:** Define a lifecycle for keys including creation, distribution, usage, storage, and destruction.

## 6. Implementation

- **Encryption Solutions:** Deploy encryption solutions for data at rest (e.g., databases, files) and data in transit (e.g., email, web traffic).
- **Integrate with Existing Systems:** Ensure that encryption mechanisms are compatible with existing IT infrastructure and systems.

## 7. User Access Controls

- **Access Control Policies:** Implement strict access controls to ensure that only authorized individuals can decrypt or have access to encrypted data.

## 8. Training and Awareness

- **Employee Training:** Train employees on the importance of encryption and how to use encryption tools properly.
- **Awareness Programs:** Conduct awareness programs to reinforce the importance of protecting sensitive data.

## 9. Monitoring and Auditing

- **Audit Trails:** Maintain audit trails for all encryption-related activities.
- **Regular Audits:** Conduct regular audits to ensure compliance with the encryption policy.

## 10. Legal and Compliance

- **Comply with Legal Requirements:** Ensure that the use of encryption complies with EU laws and regulations (e.g., GDPR).
- **International Data Transfer:** Address any restrictions or considerations for encrypted data transferred outside the EU.

## 11. Incident Management

- **Encryption Key Compromise:** Establish procedures for responding to incidents such as the compromise of encryption keys.

## 12. Review and Update

- **Policy Review and Update:** Regularly review and update the encryption policy to adapt to changing threats, business needs, and technological advancements.

## 13. Documenting and Reporting

- **Documentation:** Keep detailed documentation of the encryption policy, procedures, and audit records.
- **Reporting:** Report on the status of encryption practices to management and relevant stakeholders.

#### 14. Technical Implementations

- **Secure Configurations:** Ensure that encryption implementations are configured securely to avoid vulnerabilities.
- **Regular Testing:** Periodically test the strength and effectiveness of encryption implementations.

#### Conclusion

By following these steps, the company will be able to implement a robust encryption policy that meets the requirements of ISO 27001, ensuring the confidentiality, integrity, and availability of sensitive data. This policy should be regularly reviewed and updated to remain effective and relevant.

**C5:** Please develop a detailed procedure on how to assess risks in accordance with ISO27001 at EU-based software development company, what scales should be used to define risk levels and provide several examples of how risk register should look like?

#### GAI3-C5:

Developing a detailed risk assessment procedure in accordance with ISO 27001 for an EU-based software development company involves several critical steps. Here's a structured approach to this process:

##### 1. Establish the Risk Assessment Framework

- **Define the Risk Assessment Methodology:** Choose a risk assessment methodology that suits the company's context (e.g., qualitative, quantitative, or a combination of both).
- **Develop Risk Criteria:** Establish criteria for risk evaluation. Define what constitutes low, medium, and high risks in terms of potential impact and likelihood.

##### 2. Scope and Context Establishment

- **Define the Scope:** Clearly outline the scope of the risk assessment, including systems, processes, and locations.
- **Understand the Context:** Understand the internal and external context of the organization, including legal, regulatory, and business environment.

##### 3. Asset Identification and Valuation

- **Asset Inventory:** Create a comprehensive inventory of all information assets.
- **Asset Valuation:** Assign a value to each asset based on criteria like confidentiality, integrity, and availability.

#### 4. Threat and Vulnerability Identification

- **Identify Threats:** List potential threats that could exploit vulnerabilities in the organization's assets.
- **Identify Vulnerabilities:** Determine vulnerabilities in each asset that could be exploited by the identified threats.

#### 5. Risk Estimation

- **Likelihood Determination:** Assess the likelihood of each threat exploiting a vulnerability.
- **Impact Assessment:** Evaluate the potential impact on the organization if the threat materializes.
- **Risk Level Assessment:** Use a risk matrix to determine the risk level (e.g., Low, Medium, High) based on likelihood and impact.

#### 6. Risk Evaluation

- **Compare Against Criteria:** Evaluate the identified risks against the established risk criteria to prioritize them.

#### 7. Risk Treatment

- **Identify Treatment Options:** Determine options for treating each risk (avoid, mitigate, transfer, accept).
- **Develop Risk Treatment Plans:** For each risk that needs mitigation, develop a treatment plan.

#### 8. Risk Register Creation

- **Document in Risk Register:** Record all identified risks, their evaluation, and treatment plans in a risk register.

#### 9. Review and Monitoring

- **Regular Review:** Regularly review and update the risk assessment and risk register.
- **Monitor Risks:** Continuously monitor the risks and the effectiveness of treatment plans.

#### Risk Scales

For defining risk levels, you can use scales such as:

- **Likelihood:** Rare, Unlikely, Possible, Likely, Almost Certain.
- **Impact:** Insignificant, Minor, Moderate, Major, Catastrophic.

#### Example of Risk Register Entries

1. **Risk ID:** 001
  - **Asset:** Customer Database
  - **Threat:** Unauthorized Access

- **Vulnerability:** Insufficient Access Controls
  - **Likelihood:** Likely
  - **Impact:** Major
  - **Risk Level:** High
  - **Treatment Plan:** Implement stronger access controls, regular audits.
2. **Risk ID:** 002
- **Asset:** Source Code Repository
  - **Threat:** Malware Attack
  - **Vulnerability:** Outdated Antivirus Software
  - **Likelihood:** Possible
  - **Impact:** Major
  - **Risk Level:** Medium
  - **Treatment Plan:** Update antivirus software, conduct regular security training for developers.
3. **Risk ID:** 003
- **Asset:** Internal Communication Tool
  - **Threat:** Data Breach through Phishing
  - **Vulnerability:** Lack of Employee Awareness
  - **Likelihood:** Unlikely
  - **Impact:** Moderate
  - **Risk Level:** Low
  - **Treatment Plan:** Implement phishing awareness training, regular security drills.

By following this procedure and regularly updating the risk register, the company can ensure a comprehensive and effective risk management process in line with ISO 27001 standards.

**C6:** How to ensure the implementation of secure SDLC controls on the projects conforming to ISO27001 at EU-based software development company?

**GAI3-C6:**

Ensuring the implementation of secure Software Development Life Cycle (SDLC) controls in projects that conform to ISO 27001 at an EU-based software development company involves integrating security into every phase of the development process. Here's how to achieve this:

**1. Define Security Requirements**

- **Integrate Security in Project Requirements:** Include security requirements from the very beginning of the project. Align these requirements with ISO 27001 standards, legal and regulatory requirements, particularly GDPR for data protection in the EU.

## 2. Secure Design

- **Security by Design:** Ensure that security is an integral part of the system architecture and design. Use secure design principles and practices like least privilege, separation of duties, and defense in depth.
- **Threat Modeling:** Perform threat modeling in the design phase to identify potential security threats and vulnerabilities.

## 3. Secure Development

- **Coding Standards:** Adopt secure coding standards and guidelines. Ensure developers are trained in these standards.
- **Code Review and Analysis:** Implement regular code reviews and utilize static and dynamic code analysis tools to identify and fix security vulnerabilities.

## 4. Data Protection and Privacy

- **Data Encryption:** Encrypt sensitive data in transit and at rest.
- **Data Minimization and Anonymization:** Follow the principles of data minimization and anonymization as per GDPR.

## 5. Secure Testing

- **Security Testing:** Conduct comprehensive security testing, including penetration testing, vulnerability scanning, and application security testing, in the testing phase of the SDLC.
- **Fix and Re-test:** Ensure that any vulnerabilities found are fixed and re-tested.

## 6. Change Management

- **Secure Change Management:** Use a secure change management process to handle updates and changes, ensuring that all changes are reviewed for potential security impacts.

## 7. Deployment and Maintenance

- **Secure Deployment:** Ensure secure deployment practices, including the use of secure deployment environments and verifying the integrity of the software during deployment.
- **Regular Updates and Patch Management:** Implement a process for regular software updates and patch management to address new security vulnerabilities.

## 8. Training and Awareness

- **Developer Training:** Train developers in secure coding practices, new security technologies, and emerging threats.
- **Security Awareness:** Promote security awareness across the organization.

## 9. Documentation and Record Keeping

- **Document Security Practices:** Maintain comprehensive documentation of all security practices and procedures used throughout the SDLC.
- **Audit Trails:** Keep audit trails of all security-related activities and decisions.

## 10. Supplier Security

- **Third-Party Security:** If using third-party components, ensure they meet your security standards. Perform due diligence on third-party vendors.

## 11. Continuous Monitoring and Incident Management

- **Monitor for Security Incidents:** Continuously monitor the software for security incidents or breaches.
- **Incident Response Plan:** Have a robust incident response plan in place.

## 12. Compliance and Review

- **Regular Compliance Checks:** Regularly check for compliance with ISO 27001, GDPR, and other relevant standards.
- **Review and Improve:** Continuously review and improve security practices in the SDLC.

## 13. Risk Management Integration

- **Risk Assessment:** Integrate risk assessment within the SDLC, ensuring risks are identified, evaluated, and mitigated throughout the development process.

By systematically integrating these controls into the SDLC, the company can ensure that its software development projects are secure and compliant with ISO 27001 standards, as well as other relevant regulations and best practices in the industry.

**C7:** Could you please develop Information Security Awareness Program conforming to ISO27001, including regular training sessions on security policies, procedures, and best practices?

### GAI3-C7:

Developing an Information Security Awareness Program conforming to ISO 27001 involves creating a structured plan that promotes a culture of security awareness within the organization. Here's a comprehensive outline for such a program:

#### 1. Program Objectives

- Establish clear objectives for the awareness program, such as increasing knowledge of security threats, understanding of company security policies, and promoting responsible behavior.

#### 2. Target Audience Identification

- Identify different target audiences within the organization (e.g., developers, HR, management) and tailor the content according to their roles and responsibilities.

### 3. Content Development

- Develop training content covering key areas such as company security policies, data protection (GDPR), incident reporting, password management, phishing, and social engineering.

### 4. Training Methodology

- Use a mix of training methods such as e-learning, workshops, seminars, webinars, and infographics to cater to different learning preferences.
- Include interactive elements like quizzes, games, and discussions to enhance engagement.

### 5. Regular Training Sessions

- **Introduction to Information Security:** Basics of information security, importance of ISO 27001, and an overview of the ISMS.
- **Company-Specific Security Policies:** Detailed sessions on company-specific security policies, procedures, and their importance.
- **Data Protection and Privacy:** Training on GDPR and other relevant data protection laws, focusing on personal data handling, consent, and data subject rights.
- **Cybersecurity Best Practices:** Sessions on password management, secure browsing, email security, and safe use of social media.
- **Phishing and Social Engineering:** Training on recognizing and responding to phishing attempts and social engineering tactics.
- **Physical Security:** Guidelines on securing physical assets, access controls, and dealing with visitors.
- **Incident Reporting and Response:** Procedures for reporting security incidents and the importance of timely reporting.
- **Advanced Topics for IT Staff:** For IT and security teams, include advanced topics like network security, cryptography, and incident handling.

### 6. Schedule and Frequency

- Plan a regular schedule for training sessions, such as quarterly or bi-annually, and ensure all new employees receive training as part of their onboarding process.

### 7. Communication Plan

- Communicate the importance of the program to all employees. Use emails, newsletters, or company meetings to remind and encourage participation.

### 8. Assessment and Feedback

- Conduct assessments after training sessions to measure understanding and retention.
- Collect feedback to continuously improve the program.

### 9. Monitoring and Reporting

- Track participation and completion rates of training sessions.
- Regularly report on the program's progress and effectiveness to management.

#### **10. Continuous Improvement**

- Regularly review and update the training content to reflect the latest threats, technological changes, and compliance requirements.
- Incorporate insights and feedback from employees to make the program more effective and engaging.

#### **11. Security Champions**

- Appoint security champions within each department who can reinforce the message and assist colleagues with security queries.

#### **12. Awareness Campaigns**

- Conduct regular awareness campaigns on current security topics, such as recent phishing tactics or security updates.

#### **13. Recognition and Incentives**

- Implement a system to recognize and reward the most engaged and proactive employees in security training and practices.

#### **14. Management Involvement**

- Ensure management actively participates in and supports the awareness program, setting an example for the rest of the organization.

#### **15. Documentation and Compliance**

- Maintain documentation of all training materials, attendance records, and assessment results as part of compliance with ISO 27001.

By implementing this program, the company can significantly enhance its security posture and foster a culture where every employee understands their role in maintaining information security, in line with ISO 27001 standards.

**C8:** Are there any privacy risks or concerns that should be taken into account while developing software under CCPA regulation?

#### **GAI3-C8:**

When developing software under the California Consumer Privacy Act (CCPA) regulations, there are several privacy risks and concerns that need to be taken into account. The CCPA provides California residents with specific rights regarding their personal information and sets requirements for businesses that collect, process, or sell personal information. Here are key considerations:

##### **1. Data Collection and Minimization**



- Collect only the data necessary for the intended purpose. Avoid unnecessary collection of personal information, which can increase privacy risks and liability under CCPA.
- 2. Consent and Choice**
    - Obtain clear consent from users for the collection and use of their personal information. Provide users with options to opt-out of data collection, particularly for the sale of their personal information.
  - 3. Transparency and Notice**
    - Be transparent about data collection practices. This includes providing clear privacy notices at or before the point of collection, detailing the categories of personal data collected, the purpose for collection, and how it will be used.
  - 4. Data Subject Rights**
    - Implement mechanisms to respond to consumer requests. Under CCPA, consumers have the right to know about, access, delete, and opt-out of the sale of their personal information.
    - Ensure the software has functionalities to facilitate these rights, such as easy access to personal data, mechanisms to request data deletion, and opt-out options.
  - 5. Data Security**
    - Implement reasonable security measures to protect personal data from unauthorized access, disclosure, alteration, and destruction. This includes encryption, access controls, and secure data storage and transmission.
  - 6. Third-Party Data Sharing and Selling**
    - If the software involves sharing personal information with third parties, ensure transparency and control over this process.
    - Obtain explicit consent if personal information is sold, and provide a clear and straightforward way for users to opt-out of the sale.
  - 7. Age Verification**
    - Include age verification mechanisms if the software collects information from minors. CCPA has stricter requirements for minors under 16, including the requirement of opt-in consent.
  - 8. Data Inventory and Mapping**
    - Maintain an inventory of personal information that the software handles. Understand where data is stored, how it flows through the system, and with whom it is shared.
  - 9. Privacy by Design**
    - Integrate privacy considerations into the software development lifecycle. This includes conducting privacy impact assessments during design phases to identify and mitigate privacy risks.

## 10. Vendor Management

- Ensure that any third-party service providers or vendors who handle personal information on behalf of the software are compliant with CCPA.

## 11. Training and Awareness

- Train staff involved in the development and management of the software on CCPA requirements and the importance of privacy protection.

## 12. Record Keeping

- Keep records of data processing activities, consent, and consumer requests to demonstrate compliance with CCPA.

## 13. Legal Consultation

- Consult with legal experts specialized in privacy laws to ensure the software complies with CCPA and any other applicable privacy regulations.

By addressing these concerns during software development, you can reduce privacy risks and enhance compliance with CCPA, ultimately building trust with users and avoiding potential legal and financial penalties.

## Generated responses by GAI3 Model for Engineer role

**E1:** Which technologies you can advise for EU-based software development company with 500 employees to build on?

### GAI3-E1:

For a European Union-based software development company with 500 employees, the choice of technology stack depends on various factors like the nature of the projects, target markets, and specific company goals. However, here are some general technologies and practices that can be beneficial:

1. **Cloud Computing Platforms:** Utilize platforms like AWS, Azure, or Google Cloud. These offer robust, scalable, and secure infrastructure. With the EU's strong data protection laws, ensuring compliance with GDPR is crucial, and these platforms offer tools to aid in that.
2. **DevOps Tools:** Implementing DevOps practices can enhance efficiency. Tools like Jenkins for continuous integration, Docker for containerization, and Kubernetes for container orchestration are beneficial. These tools aid in automating many aspects of development, testing, and deployment.
3. **Cybersecurity Solutions:** Given the importance of data security, especially in the EU, investing in advanced cybersecurity tools is crucial. This includes firewalls, intrusion detection systems, and regular security audits.
4. **Data Analytics and AI:** Technologies like TensorFlow, PyTorch for AI, and machine learning, and tools like Tableau or Power BI for data analytics can be vital, especially if your company deals with large amounts of data.

5. **Programming Languages and Frameworks:** Depending on your specific domain, languages like Python, Java, JavaScript (along with frameworks like React or Angular), and C# are widely used and supported.
6. **Agile and Scrum Methodologies:** With a large team, adopting Agile methodologies can improve productivity and collaboration. Tools like JIRA or Trello can aid in project management.
7. **Database Management:** SQL and NoSQL databases (like MySQL, PostgreSQL, MongoDB) are crucial for data storage and management. Ensuring GDPR compliance in data handling is also important.
8. **Blockchain Technology:** If applicable, explore blockchain for projects requiring high security and transparency, such as in fintech or supply chain management.
9. **Mobile Development Platforms:** If your company develops mobile apps, consider technologies like React Native, Flutter, or native development tools for iOS and Android.
10. **Remote Work Tools:** Since the pandemic, remote work has become more prevalent. Tools for collaboration, communication, and project management like Slack, Microsoft Teams, and Zoom are essential.
11. **Compliance and Regulatory Tech:** Since the company is based in the EU, technologies that help in complying with regional regulations like GDPR are important.
12. **Sustainable and Green Technologies:** With increasing focus on sustainability, investing in green technologies and practices can be a unique selling point.

Remember, the right choice heavily depends on your specific business needs, target customer base, and the kind of projects your company undertakes. Regular training and skill development for your employees in these technologies will also be crucial for staying competitive and innovative.

**E2:** How should secure infrastructure of EU-based software development company with 500 employees look like on diagram?

**GAI3-E2:**

Creating a diagram for a secure infrastructure of an EU-based software development company with 500 employees involves depicting various components and their interconnections. The diagram should ideally represent the following elements:

1. **Cloud Infrastructure** (if used): Show cloud service providers (e.g., AWS, Azure, Google Cloud) with elements like servers, databases, and storage. Ensure there are connections for data flow and management between these and the company's internal network.
2. **On-Premise Data Centers:** Illustrate on-premise servers or data centers, if any, showing secure connections to cloud services and internal networks.

3. **Network Infrastructure:** Include firewalls, routers, and switches. Show segregated networks for development, testing, and production.
4. **DevOps Tools:** Represent CI/CD pipelines with tools like Jenkins, GitLab, or GitHub. Indicate connections to development, testing, and deployment environments.
5. **Cybersecurity Tools:** Add components for intrusion detection systems (IDS), intrusion prevention systems (IPS), and security information and event management (SIEM) systems.
6. **Access Control Systems:** Depict identity and access management (IAM) systems like Microsoft Active Directory or Azure AD. Show how they manage access to different network segments and cloud services.
7. **Office Network:** Represent the office network with workstations, local servers, Wi-Fi routers, and connections to the main network.
8. **VPN and Remote Access:** Show VPN systems for secure remote access, illustrating how remote workers connect to the company network.
9. **Compliance and Data Protection Tools:** Include tools for GDPR compliance and data protection, such as encryption and data loss prevention (DLP) systems.
10. **Backup and Disaster Recovery:** Show backup storage solutions and connections for data replication to a disaster recovery site.
11. **Monitoring and Logging:** Illustrate centralized logging and network monitoring solutions.
12. **Physical Security:** Represent physical security controls for access to data centers or server rooms.
13. **End-Point Protection:** Include anti-virus, anti-malware solutions, and endpoint detection and response (EDR) tools on user devices.
14. **External Connections:** Represent secure connections to external entities, like clients or partners, ensuring that these are through encrypted channels.

In the diagram, it's important to:

- Clearly label each component.
- Use arrows to indicate the direction of data flow.
- Use different colors or shapes to distinguish between different types of components (like security, network, cloud, etc.).
- Ensure the diagram is layered or segmented to enhance readability – for example, separating network infrastructure, cloud infrastructure, and security layers.

Such a diagram will be complex due to the size of the company and the diversity of the infrastructure. It might be beneficial to create multiple interlinked diagrams, each focusing on different aspects, for clarity.

**E3:** Develop a detailed instruction on how to configure access controls in Microsoft Azure in accordance with ISO 27001.

### **GAI3-E3:**

Configuring access controls in Microsoft Azure in accordance with ISO 27001 involves a series of steps to ensure that access to data and resources is securely managed. ISO 27001 is a global standard for information security management systems (ISMS), and it emphasizes the importance of managing access rights to protect sensitive information. Here's a detailed instruction on how to set this up:

#### **1. Understand ISO 27001 Requirements**

Before configuring Azure, ensure you understand the relevant parts of ISO 27001, especially those related to access control (typically found in Annex A, particularly A.9 Access Control).

#### **2. Establish an Access Control Policy**

- **Develop a Formal Access Control Policy:** This should define how access rights are granted, reviewed, and revoked. It should align with the ISO 27001 standard.
- **Regular Audits and Reviews:** Plan for regular reviews and audits of access rights.

#### **3. Identify Information Assets and Classify Them**

- **Asset Inventory:** Make an inventory of all information assets that need protection.
- **Classification:** Classify assets according to their sensitivity and importance.

#### **4. User Registration and Deregistration**

- **Create User Accounts:** Set up user accounts in Azure AD (Azure Active Directory). Each account should be associated with an individual user.
- **Role-Based Access Control (RBAC):** Assign roles based on job responsibilities. Azure provides built-in roles, and you can also create custom roles.

#### **5. Implement Strong Authentication Mechanisms**

- **Multi-Factor Authentication (MFA):** Enforce MFA for accessing Azure resources. Azure MFA provides an additional layer of security.
- **Password Management:** Implement strong password policies and consider using Azure AD Password Protection.

#### **6. Managing Privileged Access**

- **Privileged Identity Management:** Use Azure AD Privileged Identity Management to manage, control, and monitor access within Azure AD, Azure, and other Microsoft Online Services.
- **Least Privilege Principle:** Grant users only the access rights they need to perform their jobs and no more.

#### **7. Control of Network Access**

- **Network Security Groups (NSGs):** Use NSGs to control traffic to and from Azure resources in an Azure virtual network.
- **Firewall Configuration:** Configure Azure Firewall to protect Azure Virtual Network resources.

## 8. Monitor and Review Access Controls

- **Azure Monitor and Azure Security Center:** Utilize these tools for continuous monitoring and reviewing of access controls.
- **Audit Logs:** Regularly review audit logs to monitor access patterns and investigate any irregularities.

## 9. Manage User Access to External Parties

- If external parties need access, ensure they are also subject to access control policies and procedures.

## 10. Handling Access Rights in Case of Employment Change

- **Automate Deprovisioning:** Automatically revoke access when an employee leaves or changes roles.

## 11. Documentation and Training

- **Documentation:** Keep detailed documentation of your access control policies, procedures, and configurations.
- **Training:** Train staff on the importance of access control and how to follow your policies.

## 12. Regular Audits and Compliance Checks

- Regularly audit your Azure environment and access controls to ensure compliance with ISO 27001.

Remember, compliance with ISO 27001 is not just about technical controls; it also requires appropriate policies, procedures, and training. It's also important to keep up to date with both Azure's evolving features and updates to the ISO 27001 standard.

**E4:** Could you please create a procedure for IT technician on how to manage cryptographic keys in accordance with ISO 27001 and how to configure encryption on Windows devices?

### **GAI3-E4:**

Certainly, managing cryptographic keys in accordance with ISO 27001 involves establishing secure practices for the entire lifecycle of the keys, including their generation, storage, use, and destruction. Additionally, configuring encryption on Windows devices is an integral part of protecting sensitive data. Below is a procedure for an IT technician covering both aspects:

### **Managing Cryptographic Keys in Accordance with ISO 27001**

1. Establish a Cryptographic Key Management Policy

- **Policy Creation:** Develop a policy based on ISO 27001 standards that cover key management procedures.
- **Roles and Responsibilities:** Define clear roles for key management tasks, ensuring separation of duties.

## 2. Key Generation and Exchange

- **Secure Generation:** Ensure keys are generated using secure and validated methods.
- **Exchange Protocols:** If keys need to be exchanged, use secure methods such as digital certificates or secure key exchange protocols.

## 3. Key Storage

- **Secure Storage:** Store cryptographic keys securely using hardware security modules (HSMs) or encrypted digital storage.
- **Access Control:** Limit access to stored keys strictly to authorized personnel.

## 4. Key Usage

- **Usage Restrictions:** Define and enforce policies on how and when keys can be used.
- **Audit Trails:** Maintain logs of key usage for auditing purposes.

## 5. Key Renewal and Replacement

- **Regular Renewal:** Set a schedule for key renewal and replace keys before they expire.
- **Compromise Response:** Have a procedure in place for immediate key replacement in case of compromise.

## 6. Key Destruction

- **Secure Destruction:** When keys are no longer needed, destroy them securely to ensure they cannot be recovered.

## 7. Documentation and Auditing

- **Documentation:** Keep detailed records of all cryptographic keys and related management activities.
- **Regular Audits:** Conduct regular audits to ensure compliance with the policy and ISO 27001 standards.

## Configuring Encryption on Windows Devices

### 1. Identify Sensitive Data

- **Data Identification:** Identify which data on the Windows devices need encryption.

### 2. Choose an Encryption Tool

- **BitLocker:** For Windows devices, BitLocker is a robust choice for full-disk encryption.
- **EFS (Encrypting File System):** Use EFS for encrypting individual files or folders.

### 3. Enable BitLocker for Full-Disk Encryption

- **Activation:** Go to "Control Panel" > "System and Security" > "BitLocker Drive Encryption".
- **Turn On BitLocker:** Follow the wizard to initialize BitLocker encryption. Choose to unlock the drive with a password or smart card.
- **Backup Recovery Key:** Save the recovery key to a secure location separate from the device.

### 4. Using EFS for File or Folder Encryption

- **Right-Click the File/Folder:** Choose "Properties" and navigate to the "Advanced" button.
- **Check 'Encrypt contents to secure data':** Apply changes to the folder or file.

### 5. Monitor and Manage Encryption

- **Regular Checks:** Regularly check that encryption is functioning as expected.
- **Key Recovery:** Ensure that BitLocker recovery keys and EFS certificates are backed up securely.

### 6. Training and Documentation

- **Staff Training:** Train staff on how to use encryption and the importance of safeguarding recovery keys.
- **Documentation:** Document all encryption procedures and key management practices.

### Regular Review and Updates

- **Policy Review:** Regularly review both cryptographic key management and encryption procedures to ensure they align with current ISO 27001 standards and organizational needs.

Remember, the success of cryptographic key management and device encryption largely depends on adherence to these procedures and regular training and awareness for all involved personnel.

**E5:** Could you please advise what security controls should be configured in order to prevent the risk of data leakage in Microsoft 365?

#### **GAI3-E5:**

To prevent the risk of data leakage in Microsoft 365, a range of security controls should be configured and regularly monitored. These controls are designed to protect sensitive data and ensure that only authorized personnel have access to it. Here's a list of key security controls to implement:

#### **1. Use Advanced Threat Protection (ATP)**

- **Enable ATP Safe Attachments:** This feature checks email attachments for malware.
- **ATP Safe Links:** Protects against malicious links in emails and Office documents.
- **Anti-phishing Policies:** Set up policies to detect attempts at impersonation and other phishing attacks.



## 2. Implement Data Loss Prevention (DLP) Policies

- **Create DLP Policies:** These policies help identify, monitor, and automatically protect sensitive information across Microsoft 365.
- **Define Sensitive Information Types:** Customize the types of sensitive information (like credit card numbers, social security numbers) that need protection.

## 3. Enable Azure Information Protection

- **Classify and Label Data:** Automatically classify and label emails and documents based on their sensitivity.
- **Rights Management:** Apply rights management to prevent unauthorized access or sharing.

## 4. Configure Multi-Factor Authentication (MFA)

- **Enforce MFA:** Require MFA for all users to add an extra layer of security, especially for accessing sensitive data.

## 5. Use Conditional Access Policies

- **Set Up Conditional Access:** These policies can restrict access based on user, location, device state, and the application.

## 6. Secure Email Communications

- **Encryption:** Use Office 365 Message Encryption to encrypt emails.
- **Transport Layer Security (TLS):** Ensure TLS is enabled for all email communications.

## 7. Regularly Review and Update Access Permissions

- **Audit User Roles and Access Rights:** Regularly review user roles and access rights, ensuring the principle of least privilege.
- **Manage External Sharing:** Control how data is shared outside your organization.

## 8. Monitor and Audit Activities

- **Use the Security & Compliance Center:** Regularly monitor for unusual activities and potential breaches.
- **Audit Logs:** Keep audit logs enabled and review them regularly.

## 9. Train Users on Security Best Practices

- **Awareness Training:** Conduct regular training sessions on data protection, phishing, and best practices for data handling.
- **Phishing Simulations:** Run simulated phishing campaigns to educate users.

## 10. Secure Mobile Device Access

- **Mobile Device Management (MDM):** Use Intune or other MDM solutions to manage and secure mobile devices accessing Microsoft 365.

- **Application Management:** Control which mobile apps can access Microsoft 365 data.

### 11. Secure SharePoint Online and OneDrive

- **Control Sharing Settings:** Restrict sharing of files and folders from SharePoint and OneDrive.
- **Use Secure Links:** Share files with secure links that expire and require authentication.

### 12. Backup Critical Data

- **Regular Backups:** Ensure regular backups of critical data are conducted and stored securely.

### 13. Ensure Compliance with Legal and Regulatory Standards

- **Regulatory Compliance:** Use Microsoft 365 compliance solutions to meet GDPR, HIPAA, and other regulatory requirements.

Implementing these security controls requires ongoing management and vigilance. Regularly updating these measures and training staff are critical components in minimizing the risk of data leakage in a Microsoft 365 environment.

**E6:** Could you please provide the detailed technical configuration that needs to be done to secure the GitHub environment in accordance with ISO 27001?

#### GAI3-E6:

Securing a GitHub environment in accordance with ISO 27001 involves a series of technical configurations and best practices aimed at ensuring data security and managing access controls. Here's a detailed guide to achieving this:

#### 1. Access Control

- **Two-Factor Authentication (2FA):** Enforce 2FA for all users. Go to **Settings > Security > Two-factor authentication**.
- **Use SSH Keys:** Require SSH keys for code access and operations. Generate SSH keys and add them to GitHub user accounts.
- **Role-Based Access Control (RBAC):** Assign users to teams and manage access based on roles.
- **Restrict Branch Access:** Protect branches by limiting who can push or merge into them (**Settings > Branches > Branch protection rules**).

#### 2. Repository Security

- **Private Repositories:** Ensure sensitive code is stored in private repositories.
- **Disable Unnecessary Features:** Turn off wikis, projects, or issues if not in use (**Settings > Options**).

#### 3. Code Security

- **Enable Code Scanning:** Use GitHub's CodeQL or integrate with a third-party SAST tool to scan for vulnerabilities.

- **Dependency Scanning:** Enable Dependabot to scan for vulnerable dependencies (**Settings > Security & analysis**).
- **Secret Scanning:** Enable secret scanning to detect committed secrets like passwords or tokens (**Settings > Security & analysis**).

#### 4. Audit Logs

- **Enable Audit Logs:** Keep a record of important events like repository access and changes (**Settings > Audit log**).

#### 5. Automated Security Policies

- **Security Policy File:** Add a **SECURITY.md** file to your repositories to outline security policies and procedures.
- **Automated Security Fixes:** Enable automated security fixes by Dependabot.

#### 6. Compliance and Documentation

- **Compliance as Code:** Use tools like InSpec, Chef, or Ansible to define and enforce security standards as code.
- **Document Security Practices:** Maintain clear documentation of your GitHub security practices and configurations.

#### 7. Continuous Integration/Continuous Deployment (CI/CD) Security

- **Review CI/CD Pipelines:** Ensure that CI/CD pipelines enforce code reviews and include security checks.
- **Use Environment Secrets Wisely:** Manage CI/CD secrets securely, using encrypted secrets or GitHub environments for sensitive data.

#### 8. Monitoring and Incident Response

- **Integrate Monitoring Tools:** Use tools like GitHub's Advanced Security, or third-party solutions for continuous monitoring.
- **Incident Response Plan:** Develop and document an incident response plan specific to your GitHub environment.

#### 9. Training and Awareness

- **Developer Training:** Regularly train developers on secure coding practices and GitHub security features.
- **Phishing Awareness:** Educate users about phishing attempts that target source code or access credentials.

#### 10. Regular Reviews and Updates

- **Periodic Access Reviews:** Regularly review and update access permissions.

- **Keep Policies Updated:** Regularly review and update your security policies and procedures to align with ISO 27001 standards and evolving security threats.

## 11. Data Backup and Encryption

- **Regular Backups:** Ensure regular backups of your repositories and metadata.
- **Data Encryption:** Use tools that encrypt data both at rest and in transit.

Implementing these measures requires careful planning and regular maintenance. It's important to continuously monitor and adapt these practices as the organization grows and as new threats emerge. Compliance with ISO 27001 is an ongoing process that involves both technical measures and organizational commitment.

**E7:** Could you prepare a training script for privileged Windows user covering related risks and recommendations?

### GAI3-E7:

Certainly! Below is a training script designed for privileged Windows users, covering related risks and recommendations. This script is tailored to educate users about the importance of responsible use of their elevated privileges and the best practices to mitigate associated risks.

#### **Title: Responsible Use of Privileged Access in Windows Environments**

**Duration:** Approximately 30-45 minutes

#### **Introduction**

**Duration: 5 minutes**

- Greet the participants and introduce yourself.
- Briefly explain the purpose of the training: "Today, we'll discuss the risks associated with privileged access in Windows environments and how to responsibly manage these privileges to protect our systems and data."

#### **Section 1: Understanding Privileged Access**

**Duration: 5 minutes**

- **Definition:** "Privileged access refers to the ability to make significant changes to system configurations, access sensitive data, and perform administrative tasks."
- **Examples in Windows:** "This includes accounts like local administrators, domain administrators, and users with elevated permissions."

#### **Section 2: Risks Associated with Privileged Access**

**Duration: 10 minutes**

1. **Unauthorized Access:** "If compromised, these accounts can give attackers full control over the system."

2. **Malware and Ransomware:** “Elevated privileges can allow malware to cause more damage, like installing ransomware.”
3. **Data Breach:** “Privileged accounts can access sensitive data, making them a prime target for data breaches.”
4. **Internal Threats:** “Misuse of privileges by employees, intentionally or accidentally, can lead to serious security incidents.”

### Section 3: Best Practices for Privileged Users

#### Duration: 10 minutes

1. **Use of Least Privilege Principle:** “Only use privileges that are necessary for your role. Avoid using an administrator account for routine tasks.”
2. **Secure Password Practices:** “Use strong, unique passwords and consider using a password manager. Change passwords regularly.”
3. **Multi-Factor Authentication (MFA):** “Always use MFA for an additional layer of security.”
4. **Regular Software Updates:** “Keep your system and software up to date to protect against vulnerabilities.”
5. **Avoiding Suspicious Links and Downloads:** “Be cautious about links and files to prevent malware infections.”
6. **Use of Auditing and Monitoring Tools:** “Regularly review system logs to detect unusual activities.”

### Section 4: Incident Response

#### Duration: 5 minutes

- **Immediate Action:** “If you suspect a security incident, report it immediately to the IT security team.”
- **Follow the Protocol:** “Be familiar with the incident response plan and your role in it.”

### Section 5: Interactive Q&A Session

#### Duration: 5-10 minutes

- Encourage participants to ask questions or share their experiences.
- Provide clear, concise answers and thank them for their participation.

### Conclusion

#### Duration: 2-3 minutes

- Summarize the key points: “Remember, with great power comes great responsibility. Your actions as a privileged user have a significant impact on our organization’s security.”
- Encourage ongoing vigilance: “Stay alert, stay informed, and always follow best practices.”

- Thank them for their participation and remind them where they can find more resources or whom to contact for further questions.

## End of Training

*Note: Make sure to customize the script based on your organization's specific policies, procedures, and any recent security incidents or concerns.*

**E8:** How to ensure that configuration of Microsoft 365 aligns with the requirements of CCPA?

### GAI3-E8:

Ensuring that the configuration of Microsoft 365 aligns with the requirements of the California Consumer Privacy Act (CCPA) involves several steps. CCPA aims to provide California residents with more control over their personal information. Here's a guideline to configure Microsoft 365 accordingly:

#### 1. Understand CCPA Requirements

- **Data Rights:** Familiarize yourself with the rights granted by CCPA, including the right to know about personal data collection, the right to request deletion, and the right to opt-out of the sale of personal information.
- **Scope of Data:** Determine what data you collect that falls under CCPA.

#### 2. Data Discovery and Classification

- **Identify Sensitive Data:** Use Microsoft 365's data classification tools to locate and classify personal data that falls under CCPA.
- **Apply Labels:** Apply sensitivity labels to categorize and protect personal data.

#### 3. Implement Data Governance Policies

- **Data Retention:** Set up data retention policies to automatically retain or delete data as required by CCPA.
- **Data Loss Prevention (DLP):** Configure DLP policies in Microsoft 365 to prevent unauthorized sharing of sensitive information.

#### 4. Enable and Configure Customer Lockbox

- **Request Approval:** Use Customer Lockbox to ensure that Microsoft accesses your content only with your explicit approval, enhancing data privacy.

#### 5. Access Controls

- **Least Privilege Access:** Ensure that only necessary personnel have access to personal data.
- **Multi-Factor Authentication (MFA):** Enable MFA to add an extra layer of security to your accounts.

#### 6. Audit and Reporting

- **Enable Audit Logging:** Make sure auditing is enabled to track and log activities across Microsoft 365 services.
- **Regular Reviews:** Conduct regular reviews of audit logs to monitor access to and usage of personal data.

## 7. Responding to Consumer Requests

- **Data Subject Requests (DSRs):** Implement procedures for efficiently responding to DSRs under CCPA, including requests for data access and deletion.
- **Automate Responses:** Use Microsoft 365's automation tools to streamline the response process for DSRs.

## 8. Review Third-Party Integrations

- **Data Sharing:** Ensure that any third-party services integrated with your Microsoft 365 environment comply with CCPA.

## 9. Training and Awareness

- **Employee Training:** Conduct regular training sessions for employees on CCPA requirements and how they relate to your Microsoft 365 environment.
- **Update Policies:** Regularly update your privacy policies and procedures to stay compliant with CCPA.

## 10. Incident Response Plan

- **Develop a Plan:** Have an incident response plan in place for potential data breaches.
- **Notification Procedures:** Include procedures for notifying affected individuals and authorities as required by CCPA.

## 11. Documentation and Compliance Records

- **Keep Records:** Maintain records of CCPA compliance efforts, including data mapping, risk assessments, and DSR responses.

## 12. Regular Reviews and Audits

- **Compliance Audits:** Regularly audit your Microsoft 365 configuration for CCPA compliance and adjust as necessary.

Implementing these steps will help align your Microsoft 365 configuration with CCPA requirements, ensuring better control and protection of consumer data. It's essential to keep abreast of any updates to CCPA and adjust your policies and configurations as needed.