Частина 1. Причини проходження сертифікації відповідно до вимог міжнародного стандарту інформаційної безпеки ISO/IEC 27001

На основі огляду розділу «Сервіс для обміну даними компанії TechScooter», три найбільш значущі переваги впровадження ISMS на основі ISO/IEC 27001 для генерального директора Андрія Левченка:

Підвищення рівня захисту даних та зменшення ризиків інцидентів безпеки. TechScooter стикається з вразливостями в мобільних застосунках (наприклад, zero-day вразливості для iOS та Android, які експлуатуються на дарквебі), крадіжками самокатів та несанкціонованим доступом до персональних та фінансових даних користувачів. Впровадження ISMS дозволить систематично ідентифікувати та керувати ризиками, впроваджуючи контроль доступу та моніторинг, що безпосередньо підтримує стратегічну ціль компанії щодо надійного райдшерингу без втрат даних.

Зростання довіри клієнтів та партнерів, що сприяє розширенню бізнесу. Компанія співпрацює з AWS та FinPay, які сертифіковані за ISO 27001, але власні вразливості (відсутність MFA, слабкі паролі) підривають довіру. Сертифікація продемонструє зобов'язання щодо захисту даних, полегшить укладання контрактів з великими клієнтами та венчурними інвесторами, як Y Combinator, та підвищить репутацію, що є ключовим для стратегічної мети масштабування послуг у містах України.

Економія витрат на реагування на інциденти та відповідність регуляціям. Аудит виявив критичні недоліки, такі як доступ розробників до незашифрованих даних без належного контролю, що призводить до витрат на відновлення після breach. ISMS оптимізує процеси, зменшує ймовірність штрафів за порушення (наприклад, відповідно до українського законодавства щодо захисту персональних даних), та забезпечує стійкість бізнесу, підтримуючи стратегічну ціль ефективного використання хмарних ресурсів AWS для зростання.

Частина 2. Встановлення контексту ISMS

Причини впровадження ISMS: Впровадження ISMS на основі ISO/IEC 27001 є необхідним для TechScooter через часті інциденти безпеки (вразливості в застосунках, крадіжки самокатів, несанкціонований доступ до даних), що загрожують репутації, фінансам та операціям. Це дозволить систематизувати управління ризиками, забезпечити конфіденційність, цілісність та доступність інформації, та підготуватися до зростання компанії.

Вимоги локального законодавства: В Україні основним є Закон України «Про захист персональних даних» № 2297-VI від 01.06.2010, який регулює обробку персональних даних, вимагає згоди суб'єктів, реєстрацію баз даних та заходи захисту від несанкціонованого доступу. Компанія обробляє дані користувачів (персональні, фінансові), тому повинна відповідати цим вимогам, а також новому законопроєкту про гармонізацію з GDPR, що посилює штрафи за порушення до 4% річного обороту.

Міжнародні стандарти безпеки: ISO/IEC 27001 встановлює рамки для ISMS, ISO/IEC 27017 – для хмарних сервісів (як AWS), ISO/IEC 27018 – для захисту персональних даних у хмарі. Ці стандарти доповнюють GDPR, забезпечуючи глобальну сумісність.

Основні активи компанії:

Дані користувачів (персональні, фінансові, геолокація) – критичні для конфіденційності, пов'язані з Annex A.8 (Asset management).

Блокчейн-дані про самокати (місцезнаходження, стан) – забезпечують цілісність та стійкість.

Мобільний застосунок та API – ключові для доступності, пов'язані з розробкою та мережею.

Ці активи впливають на всі області ISMS, від планування до моніторингу.

Основні процеси діяльності, що впливають на ІБ: Розробка та тестування застосунку (доступ до реальних даних без шифрування), обробка платежів через FinPay, відстеження самокатів через блокчейн, хмарне зберігання в AWS. Ці процеси ризикують бути вкрадені через слабкий контроль доступу.

Частина 3. Визначення області дії ISMS

Область дії ISMS для TechScooter: Включає розробку, тестування та розгортання мобільного застосунку, управління блокчейн-даними про самокати, обробку платежів та хмарну інфраструктуру AWS. Межі: Офісна мережа (LAN з серверами баз даних та розробки), хмарні сервіси (бекенд, блокчейн), мобільні пристрої співробітників та користувачів. Виключає фізичне виробництво самокатів.

Обґрунтування: Обмеження на ключові цифрові активи фокусується на високоризикових процесах (розробка з реальними даними), забезпечуючи початкову сертифікацію без надмірного розширення. Додаткова цінність для клієнтів – посилена приватність даних (геолокація, платежі), що підвищить довіру та лояльність, дозволяючи маркетинг як "сертифікований безпечний сервіс райдшерингу".

Частина 4. Gap-аналіз

Рівень зрілості процесу доступу до даних клієнтів у блокчейні: Низький (рівень 1 за моделлю CMMI). Політики відсутні або не виконуються (розробники мають повний доступ без MFA, ролей; дані незашифровані для тестування). Аудит показує неефективність: часті зміни в БД без схвалення, що порушує цілі ISMS (Annex A.9 Access control).

Рекомендації для покращення:

Впровадити RBAC (Role-Based Access Control) для обмеження доступу (лише CISO схвалює тести з реальними даними).

Обов'язкове MFA та сильні паролі для всіх доступів до хмари.

Шифрування даних у спокої та транзиті (AES-256), з логуванням доступів для аудиту.

Регулярні рев'ю доступів щоквартально.

Частина 5. Розробка політик інформаційної безпеки

Політика використання мобільних пристроїв

Розділ	*Опис*
Вступ	*Ця політика регулює використання мобільних пристроїв (смартфони, планшети) для доступу до корпоративних ресурсів TechScooter, забезпечуючи захист даних відповідно до ISO 27001 Annex A 8.1 (User endpoint devices).*
Область дії	*Застосовується до всіх співробітників, підрядників та пристроїв, підключених до корпоративної мережі/LAN/хмари.*
Мета	*Запобігти втраті даних, несанкціонованому доступу та ризикам від мобільності (крадіжка, втрата).*
Обов'язки	*- Керівництво: Затвердження політики. - CISO: Моніторинг compliance. - Співробітники: Дотримання правил, звіт про інциденти.*
Класифікація даних	*- Конфіденційні (PII, фінансові) – лише на захищених пристроях. - Публічні – без обмежень.*
Недопустимі дії	*1. Встановлення несанкціонованого ПЗ. 2. Підключення до незахищених Wi-Fi. 3. Зберігання незашифрованих даних. 4. Використання для особистих цілей без MDM.*
Пов'язана політика	*Політика доступу, політика інцидентів.*
Санкції	*Порушення – дисциплінарні заходи, аж до звільнення.*
Огляд	*Щорічно або після інцидентів.*

Частина 6. Ідентифікація загроз, вразливостей та їх впливу

Сценарій	*Загроза*	*Вразливість*	*Вплив*	*КЦД*
Облікові дані колишнього співробітника використовуються	*Несанкціонований доступ (інсайдерська загроза)*	*Відсутність деактивації акаунтів після звільнення*	*Витік PII/фінансових даних, репутаційні втрати*	*К (конфіденційність)*
Неправильне значення в CLI сервера розробки	*Людська помилка*	*Недостатній валідація вводу*	*Відключення сервера, зупинка розробки*	*Д (доступність)*
Втрата бета-версії через несправний HDD	*Фізична несправність*	*Відсутність резервного копіювання*	*Втрата коду, затримка релізу*	*Ц (цілісність)*
Слабкі паролі співробітників	*Брутфорс-атака*	*Відсутність політики паролів/MFA*	*Несанкціонований доступ до систем*	*К, Д*
Недостатній контроль доступу до хмарного блокчейн-сервера	*Зовнішня атака*	*Слабка конфігурація IAM*	*Витік даних про самокати/користувачів*	*К, Ц*

Частина 7. Варіанти обробки ризиків

Для ризику 0,5% шахрайських транзакцій (5 млн USD втрат з 10 млн):

Прийняття (Accept): Ігнорувати, якщо витрати на заходи перевищують втрати – не рекомендовано, бо накопичує репутаційні ризики.

Зниження (Mitigate): Впровадити AI-фрод-детекцію в FinPay, ліміт транзакцій, моніторинг – рекомендовано, зменшить до <0,1%.

Передача (Transfer): Страхування від фроду або аутсорсинг платежів.

Уникнення (Avoid): Припинити кредитні картки – нереалістично для бізнесу.

Рекомендація: Зниження, з фокусом на моніторинг.

Частина 8. Процес керування моніторингом та аналізом ризиків

Моніторинг та аналіз ризиків важливий для TechScooter, бо дозволяє динамічно реагувати на нові загрози (як zero-day), забезпечувати compliance з ISO 27001 та оптимізувати ресурси в хмарі. Без цього ризики накопичуються, призводячи до business disruption.

Три ризики:

Нерозпізнаний breach (наприклад, через слабкі паролі) – фінансові втрати та штрафи.

Затримки в розробці від непередбачених вразливостей – втрата конкурентоспроможності.

Репутаційні збитки від витоку даних – відтік клієнтів та інвесторів.

Частина 9. Основний список документованої інформації

Для безперервності бізнесу (Annex A.17):

План безперервності бізнесу (BCP).

Процедура відновлення після катастроф (DRP).

Аналіз впливу бізнесу (BIA).

Резервні стратегії (backups, failover).

Тести та аудити BCP.

Реєстр активів та постачальників.

Частина 10. Контроль доступу

Опис заходу	***Відсутність дії чи контролю***	***Наслідки***
Керування привілеями користувачів (A.9.2.3)	*Не проводилося рев'ю доступів віддалених розробників до PII в хмарі.*	*Несанкціонований доступ, витік даних, штрафи за PDP.*
Многофакторна аутентифікація (A.9.4.2)	*Відсутня MFA для віддаленого доступу до бази даних.*	*Легкий компрометація акаунтів, breach PII.*
Логування та моніторинг	*Не фіксувалися доступи*	*Неможливість аудиту*

Опис заходу	*Відсутність дії чи контролю*	*Наслідки*
(A.9.4.1)	*віддалених користувачів.*	*інцидентів, затримки реагування.*

Частина 11. Заходи безпеки

1. Реагування на інциденти інформаційної безпеки

Впровадження SIEM-системи. Опис: Моніторинг логів для виявлення аномалій. Результат: Швидке виявлення breach'ів, зменшення часу реагування на 50%. Дії: (а) Інтеграція з AWS CloudWatch; (б) Навчання команди.

Розробка playbook'ів інцидентів. Опис: Стандартизовані процедури для типових загроз. Результат: Зменшення впливу на доступність. Дії: (а) Класифікація інцидентів; (б) Щомісячні симуляції.

2. Безпечне середовище розробки

Впровадження SDLC з security gates. Опис: Перевірка коду на вразливості на етапах. Результат: Зменшення zero-day у релізах. Дії: (а) Інтеграція SAST/DAST; (б) Рев'ю коду peer-review.

Сегрегація середовищ (dev/staging/prod). Опис: Окремі дані для тестів (фейкові). Результат: Захист реальних PII. Дії: (а) Конфігурація VLAN; (б) Автоматизоване деплої.

3. Заходи безпеки мережі

Впровадження next-gen firewall. Опис: Фільтрація трафіку в LAN/хмарі. Результат: Блокування DDoS, як на рисунку. Дії: (а) Розгортання в AWS; (б) Налаштування правил.

Шифрування трафіку (TLS 1.3). Опис: Для API між серверами. Результат: Захист від MITM. Дії: (а) Оновлення certs; (б) Моніторинг compliance.

4. Припустиме використання ресурсів компанії (використання активів)

Політика AUP (Acceptable Use Policy). Опис: Правила для пристроїв/мережі. Результат: Зменшення інсайдерських загроз. Дії: (а) Підписання всіма; (б) Навчання.

Моніторинг використання (DLP). Опис: Виявлення витоків даних. Результат: Контроль за активами. Дії: (а) Встановлення інструментів; (б) Щорічні аудити.

Частина 12. Програма підвищення обізнаності та навчання

Важливість: Програми зменшують людський фактор (80% breach'ів від помилок), підвищують compliance з ISO 27001 Annex A.7, та дозволяють швидко реагувати на загрози, як слабкі паролі в TechScooter.

Заходи для успіху:

Щорічне обов'язкове навчання: *Онлайн-курси з фішингу, паролів (з тестами, 90% проходження).*

Симуляції фішингу: *Щоквартально, з фідбеком.*

Рольові тренінги: *Для розробників – secure coding; для CISO – ризик-менеджмент.*

Оцінка ефективності: *Опитування, метрики (зменшення інцидентів на 30%).*

Інтеграція з HR: *В onboarding та performance reviews.*