*Неофіційний переклад НААУ*

**IAF MD 29:2024**

**Обов'язковий документ IAF**
**Вимоги щодо переходу на стандарт ISO/IEC 27006-1:2024**
**Видання 1**

---

Видання 1
Підготовлено: Технічний Комітет IAF
Затверджено: Члени IAF Дата: 25 квітня 2024
Дата видання: 21 травня 2024 Дата застосування: 21 травня 2024

Контактна особа: Віктор Ганді
Секретар IAF
Телефон: +1 (571) 569-1242
Email: secretary@iaf.nu

**Вступ до обов’язкових документів IAF**

Термін «слід» використовується у цьому документі, щоб вказати визнані засоби відповідності вимогам стандарту. Орган з акредитації (ОА) може виконувати їх еквівалентним шляхом. Термін «повинен» використовується в цьому документі, щоб вказати ті положення, які є обов’язковими та відображають вимоги відповідного стандарту.

## ОБОВ'ЯЗКОВИЙ ДОКУМЕНТ IAF

**Вимоги щодо переходу на стандарт ISO/IEC 27006-1:2024**

### 1 ВСТУП

Усі документи, які надають інформацію щодо перехідних періодів нормативних документів, будуть обов’язковими документами, якими повинні керуватися органи з акредитації (ОА), які є підписантами IAF MLA, і акредитовані органи з оцінки відповідності (ООВ), у межах, як зазначено в цьому документі. Цей документ розроблено призначеною робочою групою Технічного комітету IAF відповідно до вимог IAF PR 7:2022 «Вимоги до створення обов’язкових документів IAF щодо переходів». Документ є обов’язковим для усіх ОА-підписантів IAF MLA та акредитованих ООВ за схемою систем управління інформаційною безпекою (СУІБ).

Цей документ містить вимоги до переходу щодо:

| | |
|---|---|
| Нормативний документ: | ISO/IEC 27006-1:2024 |
| На заміну: | ISO/IEC 27006:2015, а також ISO/IEC 27006:2015/Amd 1:2020<br>Примітка: Коли в цьому документі містяться посилання на стандарт ISO/IEC 27006:2015, він охоплює ISO/IEC 27006:2015 та ISO/IEC 27006:2015/Amd 1:2020 |
| Поточний статус (на час публікації обов’язкового | IS |

| | |
|---|---|
| документа): | |
| Перехідний період: | 2 роки (24 місяці), починаючи з останнього дня місяця публікації. |

Цей обов'язковий документ був розроблений відповідно до вимог IAF PR 7, тому згідно з розділом 1.2.2 документа PR 7 цей документ не застосовується, якщо схема визначає конкретний процес переходу.

## 2. КОРОТКИЙ ЗМІСТ ЗМІН

Основні відмінності між ISO/IEC 27006:2015 та ISO/IEC 27006-1:2024 включають, але не обмежуються, наступним:

i) Уточнення вимог до дистанційних аудитів.

a) Нові вимоги до проведення дистанційного аудиту в пункті 9.1.3.3.

b) Обсяг та ефективність застосування дистанційного аудиту повинні зазначатися у звіті про проведення аудиту у п. 9.4.3.2.

c) Скасування вимог щодо отримання схвалення від ОА, якщо заходи з дистанційного аудиту становлять більше 30% запланованого часу аудиту на місці.

d) Для клієнта, який має або невелику кількість фізичних відповідних ділянок, або такі ділянки відсутні, у звіті про проведення аудиту (див. п. 9.4.3.2) і у документі про сертифікацію (див. п. 8.2.2) повинно бути зазначено, що діяльність клієнта здійснюється дистанційно.

ii) Оновлення вимоги щодо розрахунку часу аудиту (див. Додаток C).

a) Введення поняття осіб, які здійснюють певну тотожну діяльність у п. C.2.1 та визначення вимог щодо того, як визначити початкову кількість осіб у п. C.3.4 відповідно.

b) Нові вимоги до часу аудиту для розширення сфери в п. C.7.

c) Подальше уточнення підходів до розрахунку часу аудиту на декількох ділянках у п. C.6.

iii) Оновлення Додатку D до стандарту ISO/IEC 27006:2015 для узгодження із засобами контролю інформаційної безпеки, перерахованими у Додатку A до стандарту ISO/IEC 27001:2022, і його перенесення як Додатку E до стандарту ISO/IEC 27006-1:2024. Таблиця D була перейменована в таблицю E.

iv) Уточнення вимог щодо посилання на інші стандарти в документах на сертифікацію СУІБ (див. 8.2.3).

v) Усунення дублювань у ISO/IEC 17021-1:2015. Наприклад, пункти 5.2, 7.1.3, 9.3.2.2 і 9.4 (ISO/IEC 27006-1:2024) були оновлені.

vi) Вилучення кількісної вимоги до досвіду роботи та навчання аудиторів СУІБ, наприклад, щодо наявності 4-річного досвіду практичної роботи на повний робочий день.

## 3. ОСНОВНІ ЧАСОВІ РАМКИ

Стандарт ISO/IEC 27006-1:2024 був опубліковано в березні 2024 року. Згідно з рішенням IAF, наведені нижче дати розраховані, починаючи з 31 березня 2024 року

| Діяльність | Термін виконання |
|---|---|
| **OA** | |
| OA мають бути готовими проводити оцінки на відповідність вимогам ISO/IEC 27006-1:2024 не пізніше, ніж | 9 місяців, починаючи із завершення місяця публікації – 31 грудня 2024 |
| OA повинні використовувати стандарт ISO/IEC 27006-1:2024 для усіх первинних оцінок (або розширення існуючих сфер) не пізніше, ніж | 12 місяців, починаючи із завершення місяця публікації – 31 березня 2025 |
| OA мають завершити перехід OOB не пізніше, ніж | 24 місяці, починаючи із завершення місяця публікації - 31 березня 2026 |
| **OOB** | |
| OOB повинні використовувати стандарт ISO/IEC 27006-1:2024 для проведення усіх первинних аудитів та аудитів повторної сертифікації після отримання акредитації на ISO/IEC 27006-1:2024 | Дата має бути визначена для кожного OOB на основі дати переходу його акредитації |
| OOB мають використовувати стандарт ISO/IEC 27006-1:2024 для усіх клієнтів не пізніше, ніж | 24 місяці, починаючи із завершення місяця публікації - 31 березня 2026 |

## 4. ДІЇ В РАМКАХ ПРОЦЕСУ ПЕРЕХОДУ

### 4.1 Дії OA

| Діяльність | Так/Ні | Примітки |
|---|---|---|
| Заходи з боку OA | Так | - Спланувати та підготуватися до проведення оцінок за новою версією якомога швидше та не пізніше встановленого граничного терміну.<br>- Визначити відмінності між новою та старою версіями.<br>- Забезпечити своєчасне інформування OOB про необхідні заходи з переходу, включаючи будь-які проміжні кінцеві терміни протягом перехідного періоду.<br>- Переконатися в тому, що відповідний персонал, якого торкнуться зміни, є компетентним для переглянутої версії та процесу переходу.<br>- OA заохочуються спланувати та розпочинати необхідні дії якомога швидше. |

| | | |
|---|---|---|
| Аналіз документів ООВ | Ні | |
| Аналіз технічної документації ООВ | Так | Аналіз прогалин, проведеного ООВ, план переходу/впровадження, відповідна документація для змін, включаючи необхідні докази впровадження та інша відповідна інформація, яку ОА вважає необхідною. |
| Чи може знадобитися додатковий час для переходу? | Так | Мінімум 1 день оцінки для підтвердження переходу ООВ |
| Технічна оцінка у головному офісі ООВ (на місці або дистанційно) | Якщо застосовно | Якщо ОА може проаналізувати необхідні зміни та впровадження з боку ООВ в результаті аналізу технічної документації ООВ, тоді оцінка головного офісу ООВ не потрібна. *Якщо ОА не може цього зробити, тоді необхідно провести оцінку в офісі.* |
| Спостереження за аудитом ООВ | Ні | |
| Рішення ОА щодо переходу | Так | ОА має прийняти рішення щодо переходу на стандарт ISO/IEC 27006-1:2024, коли всі виявлені питання будуть належним чином вирішені, а компетентність буде продемонстрована. |

### 4.2 Дії ООВ

| Діяльність | Так/Ні | Примітки |
|---|---|---|
| Заходи з боку ООВ | Так | - Спланувати та підготуватися до подання інформації про заходи щодо переходу до ОА (відповідно до визначених ОА вимог щодо переходу) і бути готовим застосувати нові вимоги відповідно до встановлених термінів.<br>- Завершити аналіз прогалин.<br>- Розробити план переходу для вирішення наступного:<br>i) Визначити відмінності між новою та старою версіями. Типові процеси, які розглядаються для визначення відмінностей, можуть включати продажі/ціни, процес аудиту, документи з сертифікації, управління компетентністю та комунікація з існуючими сертифікованими клієнтами.<br>ii) Проаналізувати вплив змін на відповідну діяльність/процеси та визначити необхідні дії для забезпечення відповідності (наприклад, система/документи системи управління та, якщо застосовно, IT-інструменти).<br>- Моніторити докази необхідних змін і перевіряти постійне впровадження цих змін.<br>- Переконатися у тому, що відповідний персонал, якого торкнуться зміни, є компетентним для переглянутої версії та процесу переходу. Персонал може включати, але не обмежуватися, аудитора, рецензентів аудиторського звіту, особу, яка приймає рішення щодо сертифікації, рецензента заявок, планувальника.<br>- ООВ заохочуються спланувати та якомога скоріше розпочинати необхідні дії. |

### 4.3 Інше

Оскільки вимоги до визначення часу аудиту змінилися у стандарті ISO/IEC 27006-1 версії 2024 року, є вірогідність того, що угода між ООВ та їх сертифікованими клієнтами потребуватиме перегляду.

Завершення обов'язкового документу IAF «Вимоги щодо переходу на стандарт ISO/IEC 27006:2024»

**Подальша Інформація**

Для отримання додаткової інформації щодо цього документа або інших документів IAF, зверніться до будь-якого члена IAF або Секретаріату IAF.

Інформацію щодо контактів членів IAF, ви можете отримати на офіційному сайті IAF: http://www.iaf.nu .

**Секретаріат:**
Корпоративний секретар IAF
Телефон: +1 (613) 454-8159
E-mail: secretary@iaf.nu