# Архітектура Комплаєнсу: Дорожня карта впровадження Постанови НБУ № 143

Автоматизація інформаційної безпеки та кіберзахисту для небанківських фінансових установ

SecBoard Framework

# Масштаб регулювання та часові рамки

## Суб’єкти регулювання

- Страхові спілки
- Ломбарди
- Фінансові компанії

## Об’єкти захисту

- Таємниця страхування
- Таємниця фінансової послуги
- ІКС (основні бізнес-процеси та взаємодія з НБУ)

**12 місяців** на повну відповідність (Грудень 2026)

# Організаційна архітектура та управління

## Стратегічний контроль: Керівник

- Затвердження внутрішніх документів (політик, інструкцій).
- Затвердження бюджету та механізмів контролю кіберризиків.
- Офіційне призначення та контроль діяльності Відповідальної особи.

## Операційна реалізація: Відповідальна особа

- Організація щорічної інвентаризації ІКС (апаратного та програмного забезпечення).
- Управління правами доступу та контроль засобів захисту.
- Моніторинг та розслідування інцидентів інформаційної безпеки.
- Блокування несанкціонованого ПЗ.

# Архітектура ідентифікації та контролю доступу


Реалізація принципу мінімальних привілеїв (Least Privilege) із щорічним переглядом прав доступу.

# Мережевий захист та безперервне логування

## Периметральний захист мережі


Розміщення серверів та сервісів, відкритих для клієнтів.

Сегментація міжмережевими екранами. Обов'язковий антивірусний захист.

## Система безперервного логування та архівування

**Що фіксується** (п. 26):

- Доступ до конфігурацій, результати автентифікації, управління правами, зміни паролів.


**Вимога до зберігання** (п. 28):

Архівування ≥ 1 раз на рік.

Зберігання захищених логів протягом мінімум 1 року.

# Управління застарілим програмним забезпеченням

Заборона використання ПЗ без підтримки та оновлень безпеки (End-of-Life).

| Рік 1: Аналіз та Компенсація | Рік 2: Міграція (Максимум 2 роки) |
| --- | --- |
| • Проведення аналізу ризиків (п. 34).<br>• Впровадження компенсуючих заходів (ізоляція, додатковий моніторинг, бекапи). | • Повний перехід на офіційні версії ПЗ із підтримкою від розробника. |

План переходу повинен бути офіційно затверджений Наглядовою радою або іншим вищим органом управління як частина стратегії безперервності.

# Протокол реагування на кіберінциденти


## Взаємодія з НБУ

- Зобов'язання реагувати на письмові електронні запити Національного банку.
- Надання доказів, пояснень та логів у точно визначеному НБУ форматі та у вказані строки.

## Залучення підрядників (TPRM)

- **Обов'язково:** Укладання NDA з інтеграторами та SOC-провайдерами.
- **Сувора заборона (п. 9):** Жодних резидентів держави-агресора, відсутність у санкційних списках, заборона зберігання даних на тимчасово окупованих територіях.

# Матриця складності:
# Ручний підхід проти Автоматизації

| Ручний Комплаєнс (Застарілий підхід - Високий ризик) | Екосистема SecBoard (Аудиторська готовність) |
| --- | --- |
| **Документи**<br>Розрізнені файли Excel, відсутність контролю версій політик. | **Документи**<br>Централізований реєстр з автоматичним трекінгом річного перегляду. |
| **Активи**<br>Забуте legacy-ПЗ, ручна інвентаризація раз на рік. | **Активи**<br>Динамічний реєстр (Asset Management) з прив'язкою до ризиків. |
| **Докази**<br>Хаотичний пошук логів під час запиту НБУ. | **Докази**<br>Інтегрований SOC (Wazuh) з гарантованим архівом логів на 1 рік. |
| **Паролі**<br>Сліпа довіра користувачам, відсутність автоматичного відстеження 90-денного циклу. | **Паролі**<br>Синхронізація з IdP, автоматизоване навчання та контроль доступу. |

SecBoard

# SecBoard Local Compliance (NBU Resolution No. 143)

**Текст Постанови № 143**

**ДСТУ ISO/IEC 27001:2023**

**Внутрішні політики**

**Спеціалізований фреймворк для небанківського сектору**

## Мапінг вимог

Кожен абзац Постанови автоматично прив'язаний до конкретних технічних контролів.

## Індикація статусу

Вбудована система світлофорів для миттєвого відображення рівня відповідності.

## Централізація

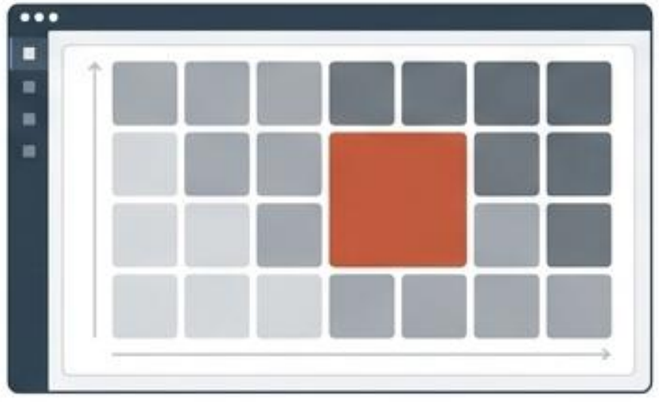
Єдина точка збору доказової бази для перевірок НБУ.

# Пряме відображення вимог у модулях SecBoard (Частина 1)

## Risk Assessment

Вимога НБУ: п. 6-8, 34

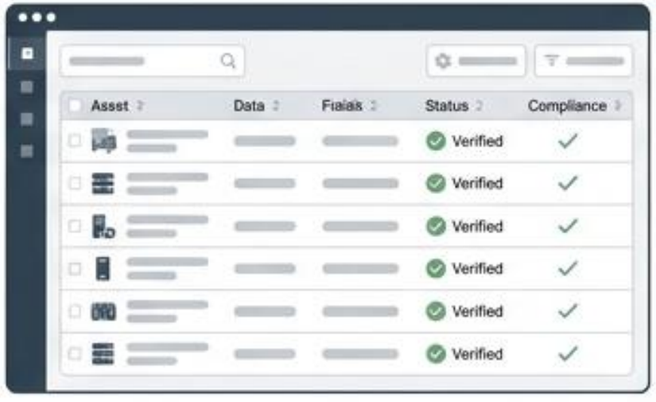
Документування ризиків, визначення компенсуючих заходів, пряма прив'язка ризиків до контролів фреймворку. Аналіз ризиків застарілого ПЗ.



## Asset Management

Вимога НБУ: п. 13

Динамічний інвентар компонентів ІКС, фіксація версій операційних систем та відстеження статусу підтримки. Щорічна актуалізація.




## Cabinet & Access

Вимога НБУ: п. 16-25

Управління групами та ролями (Least Privilege), контроль життєвого циклу сертифікатів, парольна політика, MFA.

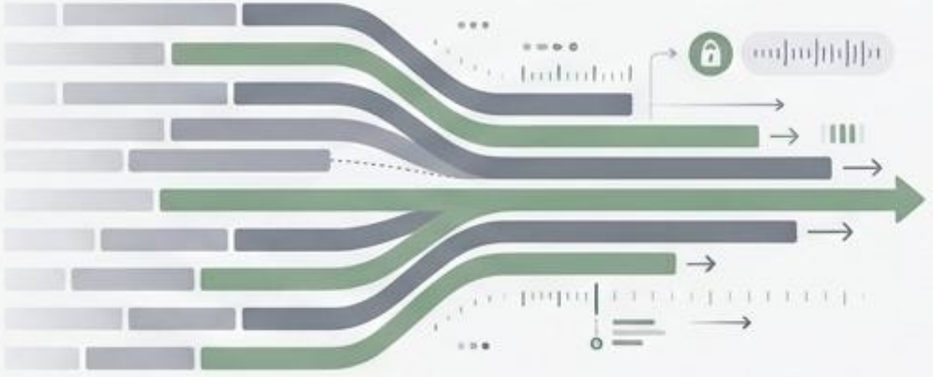

SecBoard

# Пряме відображення вимог у модулях SecBoard (Частина 2)

## SOC / Wazuh Integration

**Вимога НБУ:** п. 26-28 (Централізоване логування подій, цілісність файлів, зберігання ≥ 1 року).

**Рішення SecBoard:** Автоматичний збір подій автентифікації та змін конфігурацій. Захищений архів логів, недоступний для модифікації, з миттєвим формуванням звітів.



## TPRM (Управління ризиками третіх сторін)

**Вимога НБУ:** п. 9, 42-43 (Управління підрядниками, відсутність санкцій).

**Рішення SecBoard:** Реєстр вендорів. Автоматизований контроль підписаних NDA, перевірка зв'язків з державою-агресором, зберігання контрактів на реагування.


SecBoard

# Цифрова архівація та реєстр інцидентів

## Document Register & Legislative Docs

**Вимога НБУ**: п. 11-15 (Затвердження політик керівником, щорічний перегляд документів).

**Рішення SecBoard**: Зберігання офіційних текстів Постанови, версіювання внутрішніх політик, автоматичні нагадування про необхідність щорічного перегляду.


## Incident Register

**Вимога НБУ**: Розділ III, п. 39-46 (Процес управління інцидентами, оцінка збитків).

**Рішення SecBoard**: Журнал реєстрації кіберінцидентів. Фіксація дій у відповідь, оцінка впливу на бізнес-процеси, накопичення історичних даних.

# Генерація доказової бази для аудиту

## 1

### Запит НБУ (Тригер)

Отримання офіційної письмової вимоги від Національного банку щодо надання інформації про кіберінцидент або логів доступу.

## 2

### Централізований пошук (Дія)

Вхід у модуль Framework Compliance. Перехід до конкретного параграфа Постанови (напр., п. 26).

## 3

### Автоматична генерація (Доказова база)

Експорт готового, незмінного пакета доказів: політики з актуальними підписами, звіти Wazuh, підтвердження навчання користувачів.

**Точно за форматом НБУ. Вчасно. Без стресу.**

# SecBoard: Enterprise-Ready. Built to Scale

- A comprehensive approach.
- Uncompromising reliability.
- Pragmatic growth.

info@secboard.online
secboard.online