Active Audit Agency

Perfection has no limits...

Сучасні підходи до оцінки ризиків інформаційних технологій

(на підтримку впровадження галузевих стандартів інформаційної безпеки
ГСТУ СУІБ 1.0/ISO/IES 27001:2010 та ГСТУ СУІБ 2.0/ISO/IES 27002:2010)

Володимир Ткаченко
Директор ТОВ "Агентство активного аудиту"

Управління ризиками IT

Active Audit Agency
Perfection has no limits...

Чому?

- Забезпечує підґрунтя для всієї діяльності в сфері інформаційної безпеки
- Підтримує адекватне та завчасне реагування на вимоги регуляторів ринку

Що?

- Визначити та своєчасно реагувати на загрози, уразливості та втрати
- Розуміти можливі збитки та потенційні наслідки порушення властивостей інформації (активів)
- Забезпечує фундамент для розробки стратегії зниження ризиків
- Допомагає визначити пріоритети при впровадженні заходів захисту

Як?

- Визначення існуючих ризиків
- Розуміння та документування можливих ризиків та наслідків реалізації
- Підготовка фахівців з інформаційних ризиків

Підходи до управління IT ризиками

Active Audit Agency
Perfection has no limits...

ОСНОВНІ ПІДХОДИ до управління ризиками інформаційних технологій ґрунтуються на:

- Стандарті управління та аудиту інформаційних технологій Cobit v.4.1;
- Настановах по управлінню ризиками в інформаційних технологіях NIST 800-30;
- Настановах по управлінню ризиками ISO 3100 (готуються до прийняття);
- Стандарті управління інформаційною безпекою ISO 27005;
- Стандарті управління ризиками AS/NZS 4360:2005

Методології оцінки IT ризиків

Active Audit Agency
Perfection has no limits...

Методологія оцінки ризиків Національного Інституту Стандартів та Технологій США
(National Institute of Standards and Technology – **NIST**)

Методологія аналізу факторів ризиків інформаційних технологій
(Factor Analysis of Information Risk - **FAIR**)

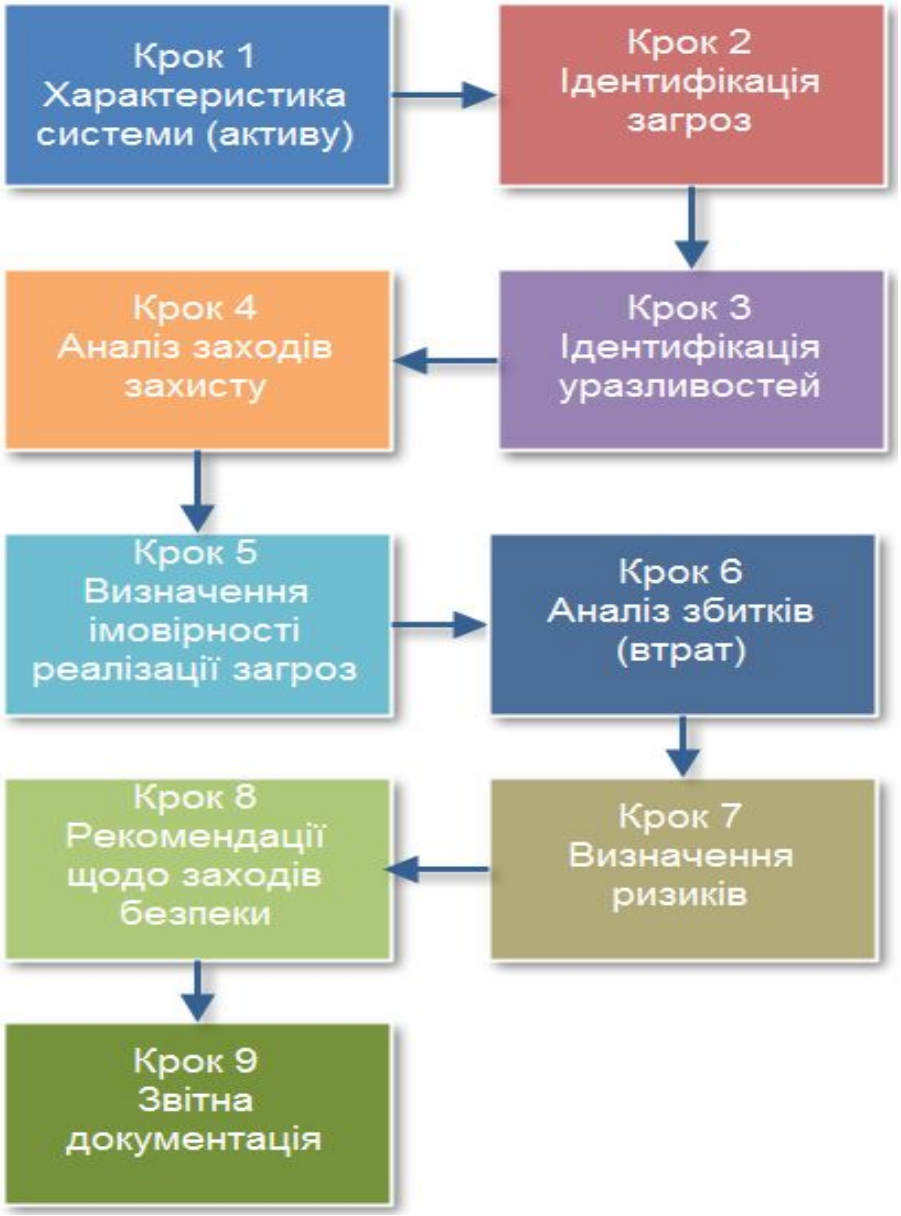
Методологія пропорційного аналізу ризиків (**MESARI**)

Метод оцінки операційно критичних загроз, активів та уразливостей
(Operationally critical threats, assets and vulnerability evaluation – **OCTAVE**)

Методологія аналізу інформаційних ризиків Міжнародного Форуму з інформаційної безпеки
(Information Risk Analysis Methodology – **IRAM**)

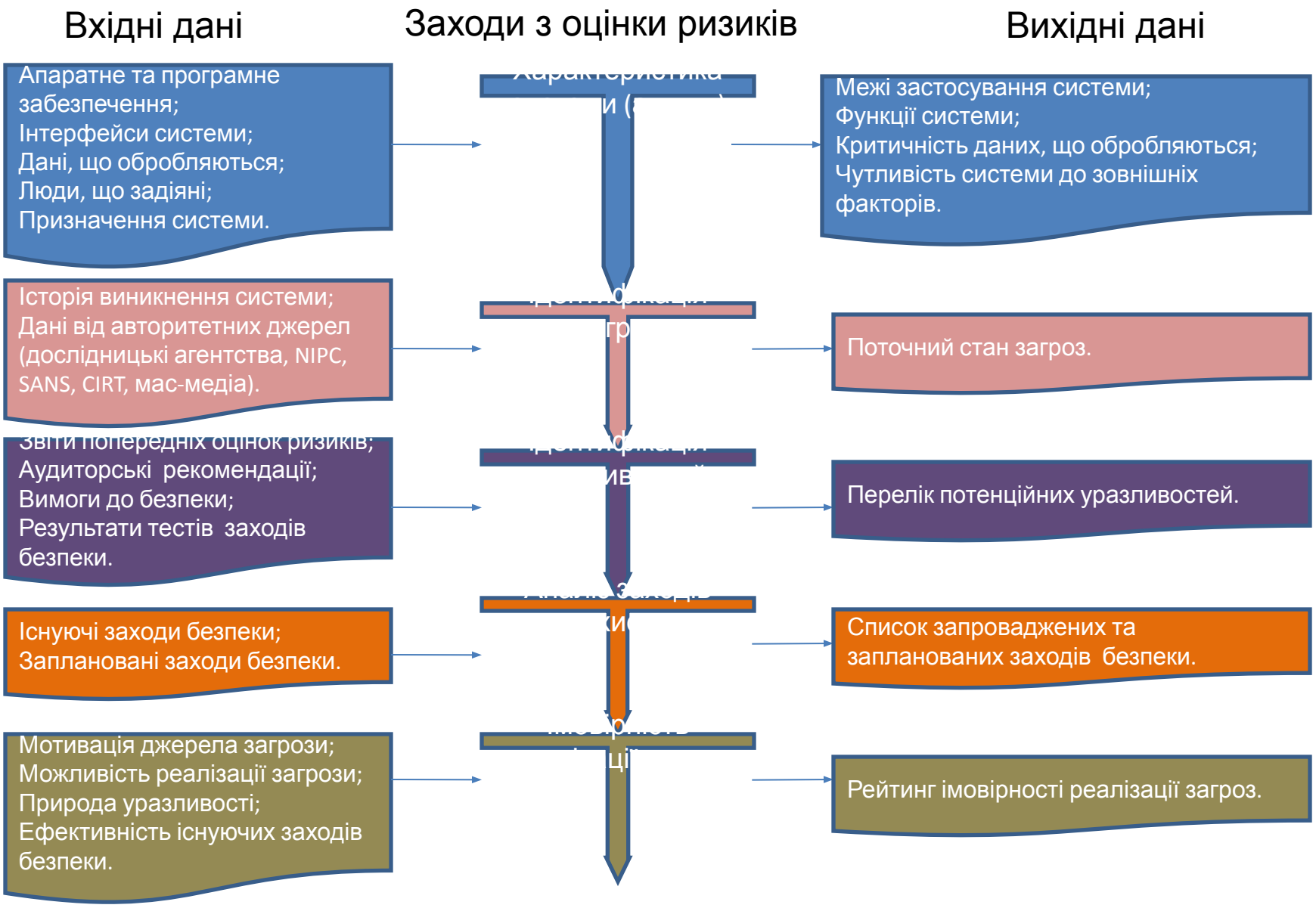
Методика оцінки ризиків NIST

Active Audit Agency
Perfection has no limits...



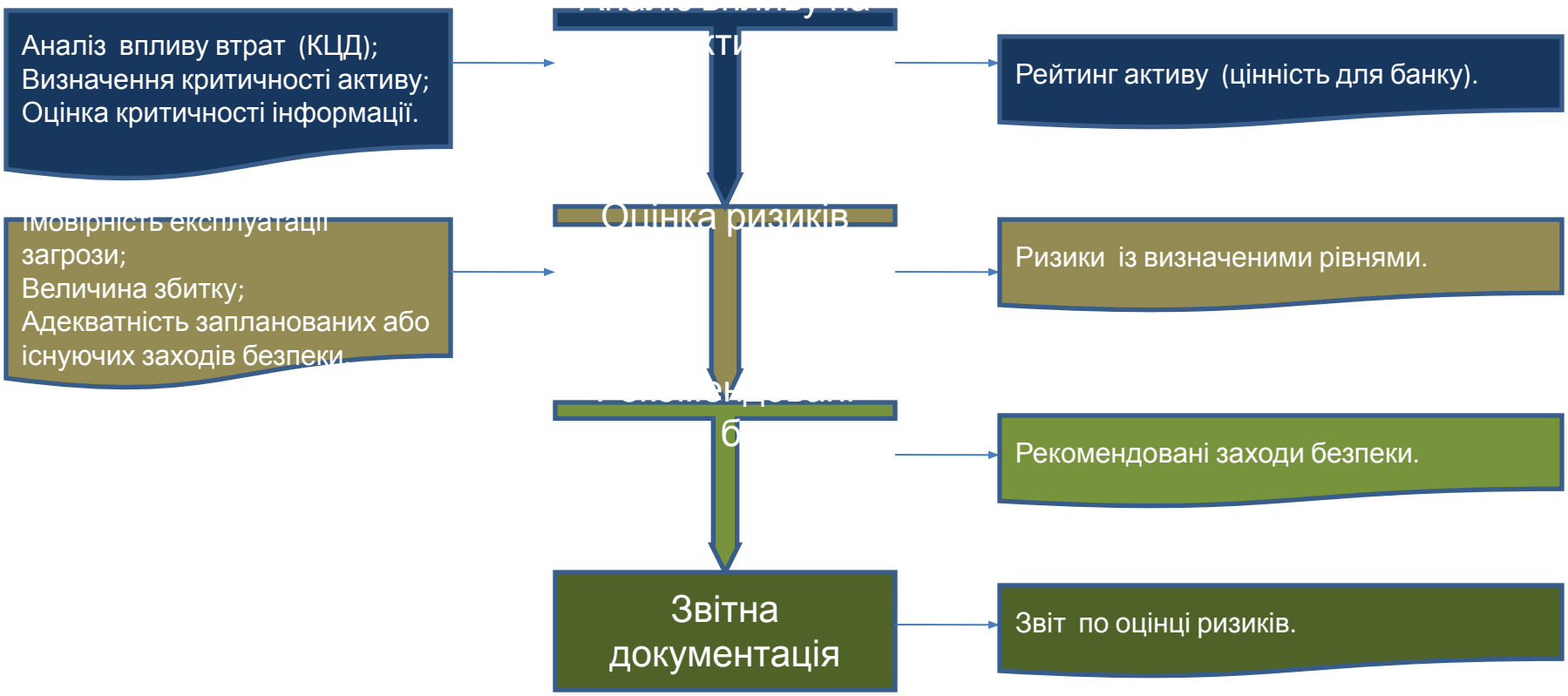
Оцінки IT ризиків згідно NIST

Active Audit Agency
Perfection has no limits...



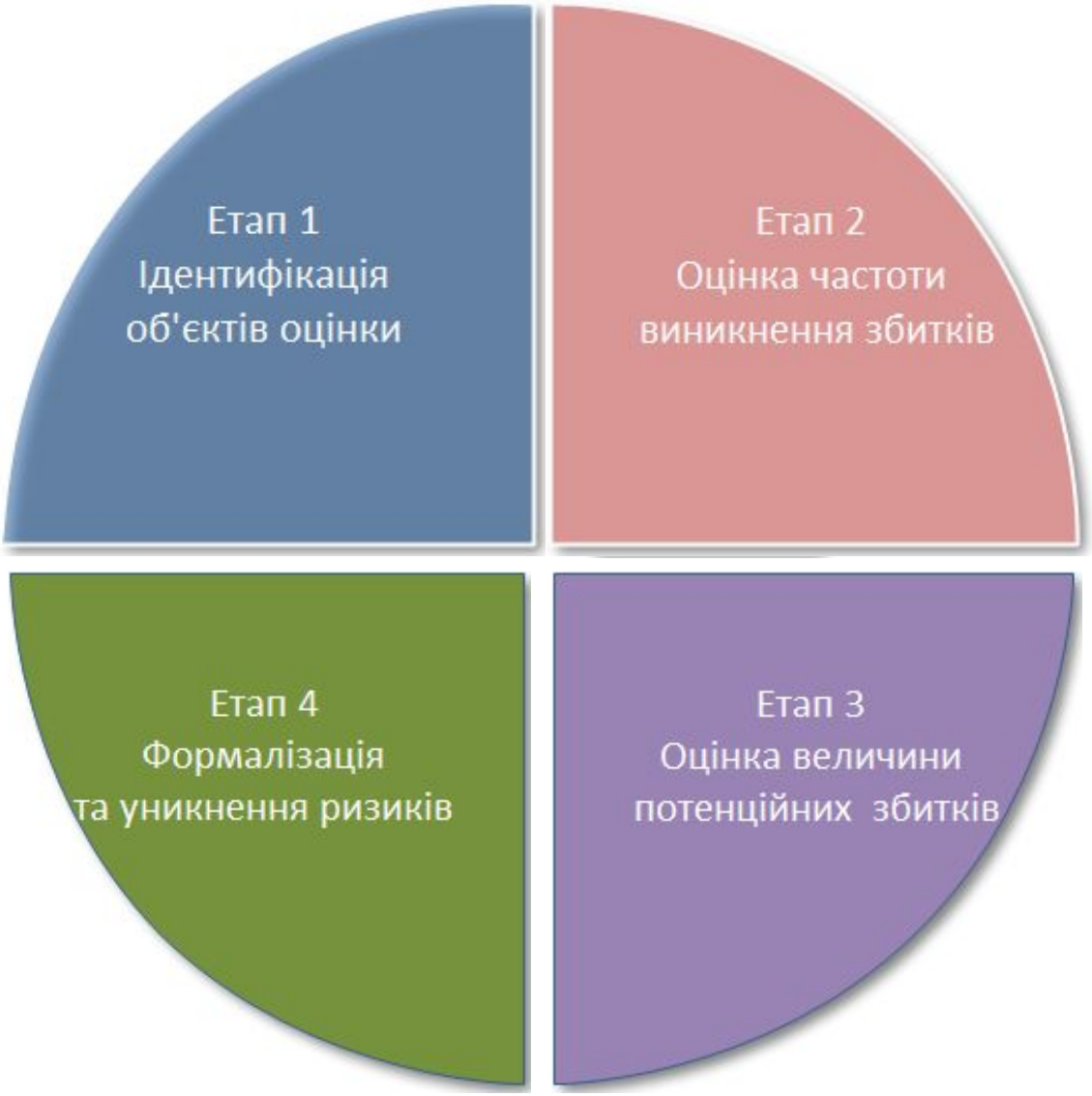
Оцінки IT ризиків згідно NIST

Active Audit Agency
Perfection has no limits...



Методика оцінки ризиків FAIR

Active Audit Agency
Perfection has no limits...



Приклад оцінки ризиків згідно FAIR

Active Audit Agency
Perfection has no limits...

Сценарій оцінки ризику

Посадова особа з відділу кадрів великого банку записала пароль та логін на нотатку та приклеїла до монітору. Таким чином, це полегшує цій особі вхід до мережних ресурсів та на сервер для запуску програмного забезпечення відділу кадрів. Перед початком поміркуємо над співвідношенням рівня ризику та оцінимо події…

Кроки аналізу ризиків

- 1.1 Визначимо актив, на який впливає ризик (ПЗ та атрибути)
- 1.2 Визначимо чинники загрози (прибиральниця, інші співробітники, відвідувачі відділу, співробітники технічної підтримки, наймані особи)
- 2.1 Оцінимо можливу частоту виникнення загрози

Rating	✓	Description
Very High (VH)		> 100 times per year
High (H)		Between 10 and 100 times per year
Moderate (M)		Between 1 and 10 times per year
Low (L)	✓	Between .1 and 1 times per year
Very Low (VL)		< .1 times per year (less than once every ten years)

Приклад оцінки ризиків згідно FAIR

Active Audit Agency
Perfection has no limits...

Кроки аналізу ризиків

- 2.2 Визначимо можливість реалізації загрози (знання та досвід)

Rating	✓	Description
Very High (VH)		Top 2% when compared against the overall threat population
High (H)		Top 16% when compared against the overall threat population
Moderate (M)	✓	Average skill and resources (between bottom 16% and top 16%)
Low (L)		Bottom 16% when compared against the overall threat population
Very Low (VL)		Bottom 2% when compared against the overall threat population

- 2.3 Визначимо рівень захищеності активу (знання та досвід)

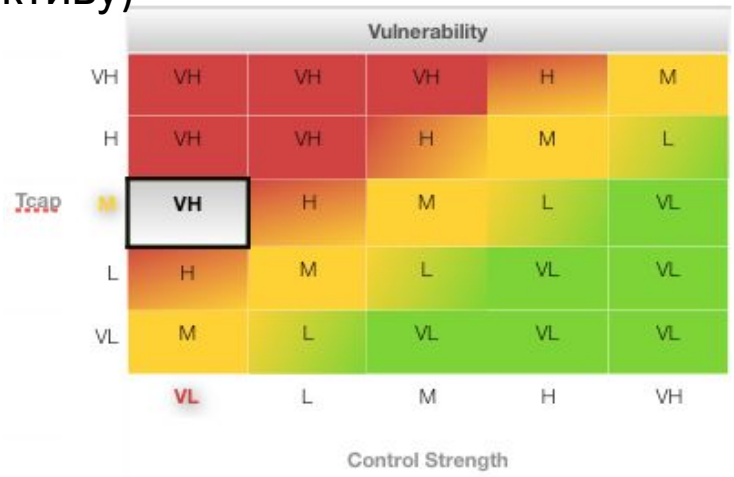
Rating	✓	Description
Very High (VH)		Protects against all but the top 2% of an avg. threat population
High (H)		Protects against all but the top 16% of an avg. threat population
Moderate (M)		Protects against the average threat agent
Low (L)		Only protects against bottom 16% of an avg. threat population
Very Low (VL)	✓	Only protects against bottom 2% of an avg. threat population

Приклад оцінки ризиків згідно FAIR

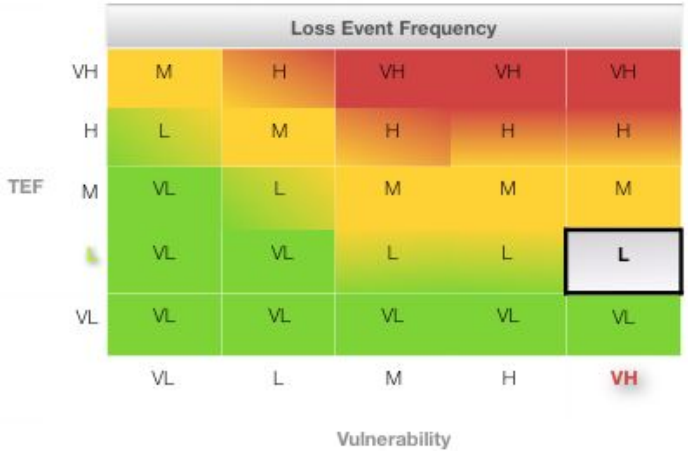
Active Audit Agency
Perfection has no limits...

Кроки аналізу ризиків

- 2.4 Визначимо уразливість активу (зусилля для отримання доступу – рівень захищеності активу)



- 2.5 Визначимо частоту виникнення втрат (втрати конфіденційності активу)



Приклад оцінки ризиків згідно FAIR

Active Audit Agency
Perfection has no limits...

Кроки аналізу ризиків

- 3.1 Визначимо втрати в найгіршому випадку

	Loss Forms					
Threat Actions	Productivity	Response	Replacement	Fine/Judgments	Comp. Adv.	Reputation
Access						
Misuse						
Disclosure	H	H	--	SV	H	SV
Modification						
Deny Access						

Magnitude	Range Low End	Range High End
Severe (SV)	$10,000,000	--
High (H)	$1,000,000	$9,999,999
Significant (Sg)	$100,000	$999,999
Moderate (M)	$10,000	$99,999
Low (L)	$1,000	$9,999
Very Low (VL)	$0	$999

- 3.2 Визначимо величину можливих втрат

	Loss Forms					
Threat Actions	Productivity	Response	Replacement	Fine/Judgments	Comp. Adv.	Reputation
Access						
Misuse						
Disclosure	M	H	VL	H	H	SV
Modification						
Deny Access						

Приклад оцінки ризиків згідно FAIR

Active Audit Agency
Perfection has no limits...

Кроки аналізу ризиків

- 4.1 Вимірюємо та формалізуємо ризик

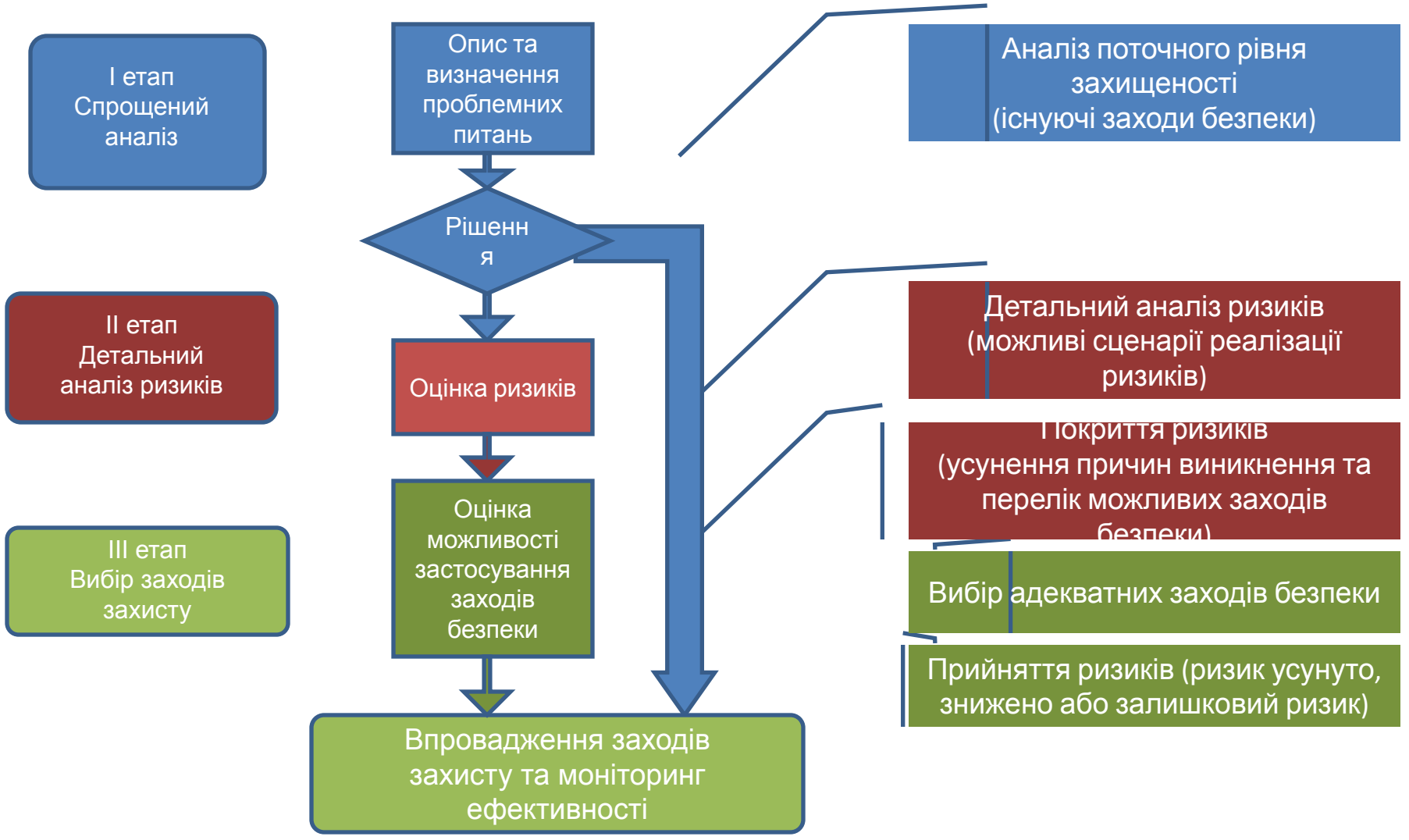
Методика оцінки ризиків MESARI

Active Audit Agency
Perfection has no limits...

I етап	II етап	III етап
Опис активів або активу та визначення проблемних питань	Визначення ризиків та заходів безпеки	Вибір заходів захисту

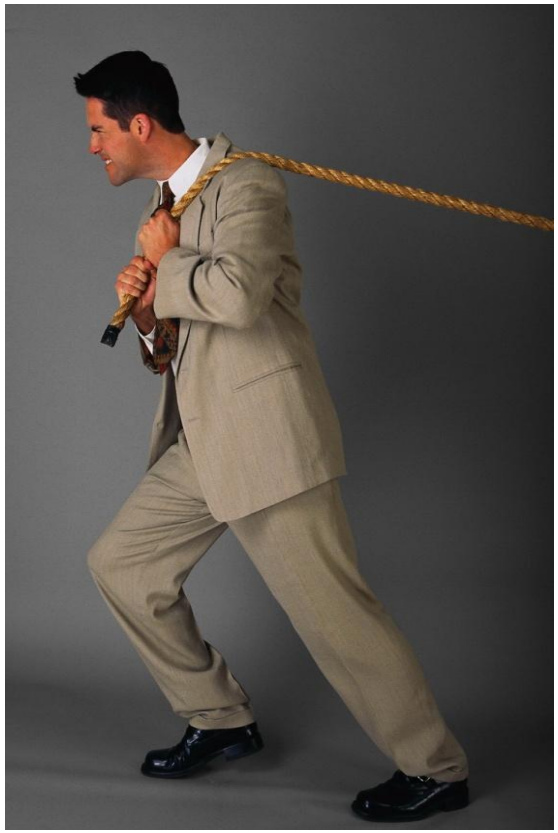
Методика оцінки ризиків MESARI

Active Audit Agency
Perfection has no limits...



Методика оцінки ризиків OCTAVE

Active Audit Agency
Perfection has no limits...



- Встановити критерії для управління ризиками
- Розробити перелік інформаційних активів
- Ідентифікувати зміст інформаційних активів
- Ідентифікувати межі застосування
- Визначити сценарії загроз
- Визначити ризики
- Проаналізувати ризики
- Обрати підходи по зменшенню ризиків

Приклад оцінки ризиків по методу OCTAVE

Active Audit Agency
Perfection has no limits...

Information Asset Ris

How would the information asset's security requirements be breached?	set.		
(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ High	❑ Medium	❑ Low

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	**(8) Severity** *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
If there is a system crash and the hospital is unable to recall backup tapes to restore transactions, then all transaction will need to be restored from paper patient records.	Reputation & Customer Confidence	Low	2
	Financial	High	12
There would be significant financial and productivity impacts to restore transaction.	Productivity	High	9
	Safety & Health	Low	5
Likely that during the restoration process many charges would be overlooked or incorrectly added. There would be losses for the missing changes and possibly increased reimbursement time as insurance companies disputed incorrect charges.	Fines & Legal Penalties	Low	1
	User Defined Impact Area		
		Relative Risk Score	**31**

Методика оцінки ризиків IRAM

Active Audit Agency
Perfection has no limits...

I Етап – Ідентифікація інформаційних активів

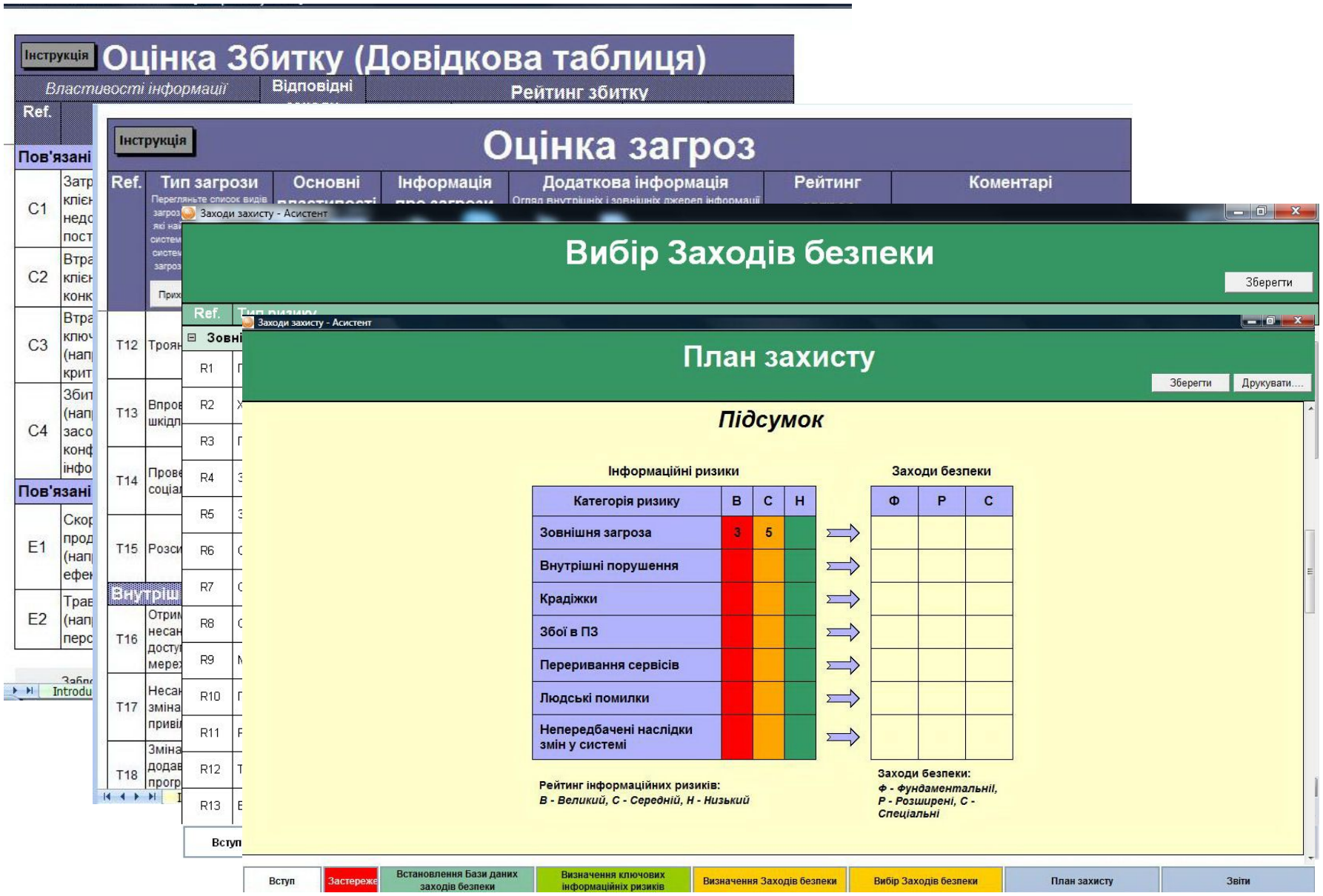
II Етап – Класифікація інформаційних активів з точки зору безпеки

III Етап – Оцінка (моделювання) загроз для інформаційних активів

IV Етап – ДІЯ (заходи по зниженню або усуненню загроз)

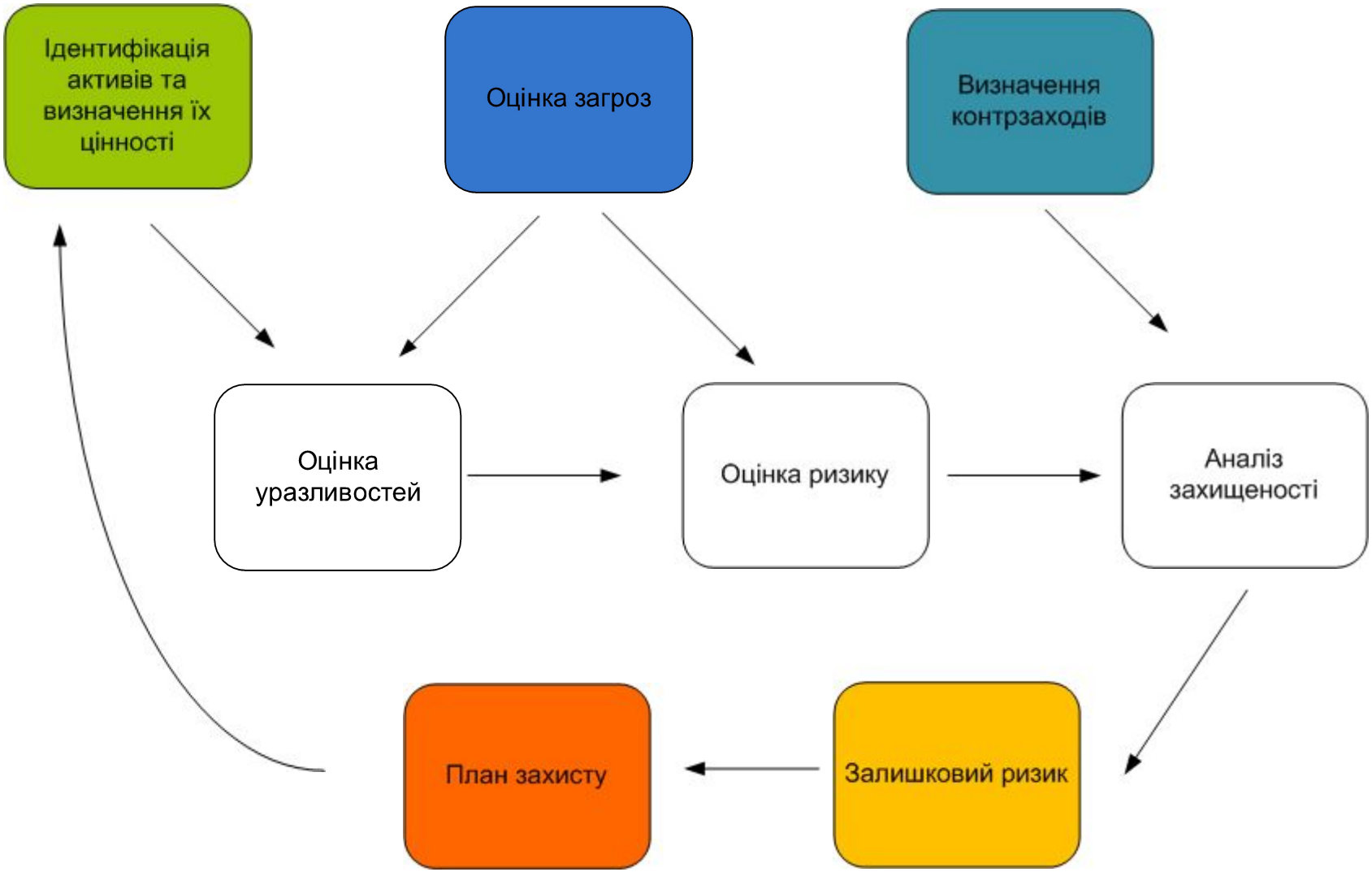
Проведення оцінки ризиків згідно IRAM

Active Audit Agency
Perfection has no limits...



Узагальнення процесу аналізу IT ризиків

Active Audit Agency
Perfection has no limits...



Порівняння методів оцінки

Active Audit Agency
Perfection has no limits...

Метод оцінки	Переваги	Недоліки
NIST	✔Детальний опис всіх ризиків для активів; ✔Найбільше підходить для відносно великих організацій.	– Довготривалий процес – Деякі функції не автоматизовані
FAIR	✔ Надає кількісний аналіз ризиків ✔ Забезпечує симуляційну модель системи	– Занадто “науковий” метод – Тільки для відносно великих банків
MESARI	✔ Спрямований на банківську діяльність ✔ Підходить для нових (новостворюваних) активів (проектів)	– Важко запровадити для існуючих активів – Достатня складність –Відсутність автоматизації процесів оцінки
OCTAVE	✔ Швидко впроваджується ✔ Добре застосовується для будь-якої організації	– Важкість реалізації окремих етапів та відсутність автоматизації – Не спрямований на специфіку банківської сфери
IRAM	✔ Відносна простота впровадження ✔ Зрозумілість для менеджерів банківських установ	– Відносно дорогий – Краще застосовується до існуючих інформаційних

Висновки

Active Audit Agency
Perfection has no limits...

- Методики оцінки IT ризиків повинні враховувати специфіку банківської справи (НБУ буде рекомендувати власну методику)

- Окремі етапи оцінки IT ризиків повністю автоматизовані;
  - розроблені (або розробляються) системні утиліти для оцінки ризиків;
  - надаються утиліти для моделювання загроз та уразливостей;
  - є програмне забезпечення та документи для проведення оцінки.

- Необхідно готувати персонал для проведення аудиту інформаційної безпеки (внутрішнього та зовнішнього) та управління ризиками IT

- Необхідно забезпечити впровадження методики та консультаційну підтримку

Запитання

Active Audit Agency
Perfection has no limits...

info@auditagency.com.ua

www.auditagency.com.ua

044 228 15 88