Rijksacademie voor Financiën,
Economie en Bedrijfsvoering
*Ministerie van Financiën*

# Тренінг із IT-Аудиту

## День 1

*Київ, грудень 2017*

Манфред ван Кестерен
Яспер Венеман

Rijksacademie voor Financiën,
Economie en Bedrijfsvoering
*Ministerie van Financiën*


- Початок - 10.00
- Перерва на каву 11:20-11:40
- Обід 13:00-14:00
- Перерва 15:15-15:25
- Завершення 16:15

# Вступ

- Хто є доповідачі?
- Огляд програми
- Хто є учасники?

Rijksacademie voor Financiën,
Economie en Bedrijfsvoering
*Ministerie van Financiën*

# Представлення

**Манфред ван Кестерен**

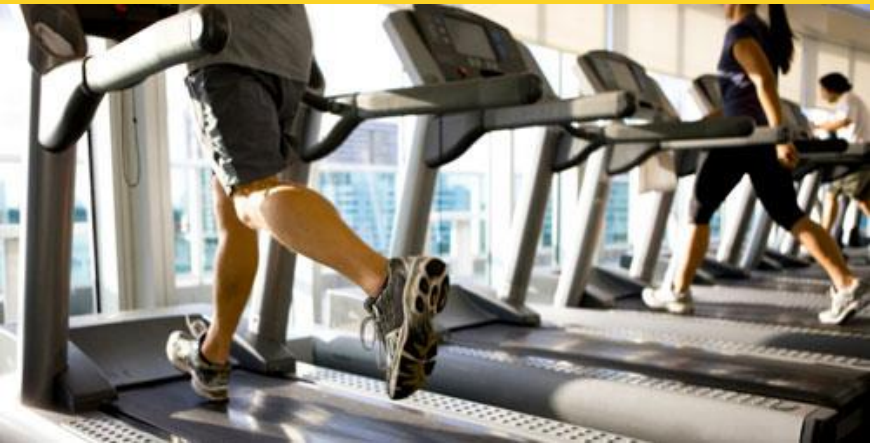

Base 800382 (A01914) 3-87


PHILIPS


TU/e
PHILIPS
DESIGN
ACADEMY
EINDHOVEN
ASML
Eindhoven


Eindhoven


PSV




POP CORN
POP CORN
take :
TICKET

- Старший внутрішній аудитор;
- Ступінь магістра соціології – політика, організація та соціальні технології;
- Більше 10 років досвіду у проведенні/управлінні внутрішнім (операційним) аудитом;
- Фокусування та управлінні та контролі;
- Міжнародний досвід у кількох проектах ЄС – Твіннінг та ДВФК;
- Член Інституту внутрішніх аудиторів (IIA);
- Керівник із Внутрішнього аудиту;
- Експерт асоціації ПЕМПАЛ (PemPal).

Rijksacademie voor Financiën,
Economie en Bedrijfsvoering
*Ministerie van Financiën*

# Представлення

**Яспер Венеман**

# Представлення Яспера Венемана

- Старший IT-аудитор в Центральній Урядовій службі аудиту
- Магістр з Бізнесу та IT
- Магістр з фінансового управління
- Виконавчий магістр з фінансового управління
- Зареєстрований IT-аудитор
- Понад 8 років досвіду з проведення/управління IT-аудитів в голландському центральному Уряді
- Зосереджувався на технічних аудитах, безпеці мережі та інформаційній безпеці

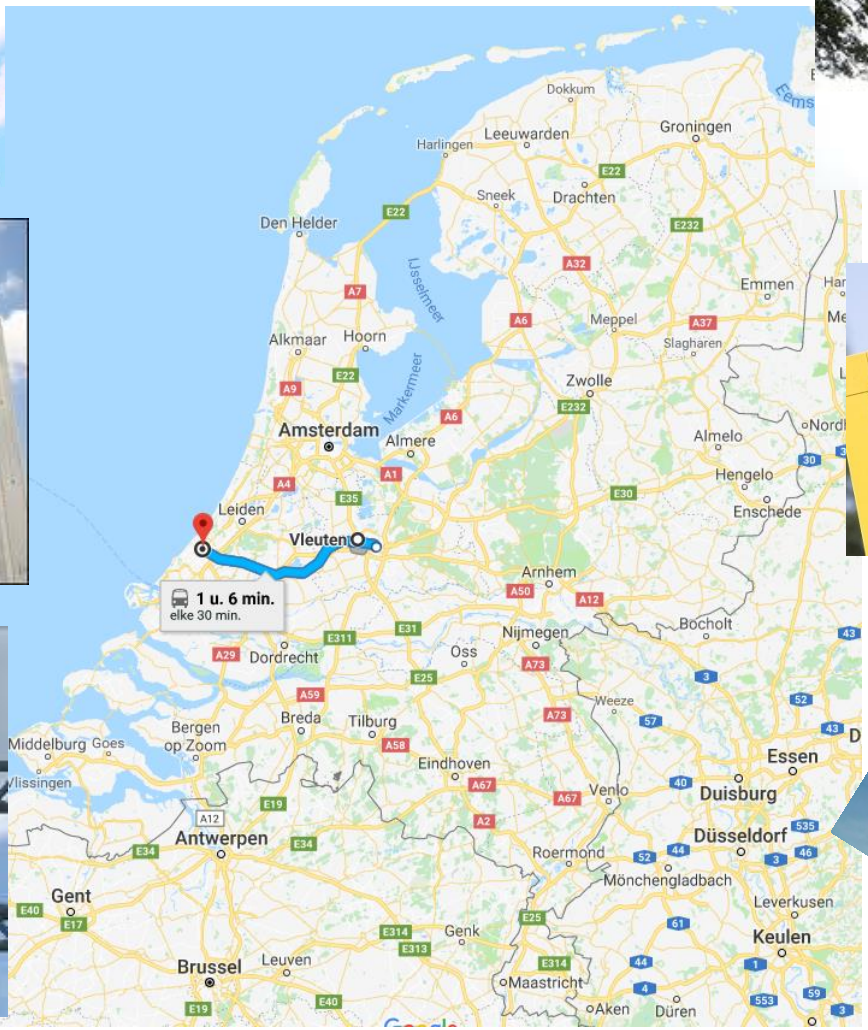

Almelo


Nieuwegein


Groningen


Utrecht


E 71
M3
MATRICA
VIGNETTE
Budapest


1 u. 6 min.
elke 30 min.
Amsterdam
Rotterdam
Den Haag
Utrecht
Eindhoven
Groningen
Leeuwarden
Arnhem
Nijmegen
Enschede
Zwolle
Almelo
Hengelo
Meppel
Emmen
Drachten
Sneek
Harlingen
Dokkum
Den Helder
Alkmaar
Hoorn
Almere
Leiden
Vleuten
Dordrecht
Breda
Tilburg
Bergen op Zoom
Middelburg
Goes
Vlissingen
Antwerpen
Gent
Brussel
Leuven
Genk
Maastricht
Aken
Düren
Venlo
Roermond
Mönchengladbach
Duisburg
Essen
Düsseldorf
Leverkusen
Keulen
Bocholt
Weeze
Oss
IJsselmeer
Markermeer


Den Haag

# Про Центральну Урядову Службу Аудиту

- Утворена 1 травня 2012

- Об'єднання/злиття департаментів аудиту міністерств.

- Нагляд, координація та моніторинг зі сторони Міністерства фінансів, незалежне розміщення та робота для всіх міністерств.

- Близько 600 працівників (100 IT- аудиторів)

# Не забувайте

- ✓Слухати / запитувати / дискутувати
- ✓Навчатися
- ✓Жартувати

# Теми на сьогодні та майбутнє

- Вступ до IT та IT аудиту;
- Кроки, що здійснюються у IT аудиті;
- IT-управління;
- Межі аудиту, інструменти IT аудиту;
- IT- заходи контролю;
- Практичні приклади;
- Короткі вправи.

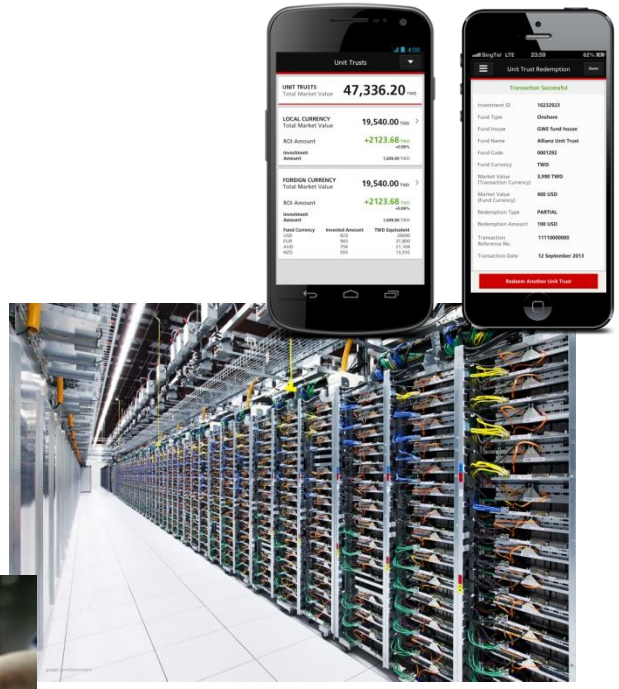
# Навчальні цілі

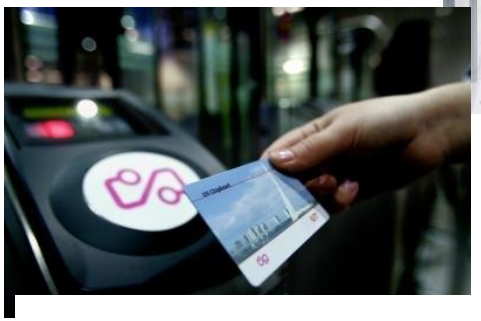
- Функція / Організація
- Що Ви вже знаєте (досвід)?
- Чого хочете навчитися?
- Що спробувати на практиці?
- Що очікуєте від нас?

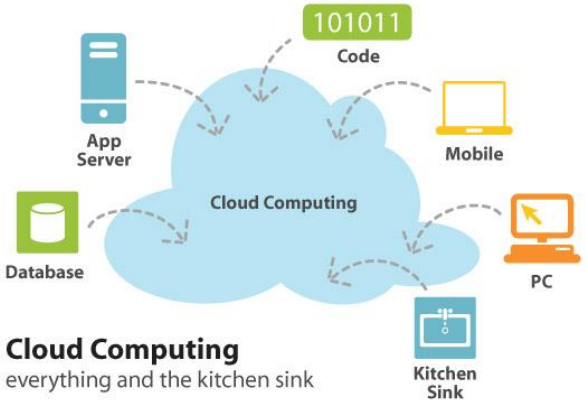
# Середовище/світ IT

- IT управління
- Проекти та програми
- Процеси та інформаційні системи
- Управління IT-послугами
- Інфраструктура
- Інформаційна безпека

# Світ IT






Можете назвати деякі нові напрямки у IT?


Vulnerability
Patch
Privacy
Threat
SIEM
Advanced
Secure
Risk
malware
Log
Risk-Management
CISO
Solution
Compliance
Configuration
Prevent
Identity
analytics.
Mobile
Detect
detection
cso
big
Value
Next-Gen
breach
Human
Scan
Unified
Business
Cloud
Data
code
CVSS
SCAP
security
Intelligence
Next-Generation
Standards
BYOD
Service
data
Authorization
Encryption
Enterprise

# Нещодавні зміни в Україні – 2017

TECH • CYBERSECURITY

## New Cyber Attacks Are Hitting Airports and Metro Systems in Ukraine

THE CABLE

## Ukraine Hit by Massive Cyberattack

It's unclear who or what is behind it.

BY EMILY TAMKIN | JUNE 27, 2017, 10:55 AM

BBC | Sign in | News | Sport | Weather | Shop | Earth | Travel

NEWS

Home | Video | World | UK | Business | Tech | Science | Stories | Entertainment & Arts

Technology

## Ukrainian postal service hit by 48-hour cyber-attack

10 August 2017 Share

TECHNOLOGY

## *Cyberattack Hits Ukraine Then Spreads Internationally*

By NICOLE PERLROTH, MARK SCOTT and SHEERA FRENKEL JUNE 27, 2017

WIKIPEDIA
The Free Encyclopedia

Article | Talk

## 2017 cyberattacks on Ukraine

From Wikipedia, the free encyclopedia

# Програма

- Вступ
  - Хто є тренери
  - Представлення Нідерландської Центральної служби аудиту
  - Навчальні цілі
- Світ ІТТ
- **Від ІТ до ІТ аудиту**
  - Визначення ІТ- аудиту, аспекти якості, рівні захисту
- Проведення ІТ аудиту від початку до кінця

# Від IT до IT - аудиту

- «Оцінка якості» IT систем та процесів, виходячи із меж проведення аудиту.
- Межі проведення аудиту визначають критерії, яким повинні відповідати  IT системи.

# Поняття IT аудиту

*"IT* аудит – це незалежна та об'єктивна оцінка надійності, безпеки (включаючи конфіденційність), ефективності та результативності автоматизованих інформаційних систем, організації автоматизованих департаментів, а також технічної та організаційної інфраструктури автоматизованих інформаційних процесів.
Цей вид діяльності застосовується як до операційних систем так і систем, що розробляються*"*
*(Norea, 1992 стор.99; Strous, 1998)*

# Поняття IT аудиту

*“ Забезпечення додаткових гарантій шляхом оцінки (управління) одного або більше якісних аспектів об'єктів інформаційного забезпечення”*

# Аспекти якості

- **К**онфіденційність: запобігати неавторизованому розкриттю даних особам, установам або процесам.
- **П**равдивість: повнота і точність даних. Немає неавторизованих змін, послідовні дані.
- **Д**оступність: надійний та своєчасний доступ до даних.

# Об'єкти IT-аудиту

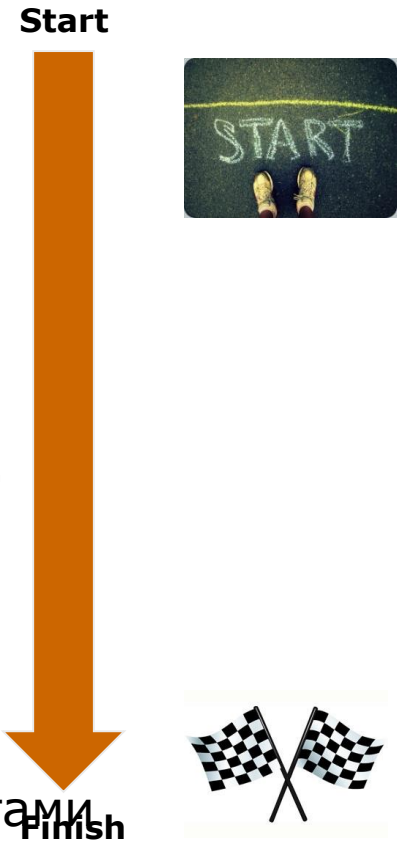
- Процес
- Процедури
- Система
- Проект
- Основні продукти
- IT-управління, політики і плани

# Деякі приклади IT аудитів, що проводила Центральна урядова служба аудиту

- Тестування системи онлайн аукціону, що був застосований урядом для  аукціонера Telecom.
- Поради в частині автоматизації документальних процесів Міністерств.
- Тестування безпеки Blackberries, які використовують службовці
- Тестування безпеки автоматизованих систем подачі заяв громадянами, у яких зберігаються дані про повернені податки.
- Аудит безпеки хмаринкових та віртуальних технологій.
- Аудит інформаційних центрів
- Тестування програмних модулів у великих фінансових системах.

# Проведення IT аудиту від початку і до кінця

1) Запит від (вищого) керівництва
2) Попередня зустріч із (вищим ) керівництвом
3) Опис аудиторського підходу
4) Проведення аудиту
    1) Збір необхідних даних
5) Інтерпретація та оцінка знахідок
6) Опис знахідок у аудиторському звіті
7) Представлення та обговорення знахідок із (вищим) керівництвом
8) Оцінка аудиту
    1) Оцінка із командою
    2) Оцінка із (вищим) керівництвом
9) Архівування всіх даних у Системі управління аудитами
10) Відстеження рекомендацій та поради



# 1. Запит/завдання від (вищого) керівництва

- Вище керівництво може мати будь-які причини для необхідності проведення IT аудиту, наприклад:
  - Відповідність (‘Я повинен відповідати ISO27001’ )
  - Відповідність новому законодавству
  - Поява порушень безпеки
  - Замовник хоче знати чи він/вона вразливі
  - Отримати інформацію щодо рівня безпеки
  - Рахункова палата поставила вимогу провести аудит
  - Укладення угоди із новим IT партнером
  - Перевірити, чи вони готові до продовження (перерва в роботі, пожежа, пошкоджені драйвера)
  - Планується встановлення нової IT системи

# 2. Попередня зустріч із (вищим) керівництвом

Перед зустріччю:

- Зберіть всю IT інформацію та інформацію про організацію, яку можете отримати та підготувати.
- Визначте можливий та приблизну потребу часу.
- Визначте кращих учасників команди

Під час зустрічі:

- Обговоріть причину проведення аудиту.
- Досягніть політичної згоди для проведення аудиту.
- Домовтеся, як збирати (вразливі) аудиторські докази та дані.

Ставте правильні запитання! Що б Ви запитали?

# 2. Попередня зустріч із (вищим) керівництвом

*Оцініть:*

- Чи є у вас (Вашої команди) достатні знання, щоб проводити аудит даного об'єкту?
- Чи можете ви виявити всі важливі аспекти?
- Чи незалежні ви від об'єкту аудиту?
- Чи замовлення на проведення аудиту надійшло він необхідного рівня керівництва?
- Чи розумієте ви запитання керівництва, чи потрібно провести попереднє дослідження щоб сформулювати більш детальні запитання?
- Профіль ризиків завдання:
  - Складність
  - Відповідна правова база
  - Необхідні знання
  - Політична та управлінська увага
  - Можливий вплив на результат аудиту

# 3. Опис аудиторського завдання

- Питання, які необхідно включити у аудиторське завдання:
  - ❑ Ключові запитання (вищого) керівництва
  - ❑ Мета аудиту
  - ❑ Запитання для аудиту
  - ❑ Вид аудиту
    - ❑ Звіт щодо надання гарантій
    - ❑ Звіт щодо одержаних знахідок
    - ❑ Звіт із рекомендаціями
  - ❑ Які критерії якості та межі будуть застосовані?
  - ❑ Границі об'єкта аудиту
  - ❑ Члени команди
  - ❑ Планування
  - ❑ Підпис керівника аудиту
  - ❑ Підпис замовника
  - ❑ Договір про нерозголошення інформації

# 4. Проведення аудиту – збір даних (I)

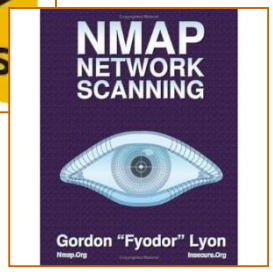
Інструменти IT аудитора:

- Сканування вразливості
- Сканування виявлення мережі
- Сканування веб-прикладних прогр
- Спостереження
- Технічна документація
- Конфігураційні файли
- Журнали реєстрації
- Інтерв'ю
- Огляди (e.g.: Limesurvey)
- Тощо…

# 4. Проведення аудиту – збір даних (II)

## Інструменти аудитора

- Які інструменти, кращі практики та стандарти Ви застосовуєте?





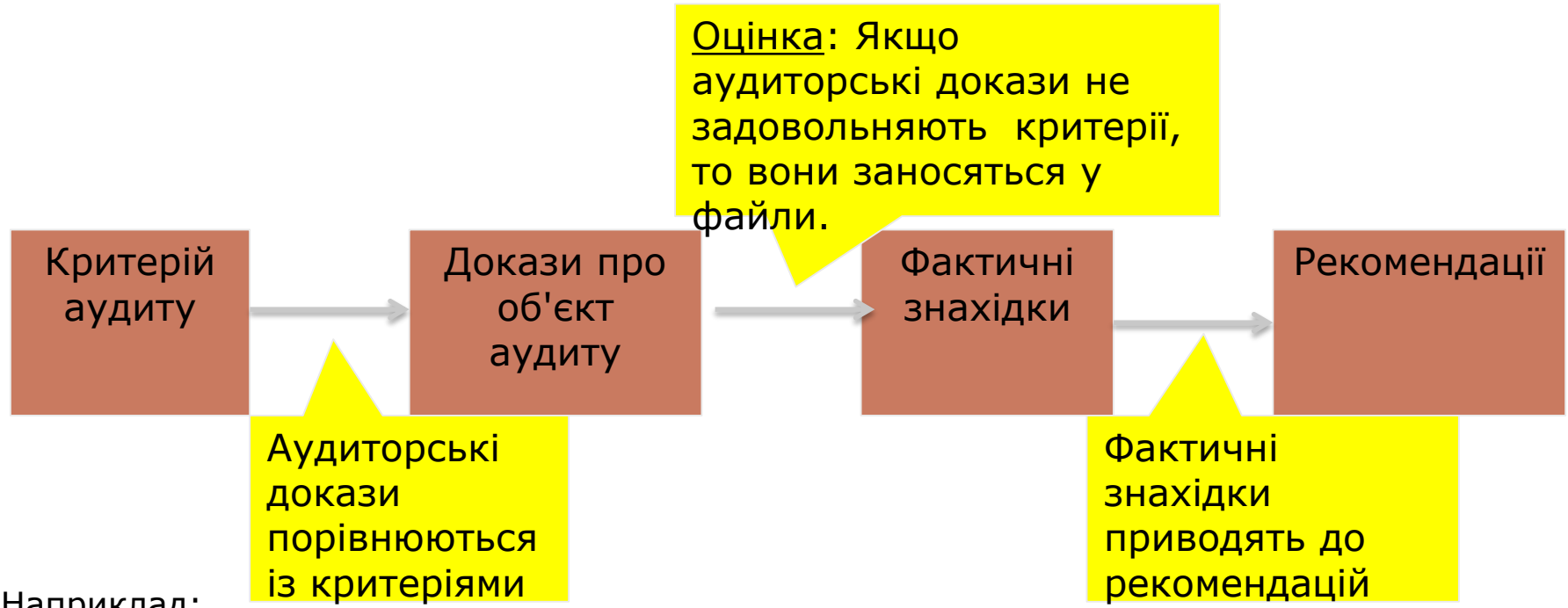
- На місці чи поза робочим місцем?
- Застосовуєте свої інструменти, чи інструменти об'єкта аудиту

# 4. Проведення аудиту – збір даних (III)

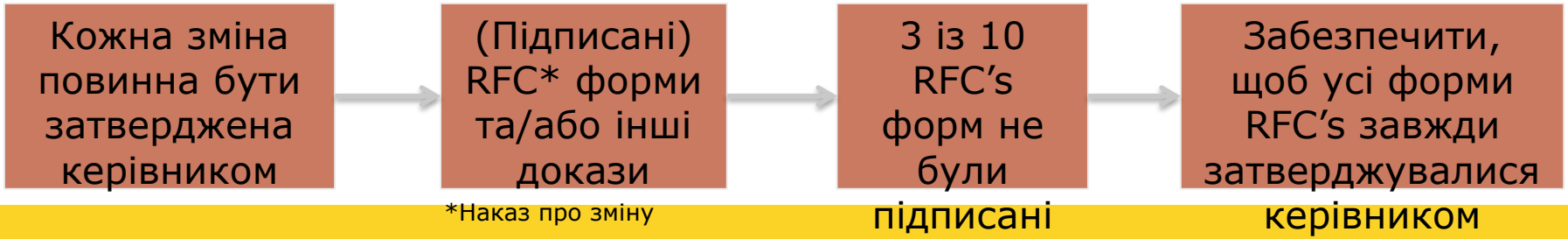
Практичні приклади

- Вивчення об'єкту аудиту: технічне та організаційне.
- Запитайте про відповідну політику на кожному рівні (напр. IT, IT безпеки).
- Ув'яжіть критерії аудиту із відповідними працівниками.
- Заплануйте інтерв'ю із працівниками.
- Перед інтерв'ю: Попросіть працівників про необхідну функціональну, технічну та тестову документацію.
- Вивчіть політики та документи.
- Проведіть інтерв'ю із працівниками, використовуючи критерії аудиту. Попросіть докази, такі як системи входу, реєстраційні форми, е-мейли, протоколи зустрічей тощо.
- Спостерігайте та аналізуйте IT процеси.
- Тестуйте IT контролі (сприятливість середовища) та/або (випадки, зміни, форми доступу).
- Доступ до IT систем (виробниче середовище), читайте записи, параметри тощо

# 5. Інтерпретація та оцінка знахідок (I)



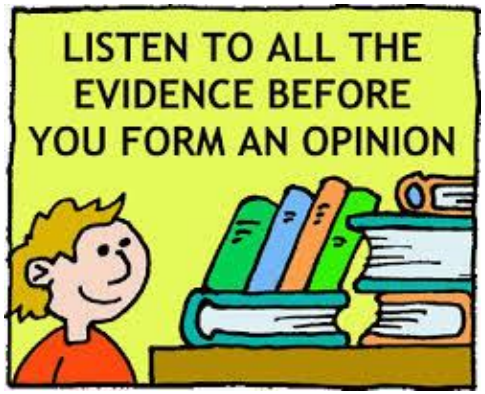

Наприклад:




*Наказ про зміну

# 5. Інтерпретація та оцінка знахідок (II)

- Пов'язуйте інформацію, індикатори, докази та думки та намагайтеся вийти на більше уявлення.
- Намагайтеся знайти причини чому.
- Рекомендації повинні бути спрямовані на причини
  а не на знахідки
- Якщо у вас проблеми із підготовкою добрих
  рекомендацій, дивіться ще раз на ваші знахідки.
- Визначайте ризики, що може відбутися, якщо…
- Робіть це конкретно для команди, підрозділу, організації.
- Впевніться що Ваш звіт про інтерв'ю, або заповнена форма подані об'єкту аудиту для коментарів.
- Коментарі від об'єкту аудиту повинні бути враховані до заключного висновку у звіті, можливо це вимагатиме додаткової роботи від аудитора.



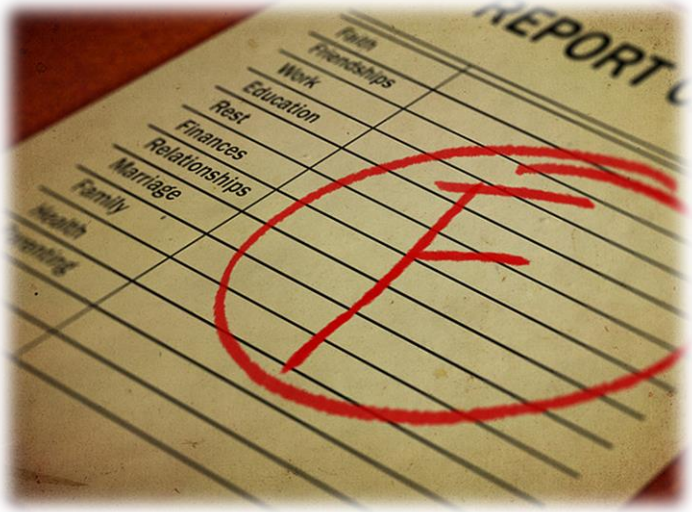
# 6. Відображення знахідок у аудиторському звіті

Два основні види звітів:

1) Звіт із гарантіями
2) Звіт про фактичні знахідки (+ рекомендації)

# 6.1 Приклад звіту із гарантіями

1. Резюме
2. Вступ
    1. Обґрунтування аудиту
    2. Структура звіту
3. Цілі аудиту та аудиторський підхід
    1. Цілі
    2. Критерії (стандарти тощо…)
    3. Аудиторський підхід
    4. Поширення звіту
4. **Висновки**
5. Рекомендації (необов'язково)
6. Підписи
7. Додатки



# 6.2 Приклад звіту із фактичними знахідками

1. Резюме
2. Вступ
    1. Підстава
    2. Структура звіту
3. Мета аудиту та аудиторський підхід
    1. Ціль
    2. Аудиторський підхід (зобов'язання щодо роботи)
    3. Поширення звіту
4. Знахідки *(немає правильно чи неправильно)*
5. Підписи
6. Додатки

Знахідки: Проблема, Ризик, Причина, Порада

Без висновків та гарантій

# 7. Представлення та обговорення знахідок із замовником

- Знахідки та рекомендації повинні бути чіткими та повними.
- Впевненість у тому, що керівник розуміє знахідки та рекомендації.
- Прохання про реакцію керівника на ваш звіт
- Переконати замовника у необхідності виділення часу та бюджету для відстеження знахідок та впровадження рекомендацій.
- Якщо є знахідки із дуже високим ступенем ризику, то дати виконання знахідок повинні бути відповідними.

# 8. Оцінювання аудиту

- Внутрішня оцінка аудиторською командою
  - Процес
  - Співпраця
  - Контроль якості
  - Комунікація
  - Планування
- Оцінювання із замовником
  - Попросити замовника заповнити анкету щодо проведення аудиту

# 9. Архівування всіх даних у системі Управління аудитами

- Для аудиторського сліду
- Для дотримання внутрішньої системи якості
- Для відповідності стандартам щодо збереження даних

# 10. Відстеження рекомендацій та поради

- При написанні аудиторського звіту можна додати графік відстеження знахідок
  - (напр.: Переконатися, що програмний сервер запрацює через 6 тижнів)
- Підтримуйте зв’язок із керівництвом, яке замовило аудит щодо впровадження керівництвом рекомендацій (час та бюджет).

National Academy for Finance and Economics
*Ministry of Finance*


Чи є запитання?

Дякуємо за увагу!