Central Government Audit Service
Ministry of Finance

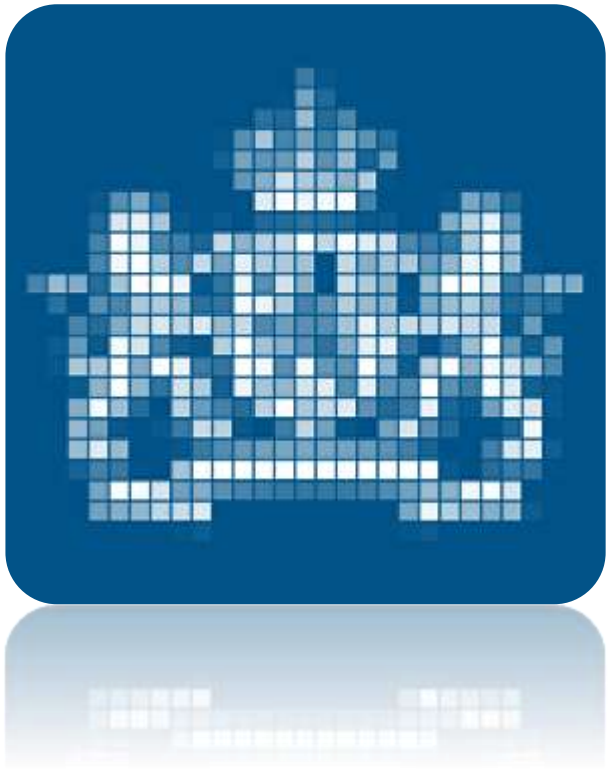
Тренінг з аудиту інформаційних технологій

Сесія 1

Маартен ван дер Ліппе

Люсінда Лунсхоф

Central Government Audit Service
Ministry of Finance



Contents

ЗМІСТ

- Вступ – лектори і ЦУСА
- Вступ IT-аудит
- Загальні заходи IT-контролю та заходи контролю прикладних програм

Goedemiddag! - Доброго дня

Маартен ван дер Ліппе

- Провідний IT-аудитор із Загальних справ
- Керівник проєкту ISAE3402
- Магістр з бізнес-управління
- Магістр з IT-аудиту, відповідності та аудиту
- Зареєстрований аудитор ЕОД (електронної обробки даних)

Люсінда Лунсхоф

- Керівниця проєкту з різних аудитів: Діджі Ді, Захисту персональних даних (Загальний регламент про захист даних / ЗРЗД), фінансовий звіт
- Магістр з управління інформацією та знаннями
- Виконавчий магістр з IT-аудиту
- Зареєстрований аудитор ЕОД (електронної обробки даних)

Про Центральну Урядову Службу Аудиту

заснована

01

травня

2012

об'єднання сильних сторін міністерських департаментів аудиту

нагляд, координація та моніторинг з боку Міністерства фінансів; незалежна позиція та робота для всіх міністерств

КЛЮЧОВІ ЦІННОСТІ

незалежна

професійна

віддана

Клієнти

міністерський рівень
(і підпорядковані органи)

Міністр

Генеральний секретар

Генеральний директор

Директор

міжміністерський рівень

Міжвідомча комісія з операційного управління

Персонал

600
працівників, з різною підготовкою

60%
фінансові аудитори

40%
операційні та IT-аудитори

спеціалізоване **стажування** з аудиту

Сектор IT

- Загалом близько 600 колег
- 100 IT-аудиторів
- спеціалісти, які працюють по всьому уряду в усіх міністерствах
- Теми:
  - Кібербезпека
    - включаючи DigiD-оцінки та пентестування
  - SAP
  - Oracle
  - ЗРЗД / персональні дані
  - Великі проекти
  - Алгоритми
  - Фінансові звіти IT та ФА

Central Government Audit Service
Ministry of Finance

Вступ до IT-аудиту

Що таке IT-аудит?

«Оцінка якості IT-систем та процесів на основі моделі аудиту.»

Хто такий IT-аудитор?

Якості та принципи:

- *Професіоналізм*
- *Доброчесність*
- *Об'єктивність*
- *Компетентність*
- *Конфіденційність*
- *Незалежність*

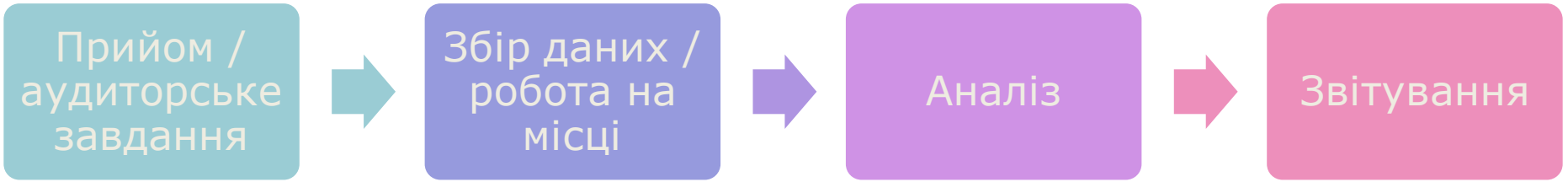
Аспекти якості

- Конфіденційність
- Цілісність
- Доступність
- Невідмова
- Контрольованість
- Результативність
- Ефективність

Об’єкти IT-аудиту

- Технічна інфраструктура (технічний аудит)
- Операційна інформаційна система (системний аудит)
- IT-процеси (наприклад, ITIL-аудит: аудит бібліотеки інфраструктури інформаційних технологій)
- Програмне забезпечення
    - Комерційне готове програмне забезпечення (COTS)
    - Стандартне програмне забезпечення з конфігурацією замовника
    - Індивідуальне програмне забезпечення
- Системи безпеки
- Захист персональних даних
- Сертифікація або акредитація
- Аудити шахрайства та судові аудити / розслідування.

Етапи IT-аудиту



- Рамкова основа
- Планування
- Зустрічі

- Інтерв’ю
- Спостереження
- Документування

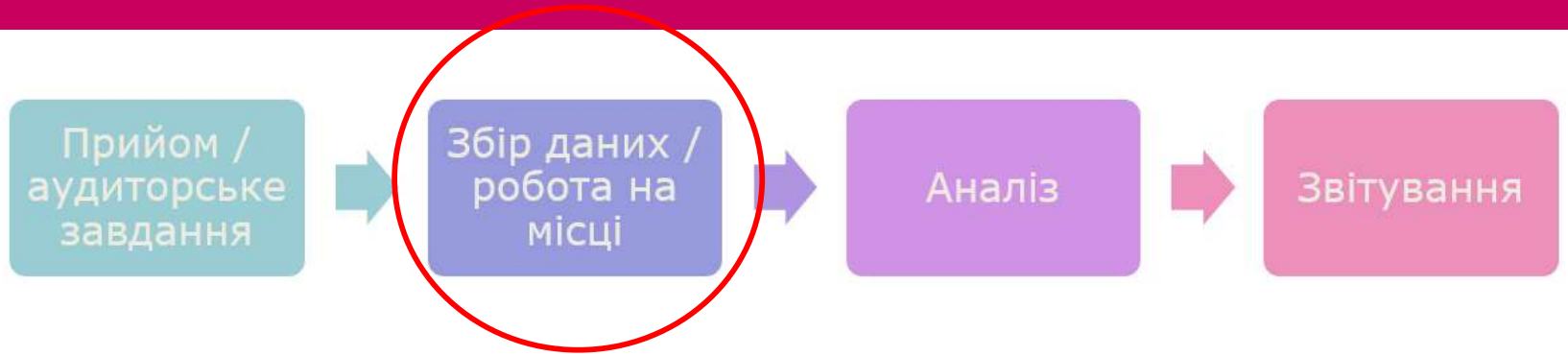
- Знахідки

- Домовленість

Прийом

- Рамкова основа
- Планування
- Зустрічі

Робота на місці



- Інтерв’ю
- Спостереження
- Документування

Аналіз

- Знахідки

Контроль	Документування	Інтерв'ю	Аналіз	Висновок
#1 пароль складається мінімум з 8 знаків	У Документі X зазначено про налаштування пароля, зокрема, що він повинен мати довжину не менше 10 символів.	Під час інтерв'ю X було сказано, що пароль має довжину 10 символів. Ми бачили це наживо під час співбесіди	Шляхом спостереження та перевірки ми визначили, що пароль має довжину 10 символів	Ефективний

Звітування

- Домовленість

Зміст аудиторського звіту:

1. Наш експертний висновок
2. Основа для експертного висновку
3. Критерії, що застосовуються
4. Питання, що покриваються нашим дослідженням
   - 4.1 Об’єкт дослідження
   - 4.2 Обмеження, пов'язані із заходами контролю
5. Обмеження щодо використання та розповсюдження звіту
6. Відповідальність керівництва сервісної організації
7. Відповідальність IT-аудитора
8. Підпис

Додаток

Central Government Audit Service
Ministry of Finance

Загальні заходи IT-контролю та заходи контролю прикладних програм

Види IT-Контролю

Огляд IT-Контролю

Говорячи про контроль IT, можна виділити дві категорії заходів контролю:

Загальні заходи IT-контролю (ЗЗІТК), що підтримують вимоги до контролю в рамках стандартних процесів підтримки IT (наприклад, управління змінами).

Заходи контролю прикладних програм (ЗКПП), які вбудовані в "стандартні" бізнес-процеси (наприклад, закупівлі, доходи тощо) і призначені для автоматизації контрольних функцій.

ЗЗІТК застосовуються до всіх системних компонентів, процесів і даних організації, в той час як заходи контролю прикладних програм є специфічними для програми або системи, що підтримує певний бізнес-процес.

*Аудитор перевіряє **дизайн** та **операційну ефективність** цих заходів контролю*

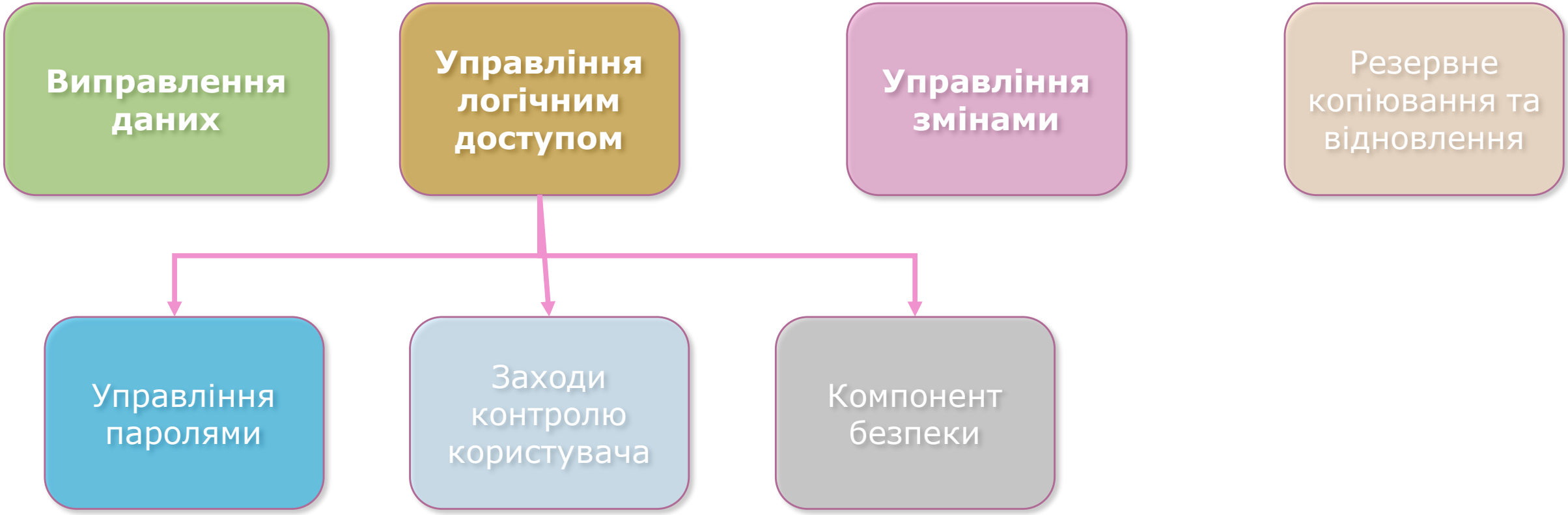
Дизайн, наявність та операційна ефективність

- *Дизайн:*
- Наприклад, опис процесу або процедури

- *Наявність:*
- Чи функціонував процес відповідно до дизайну в певний момент часу?

- *Операційна ефективність:*
- Чи функціонував процес протягом тривалого періоду часу?

Загальні заходи IT-контролю



ADR - Модель стандартів ЗЗІТК

Change management
Category
W1. Change management
W1. Change management
W1.1 : Changes must be authorised
W1.2 : Changes must be tested
W1.3 : Changes must be approved subject to test results
W1.4 : Duties to apply for, approve and implement changes must be segregated
W1.5 : Periodic checks must be made for unauthorised changes
Logical access controls
Category
L.1 Password management
L1.1 : Passwords must be periodically changed
L1.2 : Passwords must be strong
L1.3 : Two-factor authentication must be used in untrusted zones
L1.4 : Applications must be locked when inactive
L1.5 : Passwords must be encrypted when saved
L1.6 : User accounts must be blocked after a pre-set number of five incorrect login attempts
L2. User controls
L.21 : Users and administrators must have only access those rights that are necessary for their work
L2.2 : User accounts and access rights must be authorised
L2.3 : Duties to apply for, approve and implement changes in user accounts and access rights must be segregated
L2.4 : Staff departures must be processed promptly
L2.5 : Admin accounts must be limited and the reasons for them explained in so far as necessary
L2.6 : User accounts and admin accounts must be strictly personal
L2.7 : User accounts must not have direct access to underlying components
L2.8 : User and admin accounts and access rights must be periodically evaluated and the findings must be followed up
L3. Component security
L3.1 : Insight into applications and underlying components must be up to date
L3.2 : Alerts must be automatically generated for new weaknesses and systems must be periodically checked for technical weaknesses
L3.3 : Systems must be patched and updated promptly
L3.4 : Systems must not use standard passwords or backdoor accounts
L3.5 : The operating system must not run unnecessary services
L3.6 : The internal network must be isolated from untrusted environments
L3.7 : Network traffic and components must be actively monitored
Overall outcome of Logical access controls
O1. Optional
Category
O1. Optional
O1.1 : The periodicity of backups and the type of data backed up must be consistent with the systems critical for the annual accounts
O1.2 : Backup data must be kept at a secure location where the integrity of the backup is assured
O1.3 : Ability to recover the backup must be periodically tested

Управління змінами

- W1.1: Зміни повинні бути авторизованими
- W1.2: Зміни повинні бути протестованими
- W1.3: Зміни повинні бути схваленими на основі результатів тестування
- W1.4: Обов'язки щодо подання заявки, затвердження та впровадження змін мають бути розділені
- W1.5: Періодичні перевірки на наявність несанкціонованих змін

Управління паролями

- L1.1: Паролі необхідно періодично змінювати
- L1.2: Паролі повинні бути надійними
- L1.3: Двофакторна автентифікація повинна використовуватися в ненадійних зонах
- L1.4: Додатки повинні бути заблоковані, коли вони неактивні
- L1.5: Паролі повинні бути зашифровані при збереженні
- L1.6: Облікові записи користувачів повинні блокуватися після попередньо встановленого числа з десяти неправильних спроб входу

Заходи контролю користувачів

- L2.1: Користувачі та адміністратори повинні мати доступ лише до тих прав, які необхідні для їхньої роботи
- L2.2: Облікові записи користувачів та права доступу повинні бути авторизовані
- L2.3: Обов'язки подавати заявки, затверджувати та впроваджувати зміни в облікових записах користувачів та правах доступу повинні бути розділені
- L2.4: Відсутність співробітників повинна оброблятися оперативно
- L2.5: Облікові записи адміністраторів мають бути обмежені, а причини цього мають бути пояснені
- L2.6: Облікові записи користувачів та адміністраторів повинні бути суто особистими
- L2.7: Облікові записи користувачів не повинні мати прямого доступу до базових компонентів
- L2.8: Облікові записи користувачів та адміністраторів і права доступу повинні періодично оцінюватися, а знахідки повинні відстежуватися

Компонент безпеки

- L3.1: Розуміння додатків та базових компонентів повинно бути актуальним
- L3.2: Повинні автоматично генеруватися сповіщення про нові вразливі сторони, а системи повинні періодично перевірятися
- L3.3: Системи повинні оперативно виправлятися та оновлюватися
- L3.4: Системи не повинні використовувати стандартні паролі або облікові записи бекдорів
- L3.5: Операційна система не повинна запускати непотрібні служби
- L3.6: Внутрішня мережа повинна бути ізольована від ненадійних середовищ
- L3.7: Мережевий трафік та компоненти повинні активно контролюватися

Резервне копіювання та відновлення

- O1.1: Періодичність резервного копіювання та тип резервної копії повинні відповідати системам, що є критично важливими для річної звітності.
- O1.2: Резервні копії даних повинні зберігатися у безпечному місці, де забезпечується їх цілісність.
- O1.3: Необхідно періодично тестувати можливість відновлення резервної копії.

Виправлення даних

- D1.1: Клієнт та сервісні організації домовилися про контрольоване виконання виправлень даних
- D1.2: Виправлення даних тестуються в середовищі, відмінному від виробничого, а сценарії виправлень даних переглядаються.
- D1.3: Виправлення даних реєструються таким чином, щоб згодом можна було визначити, що виправлення даних були виконані правильно
- D1.4: Затвердження та виконання виправлень даних здійснюється різними працівниками, а остаточне схвалення надається клієнтом
- D1.5: Існує періодична перевірка на наявність несанкціонованих виправлень даних

Кількість тестів

Частота заходів контролю	Кількість тестів
Раз на рік	1
Раз на квартал	2
Раз на місяць	3
Раз на тиждень	5
Раз на день	25

Переваги заходів контролю прикладних програм

- **Надійність**

  Зменшує ймовірність помилок через ручне втручання

  Заощадження часу і коштів

  ›Як правило, перевірка заходів контролю прикладних програм займає менше часу і вимагає тестування лише один раз, якщо загальні заходи IT-контролю є ефективними

- **Порівняльний аналіз**

  ›Покладання на загальні заходи IT-контролю може призвести до висновку, що заходи контролю прикладних програм є ефективними з року в рік без повторного тестування