Central Government Audit Service
Ministry of Finance

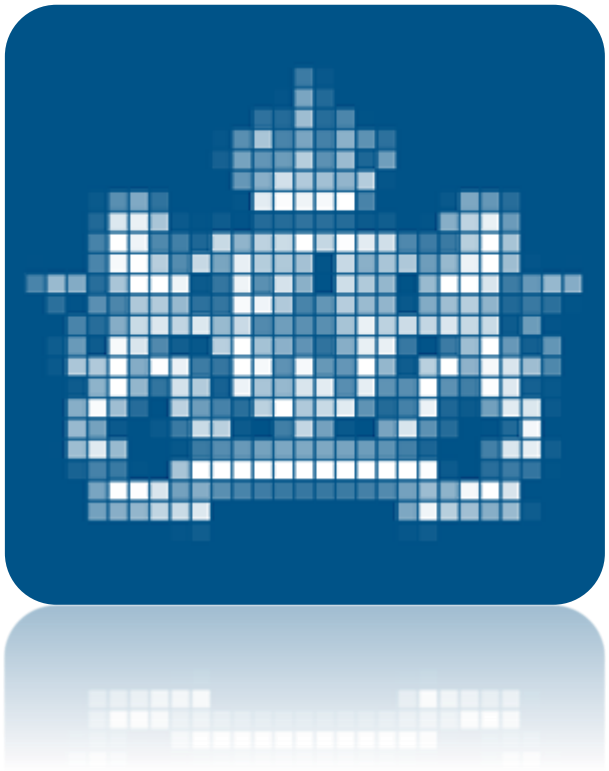
Тренінг з аудиту інформаційних технологій

День 2

Рурдьє Просе
Лодевік Янсен

Auditdienst Rijk
Ministerie van Financiën

Central Government Audit Service
Ministry of Finance



Зміст

- Рамкові основи (продовження)
- Робота на місці
- Оцінка/аналіз
- Звітування про знахідки
- Розвиток в IT

Робота на місці

Кейс (збір даних)

- Яким був би ваш аудиторський підхід?
- Які методи збору даних ви б використали (і не використали)?
- Чому?

1. Управління виправленнями
2. Безпека мобільних застосунків
3. Зрілість програми обізнаності
4. Управління і контроль

Збір даних

На основі дизайну дослідження виберіть, які методи збору даних ви будете використовувати:

Набір інструментів (IT) аудитора:

- Камеральне дослідження
- Інтерв'ю
- Спостереження
- Семінар
- Огляди (напр.: Limesurvey)
- Механічна обробка (SSL, тощо)
- Тестування в ході виконання
- Аналіз даних
- Тощо…

Документація дизайну

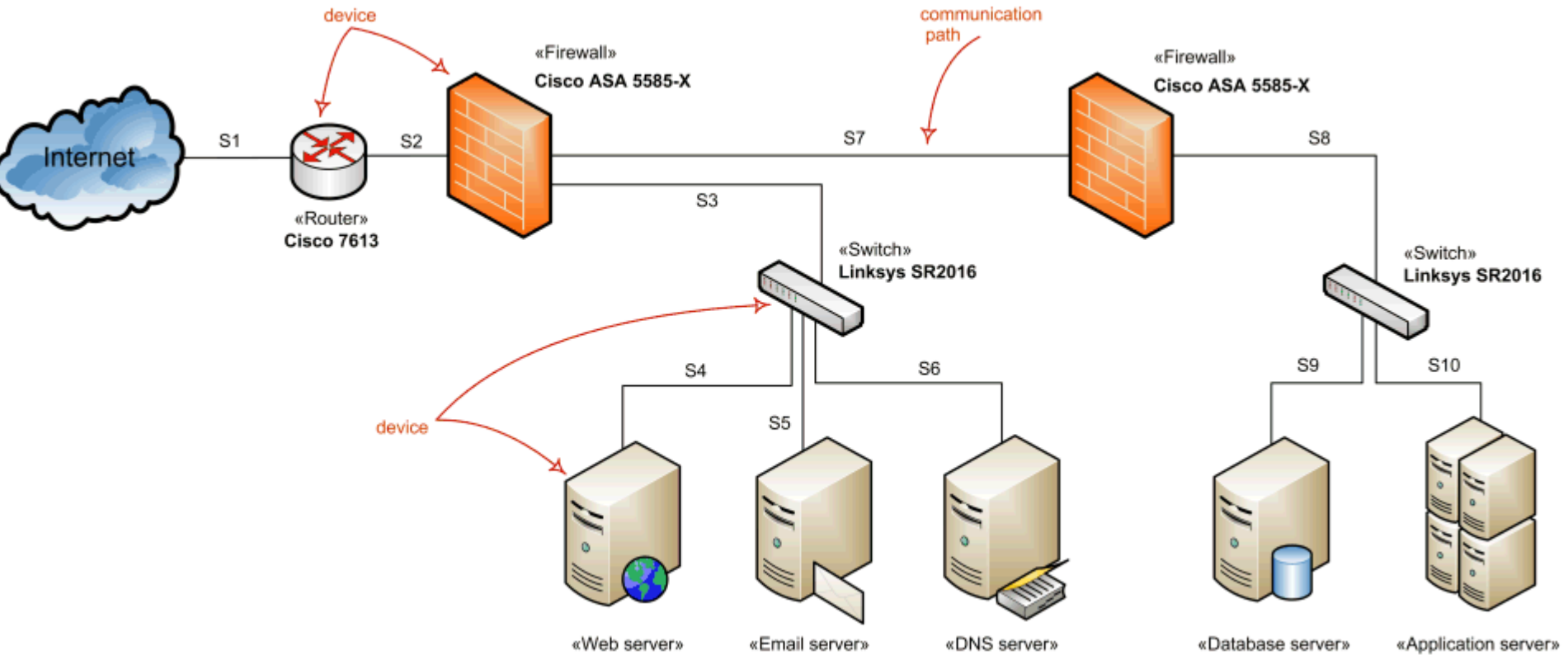
- Мапа мережевої інфраструктури
- Технічний дизайн
- Функціональний дизайн
- Документ з ініціювання проекту
- Документи архітектури
- Процедури
- Вказівки щодо загартування
- Угоди/звіти про рівень обслуговування
- Організаційна схема

Документи дизайну

- Функціональна, з використанням кейсів архітектура -> Що слід зробити?
- Технічна для рішень архітектура -> Як це запроваджується?

Мета: зрозуміти систему, доповнюйте інтерв'ю за потреби

Мапа мережевої інфраструктури



Документація з операційної результативності

- *Файли конфігурації*
- Записи журналу
- Скріншоти
- Налаштування
- Результати механічної обробки
- Результати тестування
- Інспектування доказів (напр., управління змінами)
- Відповідність (повторне виконання)

Підготовлений замовником список

- Список необхідних документів для аудиту
- Іноді такий самий, як минулого року, іноді конкретизується під час прийняття завдання

Спостереження

- Налаштування
- Переконайтеся, що ви дивитеся на правильне середовище (огляд), сервер, та ін.

Кількість тестів

Частота заходів контролю	**Кількість тестів**
Щорічний	1
Щоквартальний	2
Щомісячний	3
Щотижневий	5
Щоденний	25

Ключові загальні IT-заходи контролю

Ключові загальні IT-заходи контролю

1. **Управління змінами**
2. Управління паролями
3. **Управління доступом**
4. Компонент безпеки
5. Резервне копіювання і відновлення

Завдання

1. **Причини для тестування ключових загальних IT-заходів контролю?**

2. **Які ризики пов'язані з цими заходами контролю?**

Ризики використання IT

- Довіра до систем чи програм, які неточно опрацьовують дані, опрацьовують неточні дані, чи і те, і інше
- Неавторизований доступ (безпека/привілеї)
- Неавторизовані зміни (дані/системи/програми)
- Неналежне ручне втручання
- Потенційна втрата даних чи нездатність отримати доступ до даних, як необхідно

Рамкова основа загальних IT-заходів контролю

- На основі найкращих практик / ISO27001/2

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

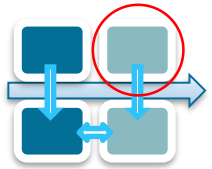
Microsoft Excel-werkblad

Управління доступом —Механізми контролю безпеки

<u>Ціль</u>: Визначити, що логічний і фізичний доступ до IT комп'ютерних ресурсів належним чином обмежений авторизованими та уповноваженими користувачами

<u>Ризики виникають з:</u>

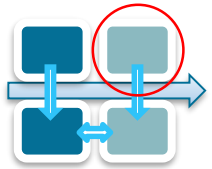
- Автентифікації (як користувачі ідентифікують себе)
- Налаштування безпеки (як IT-середовище обмежує доступ)
- Управління правами доступу



Управління доступом — Визначити ризик

Міркування

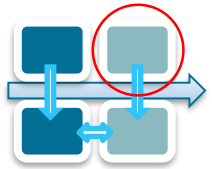
- Кількість користувачів
- Складність прав
- Простота розуміння прав доступу
- Централізація управління доступом
- Використання ролей/профілі користувачів
- Частота плинності кадрів



Управління доступом —Механізми контролю безпеки

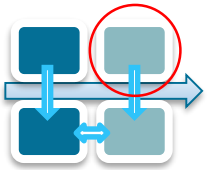
Ключові елементи контролю та тестування міркувань:

- Доступ до комп'ютерного забезпечення фізично захищений та обмежений авторизованими особами.
- Унікальні дані ідентифікації користувачів використовуються для забезпечення індивідуальної підзвітності
- Вимоги щодо надійних та складних паролів
- Ефективні механізми входу та заходи з управлінського огляду запроваджено



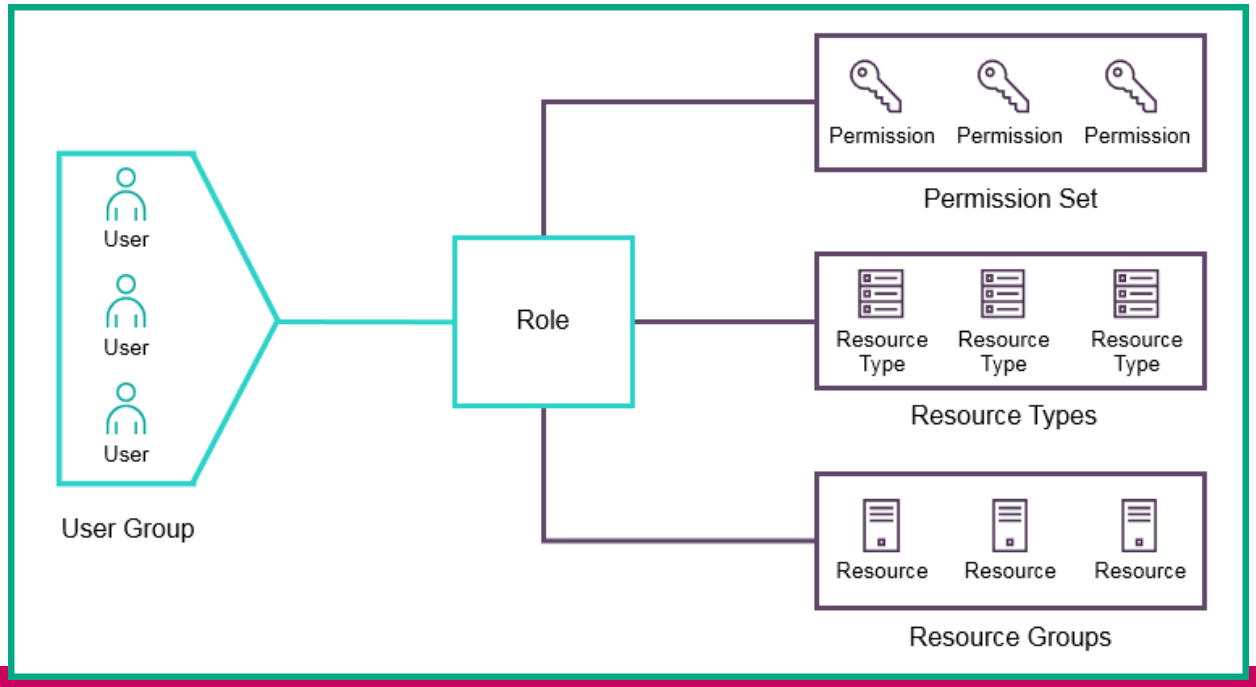
Управління доступом – Заходи контролю щодо користувача

1. Користувачі та адміністратори повинні мати тільки ті права доступу, які необхідні їм для роботи
2. Облікові записи та права доступу користувачів повинні бути авторизованими
3. Розподіл обов'язків повинен бути запровадженим для застосування, схвалення та запровадження змін в облікових записах користувачів та правах доступу
4. Має швидко опрацьовуватися звільнення персоналу
5. Облікові записи адміністраторів мають бути обмеженими і поясненими
6. Облікові записи користувачів та адміністраторів мають бути суворо особистими.
7. Облікові записи користувачів повинні не мати прямого доступу до основоположних компонентів.
8. Облікові записи та права доступу користувачів та адміністраторів повинні періодично оцінюватися і відстежуватися



Управління доступом - Запровадження (I)

- Процедури з надання доступу
- Періодична оцінка прав
- Контроль доступу відповідно до ролі



Управління доступом – Запровадження (II)

- Матриця контролю доступу

Діяльність	Адміністратор	Наглядач	Керівник
Створити обліковий запис користувача	X		
Видалити обліковий запис користувача	X		
Схвалити обліковий запис користувача		X	
Переглянути журнал			X

Користувач	Роль
Лодевік	Адміністратор
Рурдьє	Керівник
..	..

Управління доступом – Запровадження(III)

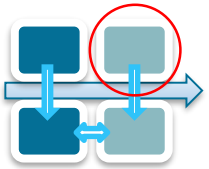
- **Активна директорія (каталог)**
  - Управління користувачами
  - Автентифікація та авторизація
  - Правила щодо паролів

Управління змінами – Авторизовані зміни відповідні процедури

<u>Ціль</u>: Визначити, що контрольні заходи запроваджено, щоб гарантувати належну авторизацію змін у системах/прикладних програмах відповідним рівнем керівництва.

<u>Ключові елементи контролю та ідеї для тестування</u>:

- Організація запровадила формальний процес управління змінами.
- Усі запити на зміни у системах/прикладних програмах формально документуються
- Аудиторський слід змін можна відстежити і співвіднести до первинних запитів



Управління змінами – Тестування змін програми

- **<u>Ціль</u>:** визначити, що контрольні заходи запроваджено, щоб гарантувати тестування, підтвердження і схвалення змін до прикладних програм і систем до запуску у виробництво.

<u>Ключові елементи контролю та ідеї для тестування</u>:

- Запроваджено окреме від виробництва середовище тестування
- Тільки обмежена кількість осіб повинна вносити зміни у виробництво.

Управління змінами - критерії

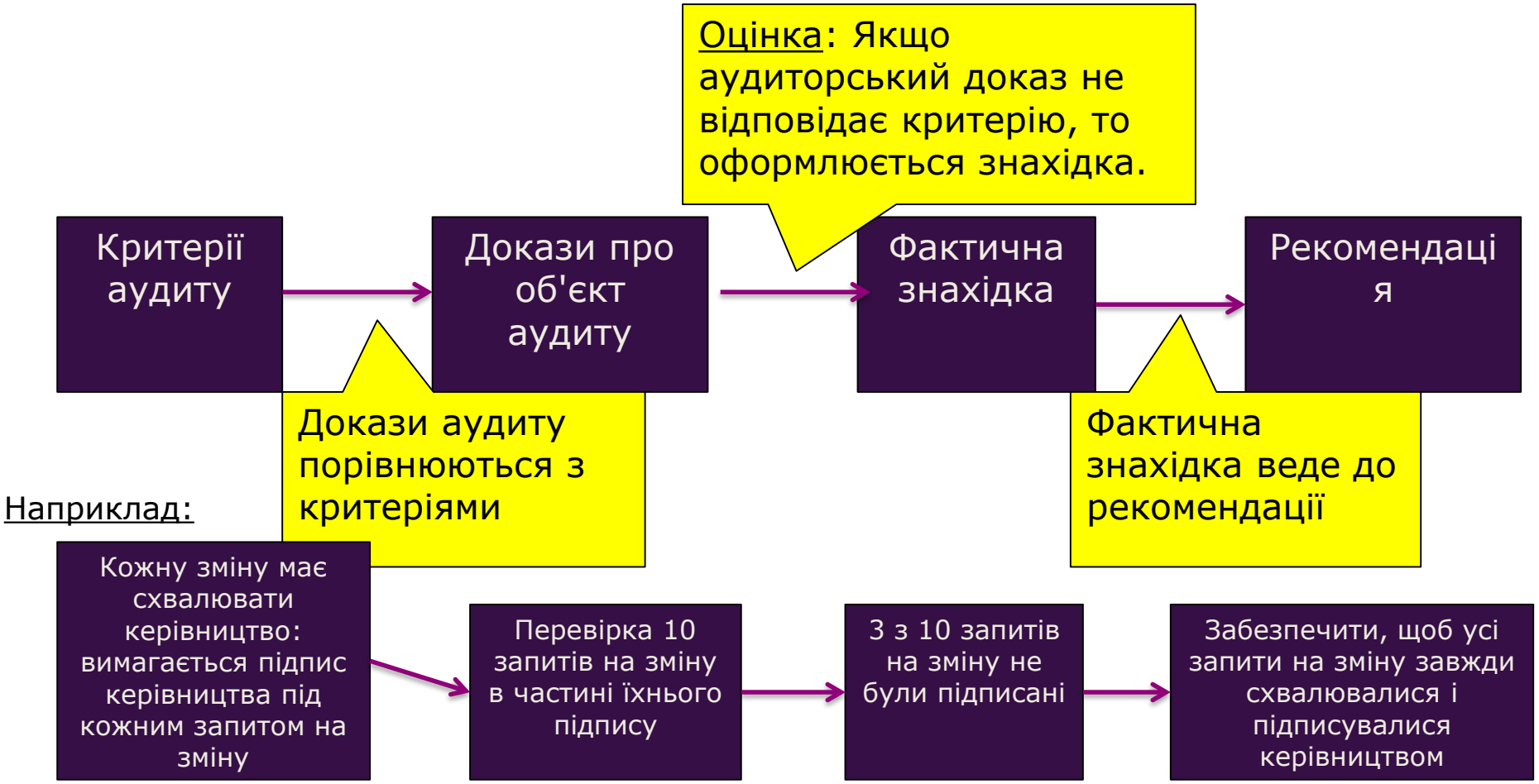
1. Зміни повинні бути авторизовані
2. Зміни повинні бути протестовані
3. Зміни повинні бути схвалені за результатами тестування
4. Обов'язки із застосування, схвалення та запровадження змін повинні бути розділені
5. Неавторизовані зміни повинні періодично перевірятися

Управління змінами - запровадження

Який у Вас досвід з управління змінами?

Оцінка і аналіз

Інтерпретація і оцінка знахідок (I)



DigiD оцінки

- Урядовий логін для веб-сайтів
- Оцінка веб-застосунку
- 20 критеріїв: гарантії в розрізі критеріїв, а не в цілому
- На основі ризиків

Оцінка: управління виправленнями

Управління виправленнями – це запроваджений процедурний процес, який підтримується вказівками, таким чином, щоб найновіші (безпекові) виправлення своєчасно вносилися в засоби ІКТ.

- Своєчасне управління виправленнями
- Немає процедури

- **Який ризик? Добре чи не добре?**

Оцінка: управління вразливістю

Оцінки вразливості (сканування безпеки) проводяться на основі процедурного процесу щодо компонентів ІКТ веб-застосунку (обсяг).

- Оцінка в контракті
- Оцінка проводиться щомісяця хостером
- Організація щомісяця отримує звіт, більшість часу тільки знахідки про низький ризик
- Організація не оцінює звіт

- **Який ризик? Добре чи не добре?**

Звітування

Запишіть знахідки в аудиторський звіт

Три основні види звітів:

- Звіт з надання гарантій
- Звіт про фактичні знахідки
- Дорадчий звіт

Представлення та обговорення знахідок із замовником

- Технічні IT знахідки і рекомендації повинні бути чіткими та повними, також для керівника чи власника процесу.
- Подбайте про те, щоб замовник зрозумів знахідки та рекомендації та знав, як пом'якшити (технічні) ризики.
- Попросіть реакцію керівництва на ваш звіт.
- Переконайте замовника у необхідності виділення часу та бюджету для відстеження знахідок та впровадження рекомендацій
- Якщо є знахідки із дуже високим ступенем ризику, то пропонуйте терміни реалізації знахідок.

Звітування знахідок

- На основі ризику (ймовірність та вплив)
- Звітувати керівництву (не занадто технічно / який ризик)
- Вплив на аудит про фінансовий звіт

Підготовка рекомендацій

- Говоріть із замовником (що важливо?)
- Знайте зрілість організації
- Обговоріть всередині команди
- Знайдіть головну причину

Приклади звітування

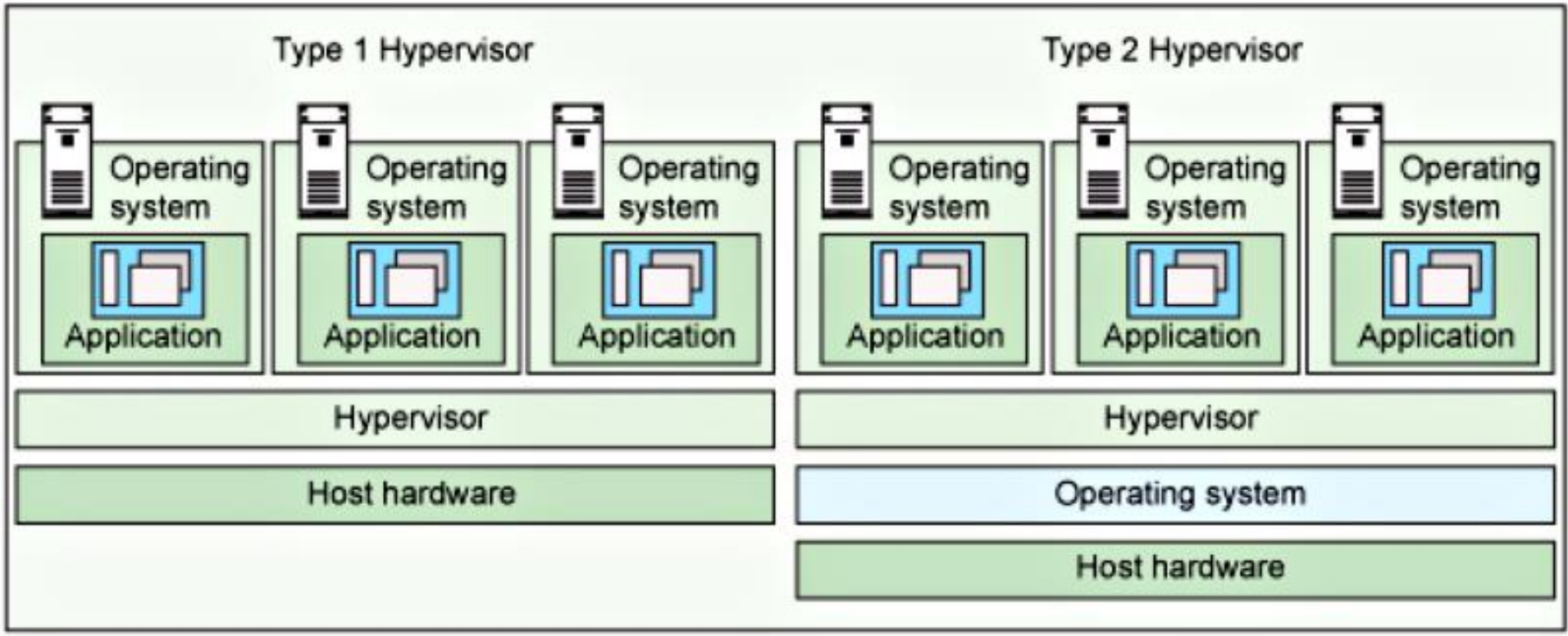
- Схема піраміди
- Більшість звітів можна знайти онлайн: online

Хмаринка / віртуалізація

Віртуалізація

Що таке віртуалізація?

https://www.youtube.com/watch?v=GeXwR32GCOw



Хмаринкові технології

Що таке хмаринкові технології:

- Використання послуг з хостингу на інфраструктурі третьої сторони

•Приклади: Webmail, Office 365, Amazon AWS, Azure

• Основоположна хмаринкова інфраструктура така, як мережа, сервери, операційні системи, збереження чи навіть застосунки контролюються і управляються третьою стороною

• Використовує технології віртуалізації та оркестрації для автоматизованого залучення нових серверів, тощо.

Піца як послуга

Традиційна на місці	Інфраструктура як послуга	Платформа як послуга	Програмне забезпечення як послуга
Обідній стіл	Обідній стіл	Обідній стіл	Обідній стіл
Содова	Содова	Содова	Содова
Електрика/газ	Електрика/газ	Електрика/газ	Електрика/газ
Піч	Піч	Піч	Піч
Вогонь	Вогонь	Вогонь	Вогонь
Тісто для піци	Тісто для піци	Тісто для піци	Тісто для піци
Томатний соус	Томатний соус	Томатний соус	Томатний соус
Добавки	Добавки	Добавки	Добавки
Сир	Сир	Сир	Сир
зроблена вдома	напівфабрикат	доставлена піца	вечеря не вдома

Ви управляєте

Продавець управляє

IT підприємства	Інфраструктура	Платформа	Програмне забезпечення
(спадкове IT)	(як послуга)	(як послуга)	(як послуга)
Застосунки	Застосунки	Застосунки	Застосунки
Безпека	Безпека	Безпека	Безпека
Бази даних	Бази даних	Бази даних	Бази даних
Операційні системи	Операційні системи	Операційні системи	Операційні системи
Віртуалізація	Віртуалізація	Віртуалізація	Віртуалізація
Сервери	Сервери	Сервери	Сервери
Місце для збереження	Місце для збереження	Місце для збереження	Місце для збереження
Мережа	Мережа	Мережа	Мережа
Центри даних	Центри даних	Центри даних	Центри даних
	Управляється замовником		Управляється провайдером

Хмаринкові технології

Переваги:

- Швидке і широке застосування / простота реалізації
- Менше власної інфраструктури
- Масштабованість
- Простота оновлення
- Гнучкість
- Низькі затрати
- Простота використання

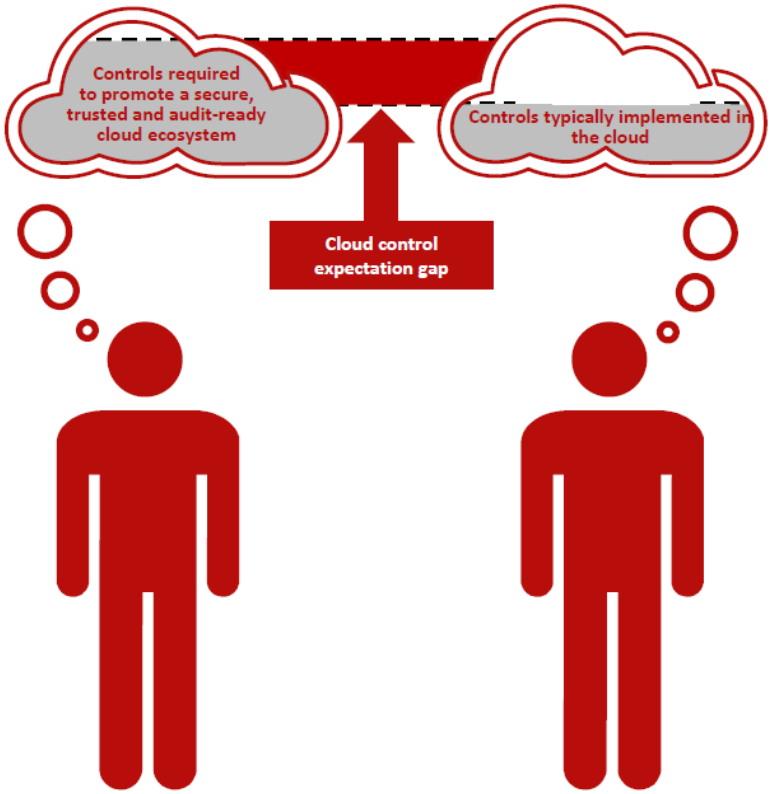
Ризики:

- Безпека даних/конфіденційність
- Відповідність
- Інтеграція з існуючими застосунками / системами
- Управління третьою стороною
- Репутація хмаринкового провайдера

Розрив очікувань щодо хмаринкового контролю

Багато організацій використовують хмаринкові технології

- Клієнти очікують, що постачальники хмаринкових технологій впровадили всі заходи контролю, щоб гарантувати конфіденційність, цілісність, доступність своїх даних
- Насправді: ми бачимо повільніше прийняття необхідних заходів контролю, що здійснюються меншими темпами
- Прогалина між очікуваними заходами контролю та типово запровадженими заходами контролю дедалі більше зростає
- Це ризик для клієнтів хмаринкових технологій



ЗГЗД

Дуже коротке представлення

Загальний регламент захисту даних

- Персональні дані
- Великі штрафи (10 мільйонів євро)
- Знати, що маєте
- Захищати

Знати, що маєте

- Документувати заходи з обробки даних
- Управляти даними структурованим способом
- Хто відповідальний? (контролер/обробник даних)
- Що треба знати: управління доступом (знову ☺)

Обмеження мети

- Ви повинні чітко знати, яка **мета** обробки даних від початку (і записати її)

- Ви повинні забезпечити, щоб персональні дані, які ви опрацьовуєте, були:
  - адекватними – достатніми для належного виконання заявленої мети;
  - доречними – з раціональним зв'язком до мети;
  - обмеженими тільки тими, що необхідні – ви не зберігаєте більше, ніж потрібно до цієї мети (мінімалізація даних)

Захист даних

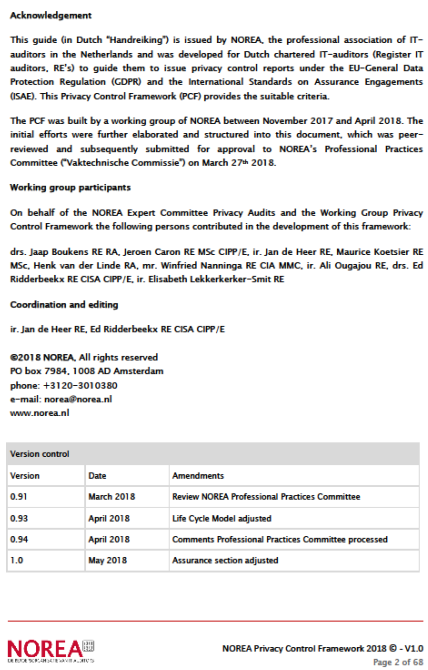
- Запровадження належних технічних та організаційних заходів
- Правила захисту даних
- Укладати контракти з компаніями, які обробляють дані для вас

- Заходи безпеки (шифрування)

Рамкова основа контролю за конфіденційністю

Цілі контролю та заходи контролю для аудитів конфіденційності та завдань з надання гарантій щодо конфіденційності

Професійна асоціація IT-аудиторів у Нідерландах



Acknowledgement

This guide (in Dutch "Handreiking") is issued by NOREA, the professional association of IT-auditors in the Netherlands and was developed for Dutch chartered IT-auditors (Register IT auditors, RE's) to guide them to issue privacy control reports under the EU-General Data Protection Regulation (GDPR) and the International Standards on Assurance Engagements (ISAE). This Privacy Control Framework (PCF) provides the suitable criteria.

The PCF was built by a working group of NOREA between November 2017 and April 2018. The initial efforts were further elaborated and structured into this document, which was peer-reviewed and subsequently submitted for approval to NOREA's Professional Practices Committee ("Vaktechnische Commissie") on March 27th 2018.

Working group participants

On behalf of the NOREA Expert Committee Privacy Audits and the Working Group Privacy Control Framework the following persons contributed in the development of this framework:

drs. Jaap Boukens RE RA, Jeroen Caron RE MSc CIPP/E, ir. Jan de Heer RE, Maurice Koetsier RE MSc, Henk van der Linde RA, mr. Winfried Nanninga RE CIA MMC, ir. Ali Ougajou RE, drs. Ed Ridderbeekx RE CISA CIPP/E, ir. Elisabeth Lekkerkerker-Smit RE

Coordination and editing

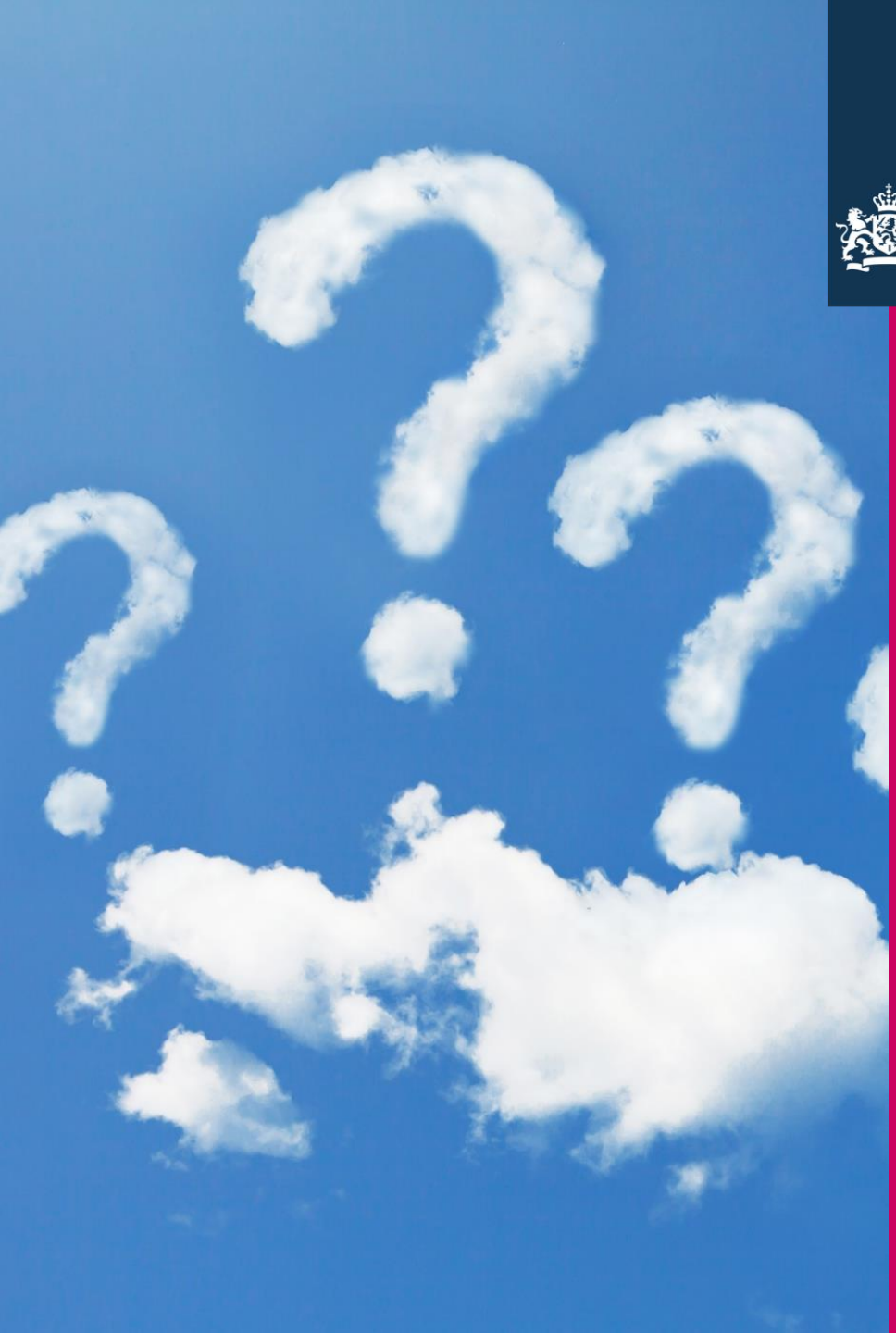
ir. Jan de Heer RE, Ed Ridderbeekx RE CISA CIPP/E

PO box 7984, 1008 AD Amsterdam
phone: +3120-3010380
e-mail: norea@norea.nl
www.norea.nl

Version control		
Version	Date	Amendments
0.91	March 2018	Review NOREA Professional Practices Committee
0.93	April 2018	Life Cycle Model adjusted
0.94	April 2018	Comments Professional Practices Committee processed
1.0	May 2018	Assurance section adjusted

Підбиття підсумків і замірювання настрою

Яким був Ваш день?



Central Government Audit Service
Ministry of Finance

Запитання?

Дякуємо за увагу!