Central Government Audit Service
Ministry of Finance

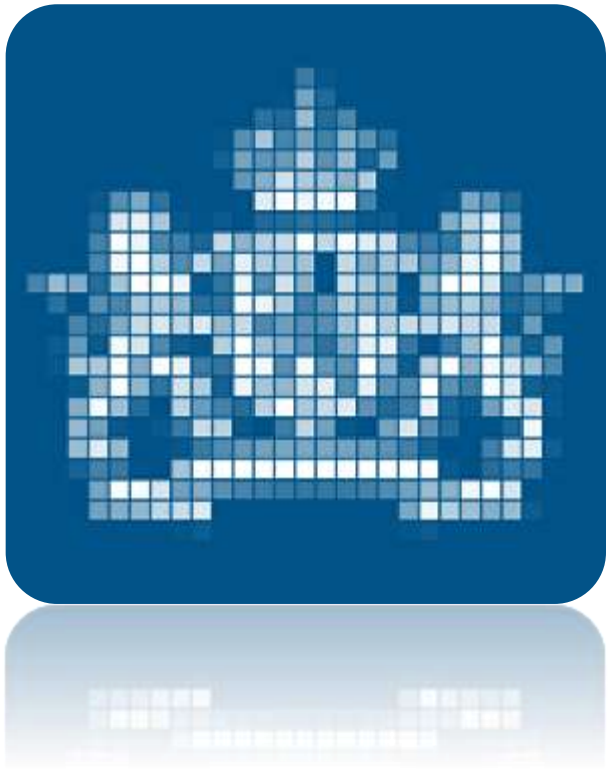
Тренінг з аудиту інформаційних технологій

Сесія 2

Маартен ван дер Ліппе

Люсінда Лунсхоф

Central Government Audit Service
Ministry of Finance



Contents

ЗМІСТ

- Підсумок попередньої сесії
- Покрокове проходження IT-аудиту

Сесія 1

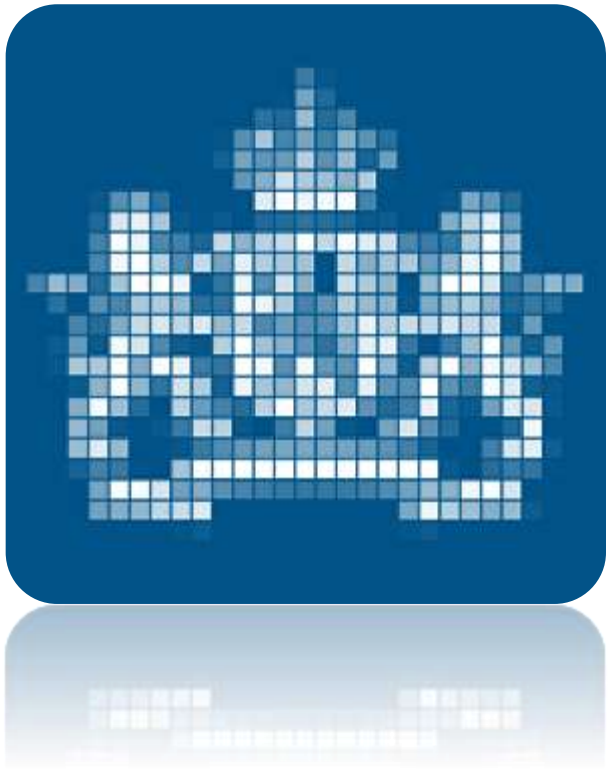
- Центральна урядова служба аудиту

- Вступ до IT-аудиту
  - Що таке IT-аудит?
  - Хто такий IT-аудитор?
  - Аспекти якості
  - Об’єкти IT-аудиту
  - Етапи IT-аудиту

ADR – Рамкова основа 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

Central Government Audit Service
Ministry of Finance

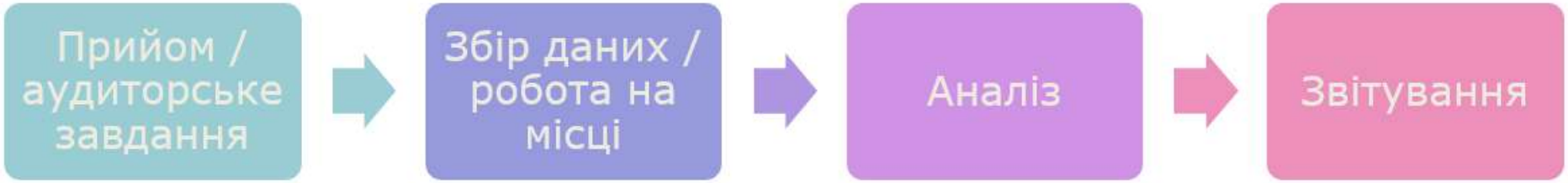


Contents

ЗМІСТ

Покрокове проходження IT-аудиту

Покрокові етапи



Прийом

- *Кроки на цьому етапі:*
  - *Прийом – що ви обговорюєте?*
  - *Схвалення завдання - ким?*
- *Підтвердження завдання*

- Що у ньому? З ким узгоджується?

Приклад змісту

Вступ

1.1 Обгрунтування

1.2 Контекст

2 Завдання з надання гарантій

2.1 Клієнт і аудитор

2.2 Мета та істотність

2.3 Об’єкт дослідження, обмеження та визначення

2.4 Критерії

2.5 Звітування

3 Виконання завдання

3.1 Планування і операції

3.2 Склад команди

3.3 Узгодження з клієнтом

4 Підпис

5 Додаток (додатки)

Робота на місці

- Документи, підготовлені клієнтом
- Інтерв’ю
- Документування
- Робота на місці
- Приклади з практики

Документи, підготовлені клієнтом

Back-up & recovery

Categorie	Beheersdoelstelling	Norm ID	Norm Naam	Beheersmaatregel	Verzoek ID	Documentatieverzoek	Populatie (P) / Samples (S) / Veldwerk (V) Evidence	Status	Datum verzoek	Datum aanlevering	Opmerking ADR	Opmerking IT dienstverlener
O1. Overig : back-up &recovery	D.m.v. Back-up & recovery wordt de integriteit van informatie en IT voorzieningen gehandhaafd (BIR 10.5)	O1.1	De periodiciteit van, en het type gegevens op, de back-up sluiten aan bij het belang van de voor de jaarrekening kritische systemen.	De periodiciteit van de back-up dient aan te sluiten bij de maximaal toegestane periode waarover gegevens verloren mogen raken. Stel vast dat de back-up de juiste systemen en data bestanden omvat die relevant zijn voor de jaarrekening.	O1.1.1	Meest recente SLA tussen klant(en) m.b.t. informatiesysteem en dienstverlener waarin de back-up / recovery eisen zijn opgenomen. Denk hierbij o.a. aan: planning, periodiciteit back-up, wijze van back-up, bewaren back-up (locatie), vernietiging van back-ups, terugzetten van back-ups en testen ervan, verslaglegging back-ups en recovery, afspraken met klant etc.	V	Open				
					O1.1.2	Technisch ontwerp (TO) infrastructuur van (applicatie)landschap waaruit is af te leiden welke servers zijn ingezet. Afspraken tussen systeemeigenaar en eventuele IT-dienstverlener waarin een duidelijke beschrijving van de IT-infrastructuur en het applicatielandschap zijn opgenomen.	V	Open				
		O1.2	De back-up gegevens worden op een veilige locatie bewaard waarbij de integriteit van de back-up geborgd blijft.	Stel vast, nadat in O1.1 is bepaald dat de back-up tijdig en volledig tot stand is gekomen, op welke wijze de back-up wordt opgeslagen. Stel vast dat de opgeslagen back-up beveiligd is tegen onbevoegde wijzigingen en op dusdanige afstand van de bron is opgeslagen dat een mogelijke calamiteit bij de bron geen effect heeft op de back-up.	O1.2.1	Aantoonbare evidence waaruit het waarborgen van integere back-up blijkt, zoals periodieke rapportages vanuit technisch beheer richting de systeemeigenaar. Opm.: denk hierbij o.a. aan KPI's als versleutelde verbindingen tussen back-up server en clients, versleutelde tape drives, logische- en fysieke toegang tot back-up omgeving.	V	Open				
					O1.2.2	Periodieke rapportages vanuit technisch beheer richting de systeemeigenaar over het opslaan van back-ups op een externe locatie, waaruit de wijze van opslag, vernietiging, beveiliging (en hoe deze gemonitord wordt) blijkt.	V	Open				
		O1.3	Het kunnen terugzetten van de back-up (recovery) wordt periodiek getest.	Om te bepalen of back-ups ook correct kunnen worden teruggezet is het van belang te bepalen of de recovery procedure betrouwbaar heeft gefunctioneerd. Dit dient minimaal jaarlijks te worden getest.	O1.3.1	Recovery procedurebeschrijving.	V	Open				
					O1.3.2	Opdracht binnen het controlejaar van de systeemeigenaar voor het terugzetten van data (database) van externe locatie voor Oracle Database.	S	Open				
					O1.3.3	Testverslag van uitgevoerde recovery-opdracht (zie documentatieverzoek #O1.3.2), inclusief datumaanduiding. Indien voor Oracle Database geen recovery heeft plaatsgevonden dan een generiek voorbeeld van een recoverytest aanreiken.	S	Open				

Інтерв’ю

- З ким ви проводитимете інтерв’ю?
- Кого ви візьмете з собою?
- Як ви підготуєтеся до інтерв’ю?
- Що робити після інтерв’ю?

Документування

- Що ви запишете у свій файл?

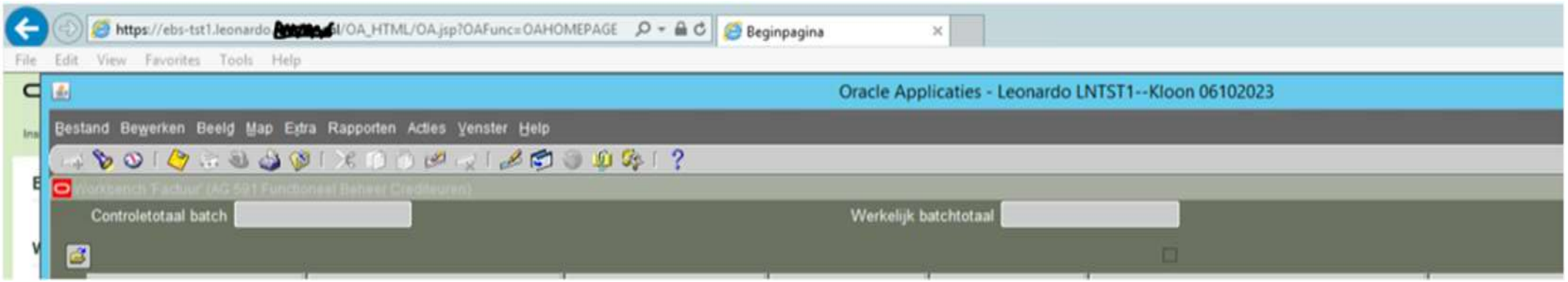
Робота на місці

- Використовуйте шаблон
- Робіть посилання на використані документи

Werkstappen per Norm	
D1.1: Klantorganisatie en serviceorganisatie hebben afspraken over het beheerst uitvoeren van datafixes	
Toelichting	**Details: datafixes dienen te worden behandeld als wijzigingen. Klant- en serviceorganisatie hebben de afspraken over het beheerst doorvoeren van datafixes vastgelegd in een proces analoog aan het wijzigingsproces.**
	Beheersdoelstelling(en) / control(s): BIO 12.1.2.1
	Sample based norm (systeemtests): nee
	Hoe te onderzoeken: Stel vast dat de klant-organisatie afspraken heeft gemaakt met de service-organisatie over de onderlinge rolverdeling, de administratie van datafixes, de risico-afweging, testen, goedkeuring van datafixes en vastlegging daarvan, logging van datafixes, bewaartermijn van de logging, controle van de logging.
Werkzaamheden	
opzet / bestaan	Bevindingen:
	Te evalueren
	Motivatie voor score:
werking	Bevindingen:
	Te evalueren
	Motivatie voor score:

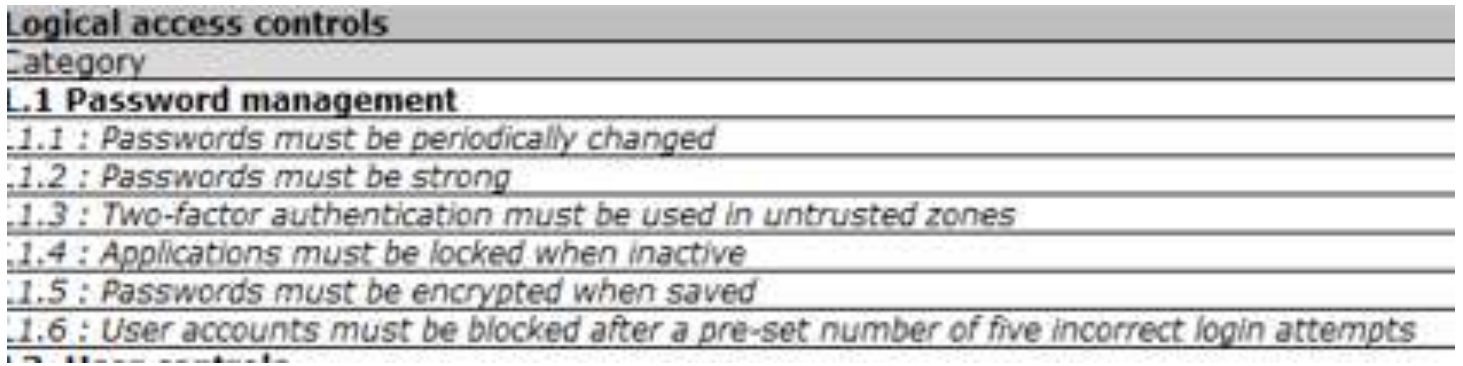
Управління змінами

- З чого розпочнете?
- Які документи ви запросите?
- Як ви можете перевіряти неавторизовані зміни?



Управління паролями

Мінімальний вік (дні)	1
Максимальний вік (дні)	365
Історія паролю (кількість)	10
Мінімальна довжина (символи)	12
Складність	Можлива
Шифрування	Активне
Максимум спроб	10
Час для заблокування (хв)	0



Logical access controls
Category
L.1 Password management
.1.1 : Passwords must be periodically changed
.1.2 : Passwords must be strong
.1.3 : Two-factor authentication must be used in untrusted zones
.1.4 : Applications must be locked when inactive
.1.5 : Passwords must be encrypted when saved
.1.6 : User accounts must be blocked after a pre-set number of five incorrect login attempts

Управління паролями

Мінімальний вік (дні)	1	L1.1: Паролі повинні періодично змінюватися
Максимальний вік (дні)	365	L1.1: Паролі повинні періодично змінюватися
Історія паролю (кількість)	10	L1.1: Паролі повинні періодично змінюватися
Мінімальна довжина (символи)	12	L1.2: Паролі повинні бути надійними
Складність	Можлива	L1.2: Паролі повинні бути надійними
Шифрування	Активне	L1.5: Паролі повинні шифруватися при збереженні
Максимум спроб	10	L1.6: Облікові записи користувачів повинні бути заблоковані після десяти неправильних спроб входу
Час для заблокування (хв)	0	L1.6: Облікові записи користувачів повинні бути заблоковані після десяти неправильних спроб входу

Що ви би обрали?

Приклад політики домену за замовчуванням 2024	
Мінімальний вік (дні)	0
Максимальний вік (дні)	450
Історія паролю (кількість)	6
Мінімальна довжина (символи)	8
Складність	Можлива
Шифрування	Вимкнене
Максимум спроб	5
Час для заблокування (хв)	0

Дрібнозернистий приклад 1 2024	
Мінімальний вік (дні)	1
Максимальний вік (дні)	42
Історія паролю (кількість)	24
Мінімальна довжина (символи)	16
Складність	Можлива
Шифрування	Активне
Максимум спроб	10
Час для заблокування (хв)	0

Управління паролями

Дайте відповідь на наступні запитання:

1. Чи достатні вимоги до паролів?
2. Хто з користувачів має пароль старіший за 1 січня 2023 року?
3. Чому мінімальний вік 1 день?
4. Навіщо потрібна історія паролів?
5. Чому поєднання мінімального віку та історії паролів є сильним?
6. Що ще, на вашу думку, є важливим?

Заходи контролю щодо користувачів

Дайте відповідь на наступні питання:

1. Скільки облікових записів на сервері?
2. Які користувачі ніколи не входили в систему?
3. Які користувачі входили в систему до 2023 року?
4. А в 2023 році?
5. Які облікові записи є обліковими записами адміністратора?
6. З'ясуйте це для *testuser 31:*

- Останній раз, коли обліковий запис було змінено
- Останній раз, коли обліковий запис входив в систему
- Останній раз, коли змінювався пароль

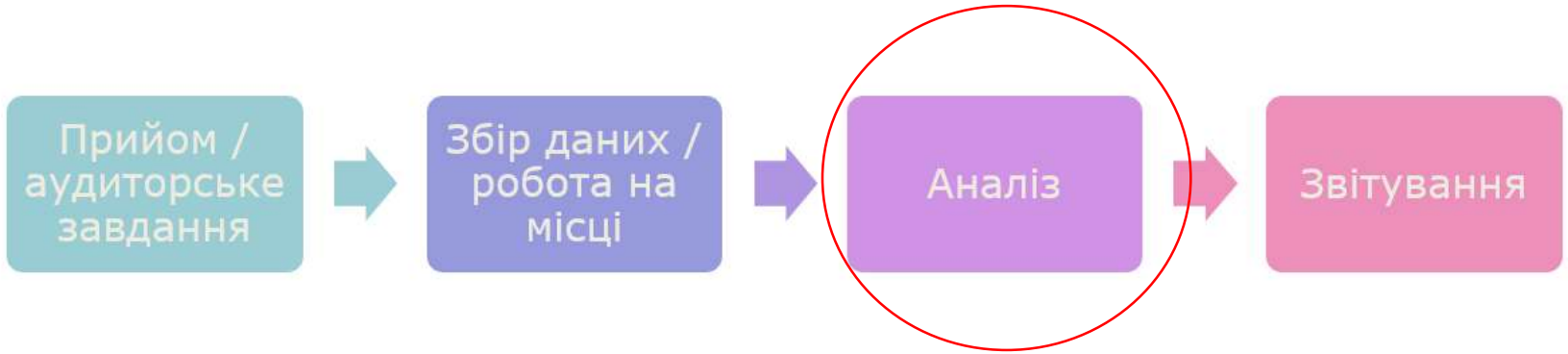
7. Скільки користувачів змінили свій пароль у 2023 році?

Резервне копіювання і відновлення

- Це ефективно чи ні?
- І чому?

Backup	Oracle8 ODC-UX-SV2000057-ORA-ar-LNBITST	Completed	full	3-3-2023 05:10:08	0:00	1:19	50,57	2	0	0	1	2023/03/03-12
Backup	Oracle8 ODC-UX-SV2000033-ORA-ar-EMAWRPRD	Completed	full	3-3-2023 05:10:08	0:00	0:00	0,51	1	0	0	1	2023/03/03-13
Backup	Oracle8 ODC-UX-sv2000034-ORA-ar-LNNTSPRD2	Completed	full	3-3-2023 05:10:08	0:00	0:01	0,18	1	0	0	1	2023/03/03-14
Backup	Oracle8 ODC-UX-SV2000033-ORA-ar-LNNTSPRD1	Completed	full	3-3-2023 05:15:01	0:00	0:01	7,41	1	0	0	1	2023/03/03-16
Backup	Oracle8 ODC-UX-ebsdb_prd-ORA-ar-LNCPRD	Failed	full	3-3-2023 07:26:52	0:00	0:01	0,00	1	8	0	0	2023/03/03-21
Backup	Oracle8 ODC-UX-ebsdb_prd-ORA-ar-LNCPRD	Completed	full	3-3-2023 07:28:39	0:00	0:01	13,40	1	0	0	0	2023/03/03-22
Backup	Oracle8 ODC-UX-bidb_prd-ORA-ar-LNBIPRD	Completed	full	3-3-2023 07:46:11	0:00	0:29	96,64	1	0	0	1	2023/03/03-25
Backup	Oracle8 KVH-UX-bidb_acc-ORA-ar-LNBIACC	Completed	full	3-3-2023 12:10:00	0:00	0:00	0,50	1	0	0	1	2023/03/03-29
Backup	Oracle8 KVH-UX-ebsdb_acc-ORA-ar-LNCACC	Completed	full	3-3-2023 12:10:00	0:00	0:00	0,70	1	0	0	1	2023/03/03-30
Backup	Oracle8 ODC-UX-SV2000033-ORA-ar-EMAWRPRD	Completed	full	3-3-2023 12:10:01	0:00	0:00	0,44	1	0	0	1	2023/03/03-32
Backup	Oracle8 ODC-UX-SV2000057-ORA-ar-LNBITST	Completed	full	3-3-2023 12:10:01	0:00	1:04	64,82	1	0	0	1	2023/03/03-33
Backup	Oracle8 ODC-UX-SV2000033-ORA-ar-LNNTSPRD1	Completed	full	3-3-2023 12:15:01	0:00	0:00	2,46	1	0	0	1	2023/03/03-35

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

Висновок

- Залежить від завдання: DigiD чи ISAE

Back-up & Recovery De beheersingsmaatregelen waarborgen met een redelijke mate van zekerheid dat back-ups in overeenstemming met het back-upbeleid worden gemaakt en dat back-ups hersteld kunnen worden.				
Norm	**Norm Naam**	**Beheersmaatregel**	**Testcriteria en bevindingen ADR**	**Oordeel ADR**
O1.1	De periodiciteit van de back-up dient aan te sluiten bij de maximaal toegestane periode waarover gegevens verloren mogen raken. Stel vast dat de back-up de juiste systemen en data-bestanden omvat die relevant zijn voor de jaarrekening.	De periodiciteit van de back-up dient aan te sluiten bij de maximaal toegestane periode waarover gegevens verloren mogen raken. Stel vast dat de back-up de juiste systemen en data omvat die relevant zijn voor de jaarrekening.	TC1: Stel vast dat SSC-ICT afspraken met de klant omtrent de periodiciteit, de soort (OS/DB) en retentietijd van back-ups zijn vastgelegd (bijvoorbeeld SLA, DAP, etc.). TC2: Stel vast dat de periodiciteit van de back-up, soort back-up en retentietijd van back-ups (back-upschema) aansluit bij de afspraken met (bijv. beschreven in de SLA met de klant of in de standaard dienstverlening van SSC-ICT). Werkzaamheden: de beschreven is opzet is voor alle maanden in de auditperiode vergeleken met de werking middels ontvangen back-up jobs. Bevindingen: Als gevolg van de terugwijk naar de oorspronkelijke productieomgeving (van voor oktober 2021) zijn niet alle productie back-ups in de periode daarna volledig gelukt. Door de controles die zijn gedaan en de maatregelen die zijn genomen door SSC-ICT, is er altijd een actuele productie back-up beschikbaar geweest. Hierdoor wordt het risico laag geschat.	Ineffectief
O1.2	De back-up gegevens worden op een veilige locatie bewaard zodat de integriteit van de back-up geborgd worden.	Stel vast, nadat in O1.1 is bepaald dat de back-up tijdig en volledig tot stand is gekomen, op welke wijze de back-up wordt opgeslagen. Stel vast dat de opgeslagen back-up beveiligd is tegen onbevoegde wijzigingen en op dusdanige afstand van de bron is opgeslagen dat een mogelijke calamiteit bij de bron geen effect heeft op de back-up.	TC1: Stel vast op welke wijze de back-ups worden opgeslagen. TC2: Stel vast dat de opgeslagen back-up beveiligd is tegen onbevoegde wijzigingen. TC3: Stel vast dat de back-ups op dusdanige afstand van de bron zijn opgeslagen dat een mogelijke calamiteit bij de bron geen effect heeft op de back-ups. TC4: Stel vast dat back-up jobs worden gemonitord en bij fouten/niet gelopen back-ups correctieve acties worden uitgevoerd. Werkzaamheden: er is vastgesteld dat de back-ups conform de opzetbeschrijving op een veilige locatie worden opgeslagen. Geen bevindingen geconstateerd.	Effectief
O1.3	Het kunnen terugzetten van de back-up (recovery) wordt periodiek getest.	Om te bepalen of back-ups ook correct kunnen worden teruggezet is het van belang te bepalen of de recovery procedure betrouwbaar heeft gefunctioneerd. Dit dient minimaal jaarlijks te worden getest.	TC1: Stel vast dat de uitgevoerde recovery test conform de recovery procedure is uitgevoerd. TC2: Stel vast dat er een uitwijktest conform de procedure (en/of afspraken met de klant) is uitgevoerd. Werkzaamheden: de opzet is vergeleken met de recoverytest die in mei 2022 is uitgevoerd. Geen bevindingen geconstateerd.	Effectief
O1.4	Uitwijktest dient jaarlijks plaats te vinden.	Jaarlijks wordt een uitwijktest conform de uitwijkprocedure uitgevoerd om vast te stellen of er in een noodsituatie uitgeweken kan worden.	TC1: Stel vast dat er een uitwijkprocedure is waarin staat beschreven op welke wijze aan de beheersingsmaatregel voldaan wordt. TC2: Stel vast dat de uitgevoerde uitwijktest conform de procedure is uitgevoerd. Werkzaamheden: deze norm is beoordeeld door middel van de terugwijk naar de productie-omgeving in september. Geen bevindingen geconstateerd.	Effectief

Nr	Beschrijving van de beveiligingsrichtlijn	Oordeel
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacy bevorderende en cryptografische technieken.	Voldoet
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.	Voldoet niet
U/PW.03	De webserver is ingericht volgens een configuratie-baseline.	Voldoet
U/PW.05	Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en wordt uitgevoerd conform het operationeel beleid voor platformen.	Voldoet niet
U/PW.07	Voor het configureren van platformen een hardeningsrichtlijn beschikbaar.	Voldoet niet
U/NW.03	Het netwerk is gescheiden in fysieke en logische domeinen (zones), in het bijzonder is er een DMZ die tussen het interne netwerk en het internet gepositioneerd is.	Voldoet
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen.	Voldoet
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.	Voldoet
U/NW.06	Voor het configureren van netwerken is een hardeningsrichtlijn beschikbaar.	Voldoet
C.03	Vulnerability assesments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope).	Voldoet niet
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).	Voldoet
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.	Voldoet
C.07	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT-systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd.	Voldoet
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	Voldoet
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT-voorzieningen.	Voldoet niet

Справедливе «слухання»

- Яку інформацію ви надсилаєте?
- Кому ви надсилаєте знахідки?
- Що стається затим?

Звітування

- Формат - стандарти
- З якими особами узгоджуєте?
- Як надсилаєте?
- Зміст

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

Запитання?

- Чи є у вас запитання?
- Чи можемо ми ще вам чимось допомогти?
- Що найважливіше ви вивчили за ці два заняття?