

**roc van
twente**

Vorbereiding tweede audit Deloitte



- **Eerste audit en aanbevelingen**
- **Verbeterde statements**
- **Statements op niveau 3 of hoger**
- **15 aangewezen statements vanuit audit**
- **22 statements vanuit weerbaarheidspool**
- **Intake en kick off van Deloitte**
- **Betrokkenen informeren**
- **Trustbound**

Eerste audit en aanbevelingen

Planning 1e audit

Stap	Intake	Kick-off	GRC-analyse	Aanvullend bewijs	Interviews
Datum	3 juni 2024	6 juni 2024	6 juni – 1 juli 2024	Gedurende het project	1 & 3 juli 2024
Uitgevoerde activiteiten	Introductie en bespreken planning, scope en uitgevoerde self-assessment	Kick-off sessie met alle relevante stakeholders binnen de instelling	Analyse GRC-applicatie; analyseren op basis van criteria	Opvragen aanvullend bewijs	Interviews met specifieke control eigenaren/uitvoerders
Uitkomst	Instelling en security auditteam kennen elkaar; informatie nodig voor het uitvoeren van de security audit is uitgewisseld.	Stakeholders kennen security auditteam en begrijpen aanpak van de security audit en wat van hen verwacht wordt.	Overzicht in hoeverre op het self-assessment gesteund kan worden en aan welke criteria nog niet voldaan wordt.	Aanvullende bewijsstukken, zodat alsnog aan criteria voldaan kan worden.	Aanvullende informatie, zodat alsnog aan criteria voldaan kan worden.

Stap	Analyse	Afstemming	Rapportage	Afsluiting
Datum	3 juli – 23 augustus 2024	23 augustus 2024 – 26 augustus 2024	23 september 2024	Nader te bepalen
Uitgevoerde activiteiten	Analyse, toekennen van scores, formuleren van observaties	Afstemming scores en observaties tussen Deloitte en ROC van Twente en verwerken feedback in werkprogramma	Opstellen rapportage, inclusief aanbevelingen	Verwerken feedback in definitieve rapportage en presentatie aan stakeholders
Uitkomst	Uitgevoerde analyse, vastgelegd in ons werkprogramma, met scores en observaties per control.	Afgestemde scores en observaties via e-mail.	Conceptrapportage, ter afstemming met instelling.	Definitieve rapportage; presentatie aan stakeholders.

Verbeterde statements

Verbeterde statements vanuit het jaarplan

- **5 statements verbeterd naar volwassenheidsniveau 3**

Statement op 3 of hoger

Statements op 3

Bij ROC van Twente staan 22 statements op niveau 3 of hoger in afgelopen audit

5 van de 22 worden getoetst op werking

15 aangewezen statements vanuit audit

15 Statements beoordeeld op werking

HR.04	Verandering of beëindiging van functie	x
IM.01	Incident Management	x
IM.02	Incident escalatie	x
IM.03	Incidentrespons op informatiebeveiligingsincidenten	x
IM.04	Problem Management	x
CH.01	Normen en procedures voor aanpassingen	x
CH.02	Impact assessment, prioriteren en autoriseren	x
CH.03	Noodaanpassingen	x
CH.05	Testen van aanpassingen	x
CH.06	Promotie naar productie	x
ID.01	Toegangsrechten	x
ID.02	Administratie van toegangsrechten	x
ID.03	Super Users	x
ID.04	Noodtoegang (envelopprocedure/breek-hetglasprocedure)	x
ID.05	Periodieke beoordeling van toegangsrechten	x

15 Statements beoordeeld op werking

HR.04	Verandering of beëindiging van functie
-------	--

Risico HR.04	Gebruikerstoegang wordt niet tijdig uitgeschakeld nadat medewerkers het team hebben verlaten of om een andere reden geen toegang meer mogen. Door gebrekkige kennisoverdracht wordt de continuïteit van de functie bedreigd.
---------------------	--

Aan te leveren documenten t.a.v. aantoonbaarheid werking per deelwaarneming:	
1)	Onderbouwing/ trigger om account te disablen of wijzigen. Denk daarbij aan: een ticket, opzegbrief of tijdelijk contract waaruit uitdiensttredingsdatum staat vermeld. Zorg dat zichtbaar is om welke persoon het gaat en disableing datum.
2)	Snipprint uit de applicatie waaruit het volgende blijkt: username, disableing (of wijzigings)datum.

Selectie:

Indicatie van frequentie hoe vaak accounts zijn disabled de afgelopen 3 maand:
Meer dan 10 keer

Aantal aan te leveren deelwaarnemingen:
3

Te selecteren waarnemingen:
De eerste van de afgelopen drie maanden

Lijstwerk
Lever het lijstwerk aan (denk aan: ticketoverzicht van mutaties/ verwijderverzoeken of HR-lijst van uitdiensttredingen en wijzigingen) en licht toe dat de waarnemingen conform bovenstaande selectie zijn geselecteerd.

Toelichting:

Vraag/ aan te leveren toelichting:

Hoe is gewaarborgd dat alle accounts die disabled moeten zijn, daadwerkelijk tijdig worden disabled?

Antwoord:

Controle:

Identificatie	Het account is tijdig disabled?	Toelichting/ beschrijving waaruit blijkt dat account tijdig is disabled. Indien blijkt dat account niet tijdig is disabled toelichting waarom niet:

22 aangewezen statements vanuit CWP

22 Statements behorende bij Cyberweerbaarheidspool

NBA-ID	Statement	Cyberweerbaarheidspool
GO.05	Onafhankelijke toetsing	x
OR.01	Eigenaarschap, rollen en verantwoordelijkheden	x
RM.03	Plan voor risicobehandeling	x
HR.06	Veiligheidsbewustzijn	x
CO.01	Identificatie en onderhoud van configuraties	x
IM.03	Incidentrespons op informatiebeveiligingsincidenten	x
DM.02	Classificatie	x
ID.01	Toegangsrechten	x
ID.02	Administratie van toegangsrechten	x
ID.03	Super Users	x
ID.05	Periodieke beoordeling van toegangsrechten	x
SM.02	Authenticatiemechanismes	x
SM.03	Mobiele apparaten en telewerken	x
SM.04	Logging, Monitoring en Opvolging	x
SM.06	Patchmanagement	x
SM.07	Threat en Vulnerability Management	x
SM.11	Network Security	x
SM.12	Beheersing van malware-aanvallen	x
OP.02	Procedures voor backup en herstel	x
BC.01	Bedrijfscontinuïteitsplanning	x
BC.02	Testen van Disaster recovery	x
SC.01	Service Level Overeenkomst	x

Intake en kick off

Intake

- **Contact met Henry voor voorinformatie**
- **Op 16 december met Deloitte**

Kick off

- **6 januari interne kick off betrokkenen**
- **Eind januari alle betrokkenen en Deloitte**

Betrokkenen informeren

Intern betrokkenen

- **In november een bijeenkomst gepland voor januari**
- **Informatie over de nieuwe werkwijze delen**
- **Taken verdelen voor het aanleveren van bewijs voor werking**
- **Inzicht geven in de statements vanuit de weerbaarheidspool**

Trustbound

- **Niveau wijziging aangeven in Trustbound en onderbouwen met documentatie**
- **Werking hoeft niet via Trustbound, maar via Teams en excel formulier**
- **Verwerkingsregister wordt ingericht in Trustbound**

Vragen?