Welkom!

49ste MBO Digitaal Conferentie

8 maart 2024

Security Audits in het MBO

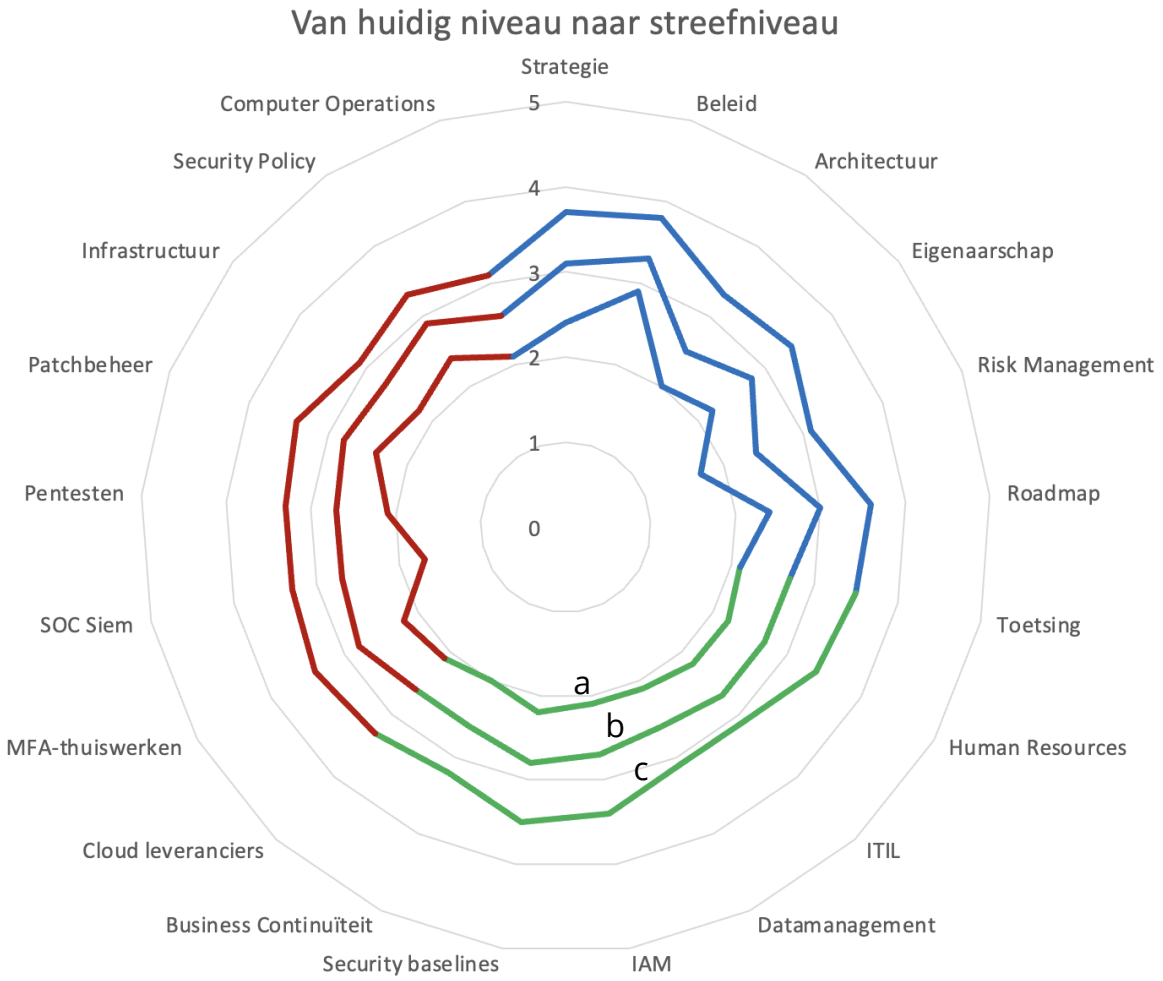
Niels Dutij
MBO Digitaal

Self-assessments en benchmark

1. Sinds 2015 al self-assessments op het gebied van IBP;
2. Benchmark op basis van self-assessments;
3. Externe validatie via peer review en expert review.

mbo digitaal

Nulmeting volwassenheid Informatiebeveiliging



Groei in volwassenheid

a) Volwassenheid Q3 - 2022: 2,1

b) Prognose Q3 - 2023: 2,8 ?

c) Streefvolwassenheid: 3,3

Governance
Processen
Technische weerbaarheid

- Gaan we dit redden in 2024?
- En wat gaat de auditor betekenen?

Security audits in het MBO

1. In cyberconvenant MBO opgenomen dat mbo-instellingen gaan deelnemen aan de onafhankelijke security audits van MBO Digitaal;
2. Sectorale aanpak zorgt voor efficiency en uniforme meetlat;
3. Validatie van de benchmark en betere verantwoording aan externe partijen;
4. Aanbesteding van MBO Digitaal om 1 auditpartij te werven voor het verrichten van security audits;
5. **Start audits per mei 2024**

Auditplan

1. Twee audits in de periode 2024-2027 op het NBA-toetsingskader;
2. Eerste audit meer educatief karakter en toetst op opzet en bestaan;
3. Tweede audit toetst op opzet, bestaan en werking;
4. Toetsing op vier kern-applicaties (SIS, Finance, HR, Studentenbegeleidingssysteem) bij systeem-gebonden statements;
5. Toetsing op proces bij de generiekere statements.
6. GRC-applicatie 'Trustbound' van groot belang!

mbo digitaal

Controls op applicatie-niveau

Domeinnr	Domeinnaam	Stnr	NBA-id	Statement		Applicatie
7	Change Management	23	CH.01	Normen en procedures voor aanpassingen		X
		24	CH.02	Impact assessment, prioriteren en autoriseren		X
		25	CH.03	Noodaanpassingen		X
		26	CH.04	Testomgeving		X
		27	CH.05	Testen van aanpassingen		X
		28	CH.06	Promotie naar productie		X
9	Datamanagement	32	DM.01	Data (en systeem) eigenaarschap		X
		33	DM.02	Classificatie		X
		34	DM.03	Beveiligingseisen voor datamanagement		X
		35	DM.04	Inrichting van opslag en retentie		X
		36	DM.05	Uitwisseling van (gevoelige) gegevens		X
		37	DM.06	Verwijdering van data		X
10	Identity & Access Management	38	ID.01	Toegangsrechten		X
		39	ID.02	Administratie van toegangsrechten		X
		40	ID.03	Super Users		X
		41	ID.04	Noodtoegang (envelopprocedure/breek-het-glasprocedure)		X
		42	ID.05	Periodieke beoordeling van toegangsrechten		X
11	Security Management	43	SM.01	Security baselines		X
		44	SM.02	Authenticatiemechanismes		X
		46	SM.04	Logging en Monitoring		X
		55	SM.13	Bescherming van beveiligingstechnologie		X
13	IT-operatie	58	OP.01	Job processing		X
		59	OP.02	Procedures voor back-up en herstel		X
		60	OP.03	Capacity and Performance Management		X
		64	BC.04	Gegevensreplicatie		X
15	Ketenbeheer	66	SC.01	Service Level Overeenkomst		X
		67	SC.02	Service Level Management		X
		68	SC.03	Supplier Risk Management		X
		69	SC.04	Interne beheersing bij derden		X

Planning en start audits

1. Planning van de audits zal nog met leverancier worden afgestemd;
2. Loting bij de planning van audits;

Interesse om als eerste de audit te krijgen? Laat het weten!

mbo digitaal

Tijdslijn

Jaar	Security audit	januari	februari	maart	april	mei	juni	juli	augustus	september	oktober	november	december
2024	*1ste*	-	-	V	2	4	4	-	-	2	4	4	2
2025	*1ste*	2	4	4	4	4	4	-	-	2	4	4	2
2026	*2de*	2	4	4	4	4	4	-	-	2	4	4	2
2027	*2de*	2	4	4	4	4	2	U	U	U	-	-	-

Vragen?