



MBO Security Audits Workshop Deloitte

11 december 2025



Introductie

Het team van Deloitte



Mark Bouman-
Schildkamp



Linda Otte



Amy Tjin
Tjoen Jin



Agenda

Programma van vandaag

Inzicht in de resultaten tot nu toe

Generieke observaties

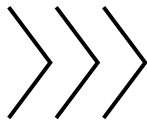
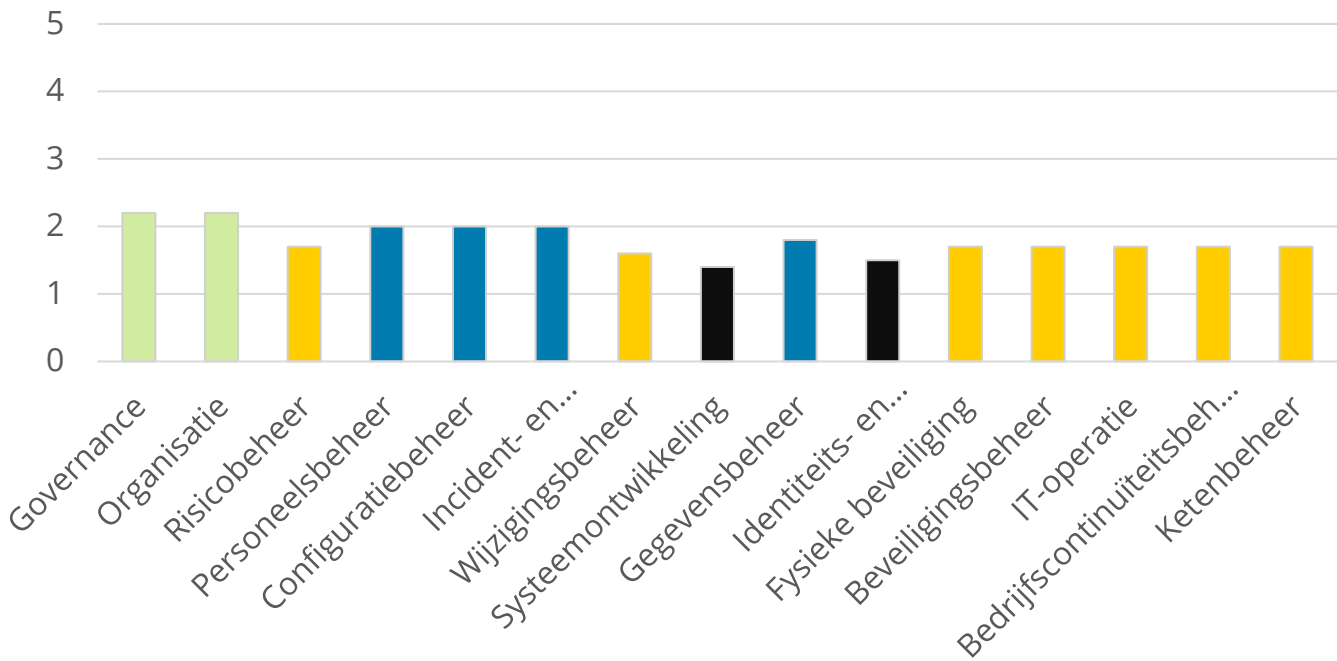
Stellingen

Vragen

Project in cijfers

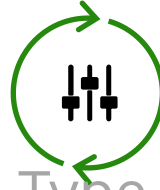
Inzicht in de resultaten tot nu toe

Dit overzicht geeft de gemiddelde volwassenheidsscores weer per domein. Tot nu toe is de audit bij 43 instellingen afgerond en ligt de **gemiddelde score op 1.8**



Domein	Score
Governance	2,2
Organisatie	2,2
Risicobeheer	1,7
Personeelsbeheer	2,0
Configuratiebeheer	2,0
Incident- en Probleembeheer	2,0
Wijzigingsbeheer	1,6
Systeemontwikkeling	1,4
Gegevensbeheer	1,8
Identiteits- en Toegangsbeheer	1,5
Fysieke beveiliging	1,7
Beveiligingsbeheer	1,7
IT-operatie	1,7
Bedrijfscontinuïteitsbeheer	1,7
Ketenbeheer	1,7

Generieke observaties



Veel voorkomende observaties tijdens de Type A Audit

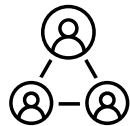
Sterke punten

Vastgesteld IBP-beleid



Vormt de basis voor informatie beveiliging.

Rollen en verantwoordelijkheden toegewezen



Vergroot duidelijkheid en escalatie.

Processen rondom incidentmanagement vastgelegd



Verkort detectie- en hersteltijden en maakt structurele verbeteringen mogelijk.

Veiligheidsbewustzijns programma's gedefinieerd



Vergroot het bewustzijn onder medewerkers en versterkt de effectiviteit van maatregelen.

Verbeterpunten

Kaders rondom risicomanagement ontbreken



Risico's worden mogelijk niet tijdig vastgesteld.

Kaders rondom ketenbeheer ontbreken



Er bestaat een risico dat prestatie afwijkingen niet tijdig worden gedetecteerd.

Formalisatie van processen ontbreekt



Kans dat uitvoering niet gestructureerd of formeel plaatsvindt.

Periodieke beoordeling van toegangsrechten ontbreekt



Risico dat onjuiste bevoegdheden onopgemerkt blijven en toezicht op overtredingen ontbreekt.

Stellingen



Stelling 01

A hand holding a lit lightbulb inside a thought bubble. The background is a dark green surface with a pattern of overlapping, slightly crumpled paper documents. The thought bubble is white and contains the text.

Beter een informeel beleid dat werkt dan een formeel beleid dat niet werkt.

Stelling 02

Omdat het cyberrisico bij kleinere instellingen beperkt is, is een lager volwassenheidsniveau passend.



Stelling 03

Op het moment dat we diensten uitbesteden aan derden, zijn we niet meer verantwoordelijk voor de processen, omdat wij afspraken met de leverancier contractueel hebben vastgelegd.



Stelling 04

Naast de benchmark
moeten wij ook nog
beschikken over andere (in-
of externe) onafhankelijke
toetsing voor een
volwassenheids-
niveau 3.



Stelling 05

Als we aangesloten
zijn bij de SOC/SIEM van SURF
voldoen wij aan niveau 5 en
hoeven we geen beleid/processen
rondom dit onderwerp
te hebben.



Stelling 06

A hand holding a lit lightbulb inside a thought bubble. The background of the slide is a dark green with a pattern of overlapping, semi-transparent white documents or papers. The thought bubble is white and contains the text and the lightbulb.

De MORA is voldoende als
Enterprise Information
Architecture Model (EIAM).

Stelling 07

A hand holding a lit lightbulb next to a thought bubble containing text.

Als ik alleen cloud-applicaties gebruik en geen on-premise systemen heb, is een noodprocedure niet vereist.

Stelling 08

Één keer per jaar de
SOLL-matrix vergelijken
met de huidige situatie is
voldoende.



Stelling 09

Het hebben van back-ups is niet voldoende. We moeten ook aantoonbaar kunnen herstellen uit back-ups via reproduceerbare, geteste herstel-configuraties.



Vragen



Project in cijfers

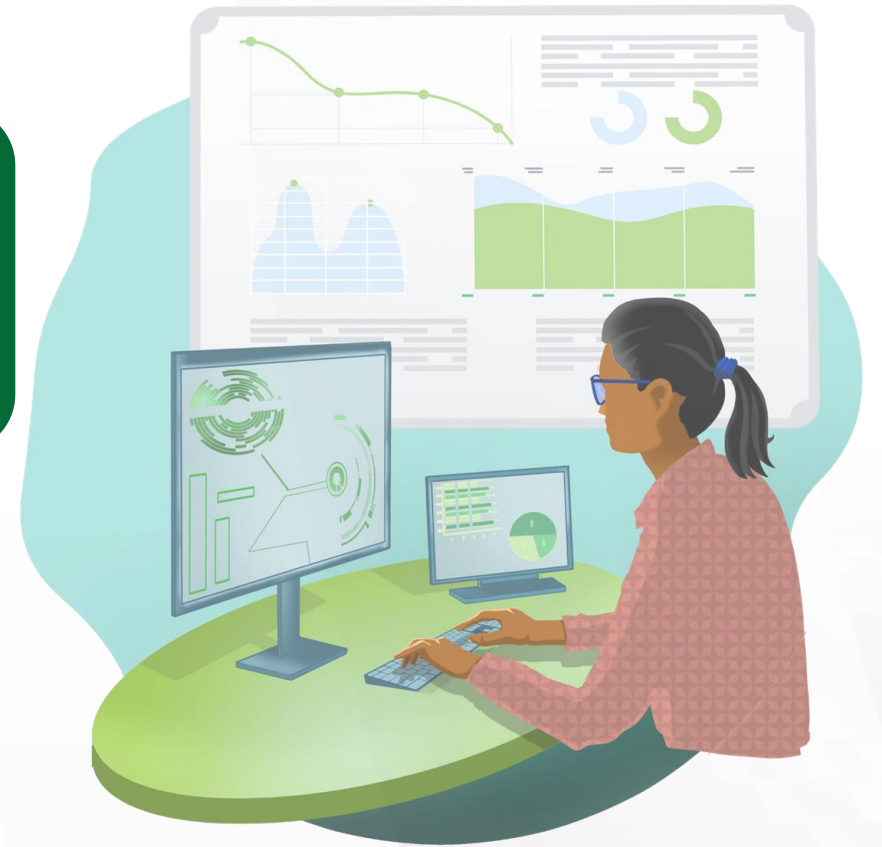
Aantal
documenten
geanalyseerd:
7700

Afgenomen
interviews:
105

In totaal hebben
36 collega's aan
dit project
gewerkt

In totaal **102**
intake en kick
offs afgenomen

Totaal bestede
uren aan dit
project:
10.198 uur





Bedankt & fijne feestdagen namens het Deloitte MBO team.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms and their related entities. DTTL (also referred to as "Deloitte Global") and each of its member firms are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.nl/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 286,000 people make an impact that matters at www.deloitte.nl.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms or their related entities (collectively, the "Deloitte network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.