Checklist BIO voor bestuurders

Samen slimmer met data

De Baseline Informatiebeveiliging Overheid (BIO) vraagt risicogerichte informatiebeveiliging (IB) in alle geledingen van een organisatie en kan daarom niet worden gezien als een afvinklijstje. Voor **sturingsdoeleinden** is onderstaande checklist met algemene en verdiepende vragen opgesteld langs 16 onderwerpen[1] die samen een aggregatie zijn van de volledige BIO. Aan de hand van de checklist kunnen bestuurders gesprekken aangaan met hun CISO om een beeld te krijgen van de **staat van informatiebeveiliging** in de eigen organisatie.

Een rode bol met een cijfer geeft aan hoeveel (van de in totaal 110) BIO-maatregelen aan een specifiek onderwerp zijn verbonden. Voor een diepgaander self-assessment BIO kan gebruik worden gemaakt van de tool die te vinden is via onderstaande link.

[1] https://www.cip-overheid.nl/

Onderwerp	Algemeen	Verdiepend
2 **IB-beleid** is passend, effectief en cyclisch (P&C)	Is er organisatiebreed informatiebeveiligings-beleid vastgesteld en geïmplementeerd?	Wanneer is het beleid voor het laatst opnieuw beoordeeld of herzien?
4 **IB-organisatie** is formeel ingesteld en gepositioneerd	Is er een IB-organisatie ingesteld (o.a. CISO, FG) en is daarvoor mandaat vastgesteld?	Wanneer is de IB-organisatie voor het laatst bijeen geweest en wat hebben zij gerapporteerd?
6 Informatiebeveiliging is verankerd in **personeelsbeleid**	Is IB opgenomen in het personeelsbeleid? (bijv. bewustzijn, functie eisen of sanctiebeleid)	Wanneer was de laatste bewustwordings-campagne en is IB onderwerp van de gesprekscycli?
17 **Werkomgevingen** (fysiek/online) zijn passend beveiligd	Zijn de fysieke en digitale werkomgeving risicogericht beveiligd?	Wanneer is voor het laatst de beveiliging getest en wat was de uitkomst?
14 **Toegang tot de ICT-infrastructuur** is logisch beveiligd	Is er passend en risicogericht wachtwoordbeleid ingericht?	Wanneer is het wachtwoordbeleid herzien; voor welke risico's is multifactor authenticatie geïmplementeerd?
5 **Systeembeheer** borgt wijzigingen en bewaakt prestaties	Hoe worden de systemen waarmee we werken up-to-date gehouden?	Welke technische kwetsbaarheden zijn het meest recent verholpen en is daarvan een verslag beschikbaar?
6 **IB-incidenten** worden vastgelegd om van te leren	Op welke wijze worden IB-incidenten gelogd en hoe wordt daarvan geleerd?	Hoeveel incidenten waren er in afgelopen jaar en wat is de top 3 van de oorzaken van incidenten?
7 ICT wordt beschermd tegen **kwetsbaar-heden en aanvallen**	Op welke wijze worden IB-incidenten/ aanvallen voorkomen en gemonitord?	Hoeveel aanvallen zijn er het afgelopen jaar geweest; hoeveel werden onderschept en hoeveel zijn doorgedrongen?

Onderwerp	Algemeen	Verdiepend
6 **Netwerken en informatiestromen** worden bewaakt	Hoe wordt informatie geclassificeerd en hoe worden informatiestromen beschermd?	Welke data hebben we inmiddels geclassificeerd?
12 **Testen/ontwikkelen** kent procedures en security by design	Zijn er gescheiden productie- en testomgevingen?	Welke testomgeving werd het laatst gebruikt, wanneer was dat en is deze testomgeving nog steeds actief?
5 **Wetten/contracten** worden aantoonbaar nageleefd	Worden er verwerkers-overeenkomsten afgesloten en risico-beoordelingen uitgevoerd?	Wanneer is de laatste verwerking van persoonsgegevens opgenomen in het verwerkingsregister?
2 **Cryptografie** wordt in beleid geborgd en passend uitgevoerd	Hoe wordt versleuteling van gegevens toegepast in de organisatie?	Wanneer is de huidige methodiek van versleuteling opnieuw beoordeeld?
5 **Back-up/redundantie/ uitwijk** is onderdeel van BCM	Is Back-up en Restore onderdeel van bedrijfs-continuïteitsplanning?	Wanneer is voor het laatst succesvol een volledige back-up teruggezet?
10 De **lifecycle van alle apparatuur en data** is geregistreerd	Worden apparatuur en informatiedragers veilig vernietigd?	Wanneer was de laatste vernietiging en is daarvan een rapport beschikbaar?
5 In **leveranciersbeheer** zijn risicoafwegingen doorslaggevend	Op welke wijze is er aandacht voor keten-risico's, onder andere bij leveranciers?	Wanneer hebben de laatste leveranciers-beoordelingen plaatsgevonden?
4 Periodiek vinden **audits en beoordelingen** plaats adhv ISMS	Is er een managementsysteem ingericht voor IB?	Wanneer vond de laatste audit plaats en welke bevindingen werden gerapporteerd?

TLP: WIT