Bestuurlijke Cbw-checklist

Cyberbeveiligingswet in de praktijk

Een praktische eerste zelfcontrole voor bestuurders, directieleden, CISO's, security- en compliance verantwoordelijken.

Cbw

Doel

In 15-20 minuten vaststellen waar de bestuurlijke basis op orde is en waar directe actie nodig is. Gebruik de checklist als startpunt voor overleg, bewijsvoering en een concreet verbeterplan.

Hoe gebruikt u deze checklist?

Vink een controlepunt alleen af wanneer u het aantoonbaar kunt onderbouwen. Een mondelinge aanname is niet voldoende. Noteer bij open punten direct een eigenaar en streefdatum. Deze checklist is bedoeld als bestuurlijke eerste controle en vervangt geen sectorspecifieke juridische of technische beoordeling.

Belangrijk

De Cyberbeveiligingswet (Cbw) is sinds 15 augustus 2026 van kracht. Voor organisaties die onder de wet vallen gelden onder meer een registratieplicht, zorgplicht, meldplicht en bestuurlijke verantwoordelijkheid. Bestuurders moeten maatregelen goedkeuren, toezicht houden op de uitvoering en passende training volgen.

Organisatiegegevens

Organisatie _____

Datum beoordeling _____

Bestuurlijk eigenaar _____

Uitgevoerd met _____

Snelle uitkomst

Gebruik op pagina 4 de scorekaart. Open punten bij incidentmelding, bestuurlijke training, risicoanalyse of registratie verdienen altijd directe aandacht, ongeacht de totaalscore.

BESTUURLIJKE Cbw-CHECKLIST

1 Toepasselijkheid en registratie

Eerst vaststellen of de organisatie onder de Cbw valt en of de formele registratie klopt.

OK	Controlepunt	Eigenaar / rol
☐	We hebben formeel vastgesteld of onze organisatie onder de Cyberbeveiligingswet valt en de onderbouwing is vastgelegd.	Bestuur / Legal
☐	Sector, omvang, type entiteit en eventuele aanwijzing zijn gecontroleerd aan de hand van actuele NCSC-informatie.	Legal / Compliance
☐	Indien van toepassing is de organisatie geregistreerd in het nationale entiteitenregister via MijnNCSC.	CISO / Bestuur
☐	De geregistreerde contact- en netwerkgegevens zijn actueel en er is een eigenaar voor wijzigingen binnen de wettelijke termijn.	CISO / IT

2 Bestuurlijke verantwoordelijkheid

Kan het bestuur aantoonbaar sturen, beoordelen en toezicht houden?

OK	Controlepunt	Eigenaar / rol
☐	Het bestuur heeft de maatregelen uit de zorgplicht expliciet goedgekeurd of heeft een aantoonbaar proces om dit te doen.	Bestuur
☐	Cyberrisico's staan periodiek op de bestuurs- of directieagenda.	Bestuur
☐	Er is vastgelegd welke cyberrisico's het bestuur bewust accepteert en waarom.	Bestuur / CISO
☐	Bestuurders hebben passende training gevolgd om cyberrisico's en beveiligingsmaatregelen te kunnen beoordelen.	Bestuur / HR
☐	Besluiten over belangrijke beveiligingsmaatregelen en restrisico's worden aantoonbaar vastgelegd.	Bestuur

3 Risicoanalyse en zorgplicht

Van technisch risico naar bestuurbare bedrijfsrisico's.

OK	Controlepunt	Eigenaar / rol
☐	Er is een actuele risicoanalyse van netwerk- en informatiesystemen, processen, mensen en relevante afhankelijkheden.	CISO / Risk
☐	Kritieke diensten en systemen zijn geïdentificeerd en geprioriteerd.	CISO / IT / Business
☐	Voor de belangrijkste risico's zijn passende en evenredige technische, operationele en organisatorische maatregelen vastgesteld.	CISO / Bestuur
☐	De werking van maatregelen wordt periodiek getest en niet alleen op papier beoordeeld.	CISO / Audit
☐	Bedrijfscontinuiteit, herstel en crisisbeheersing zijn onderdeel van de cyberaanpak.	BCM / CISO

4 Incidentmelding en respons

Een significant incident laat weinig tijd voor improvisatie.

OK	Controlepunt	Eigenaar / rol
☐	Er is een vastgesteld incidentresponsproces met rollen, escalatielijnen en bereikbaarheid buiten kantooruren.	CISO / IT / Bestuur
☐	De organisatie kan significante incidenten tijdig beoordelen en melden aan het juiste CSIRT en de bevoegde autoriteit.	CISO / Legal
☐	De 24-uurs meldtermijn is bekend bij de functionarissen die een incident kunnen signaleren of escaleren.	CISO / Management
☐	Sectorspecifieke drempelwaarden voor significante incidenten zijn bekend en verwerkt in procedures.	CISO / Legal
☐	Het incidentresponsproces wordt geoefend, inclusief bestuurlijke besluitvorming en communicatie.	CISO / Bestuur / Communicatie

5 Leveranciers en keten

Uitbesteden van IT betekent niet dat het risico is uitbesteed.

OK	Controlepunt	Eigenaar / rol
☐	Kritieke leveranciers en digitale afhankelijkheden zijn in kaart gebracht.	Inkoop / CISO
☐	Cybersecurity-eisen zijn opgenomen in selectie, contractering en periodieke beoordeling van kritieke leveranciers.	Inkoop / Legal / CISO
☐	Voor kritieke leveranciers is bekend wat de impact is bij uitval of een beveiligingsincident.	Business / BCM
☐	Er is een proces voor het opvolgen van relevante kwetsbaarheden en incidenten bij leveranciers.	CISO / Vendor Mgmt

6 Medewerkers en organisatiebreed bewustzijn

Digitale weerbaarheid werkt alleen wanneer mensen weten wat van hen verwacht wordt.

OK	Controlepunt	Eigenaar / rol
☐	Medewerkers krijgen structurele en rolgerichte training in informatiebeveiliging en veilig digitaal gedrag.	HR / CISO
☐	Medewerkers weten hoe zij phishing, verdachte situaties en mogelijke incidenten moeten melden.	CISO / HR
☐	Nieuwe medewerkers ontvangen beveiligingsinstructies als onderdeel van onboarding.	HR / IT
☐	Kennis en bewustwording worden periodiek herhaald en aantoonbaar geregistreerd.	HR / Compliance
☐	Toegangsrechten en accounts worden tijdig aangepast bij functiewijziging of uitdiensttreding.	HR / IT

BESTUURLIJKE Cbw-CHECKLIST

7 Monitoring, toezicht en aantoonbaarheid

Bestuurlijke controle stopt niet na implementatie.

OK	Controlepunt	Eigenaar / rol
☐	Er is een compact periodiek management- of bestuursdashboard met de belangrijkste cyberrisico's en openstaande maatregelen.	CISO / Bestuur
☐	Incidenten, bijna-incidenten en relevante trends worden periodiek besproken.	CISO / Bestuur
☐	Interne controles, audits of onafhankelijke beoordelingen toetsen of maatregelen daadwerkelijk werken.	Audit / CISO
☐	Verbeteracties hebben een eigenaar, prioriteit en streefdatum en worden bestuurlijk gevolgd.	Management
☐	Documentatie is voldoende om richting toezichthouder aan te tonen hoe de organisatie haar verplichtingen beheerst.	Compliance / CISO

Scorekaart

26-30	**Basis grotendeels op orde**	Controleer open punten, bewijsvoering en sectorspecifieke eisen. Blijf periodiek monitoren.
19-25	**Verbetering nodig**	Maak een bestuurlijk verbeterplan met eigenaren, prioriteiten en termijnen.
0-18	**Verhoogd bestuurlijk risico**	Start direct met toepasselijkheid, registratie, risicoanalyse, incidentrespons en bestuurlijke training.

Mijn drie directe acties

1. _____
2. _____
3. _____

Volgende stap

Gebruik deze checklist als startpunt voor een bestuurlijk verbeterplan. Voor de Cbw is het belangrijk dat bestuurders voldoende kennis hebben om cyberrisico's en maatregelen te beoordelen. Organisatiebrede bewustwording ondersteunt daarnaast de dagelijkse uitvoering. ComplianceTrainingen.nl biedt hiervoor praktische trainingen en een gratis demo.

Actualiteit en bronnen: gebaseerd op actuele informatie van Rijksoverheid en NCSC over de Cyberbeveiligingswet, geraadpleegd op 2 september 2026. Sectorspecifieke regelingen kunnen aanvullende eisen bevatten. Deze checklist is een praktische zelfcontrole en geen juridisch advies, certificering of formele Cbw-audit.