TOEZICHT CHECKLIST

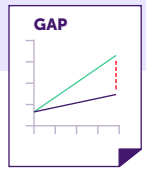
DORA-checklist

Digital Operational Resilience Act is een Europese verordening die zich richt op het vergroten van de cyberweerbaarheid van financiële ondernemingen. Deze ondernemingen hebben tot 17 januari 2025 de tijd om aan de vereisten te voldoen. Deze DORA-checklist is bedoeld om helder te krijgen wat er qua beleid en procedures nodig is om te voldoen aan de regelgeving aan de hand van 10 belangrijke thema's. Let op: vanwege de omvang van DORA is de checklist niet volledig. Daarvoor verwijzen wij naar de verordening en bijbehorende RTS en ITS voor nadere toelichting op de vereisten.
Zie de AFM website voor meer informatie.

Antwoordmogelijkheden

Nee

Advies om DORA GAP-analyse te starten

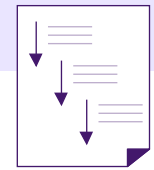


Deels

Advies om DORA GAP-analyse om te zetten in acties

Ja, opgesteld

Advies om implementatie-programma te starten en relevante (bedrijfs)processen aan te passen



Ja, opgesteld en geïmplementeerd

Advies om adequate werking van beleid en procedures doorlopend te monitoren

Let op: voor een aantal kleinere partijen geldt een vereenvoudigd kader voor ICT risicobeheer, zoals toegelicht in artikel 16(1) en AFM DORA update 3.

AFM

TOEZICHT CHECKLIST

Vragen

	Nee	Deels	Ja, opgesteld	Ja, opgesteld en geïmplementeerd

Governance (art. 5)

1/10

Heeft het leidinggevend orgaan een governance- en controlekader opgesteld voor het beheer van ICT-risico's?

Dit dient o.a. te voorzien in: duidelijke taken en verantwoordelijkheden van ICT-functies, zoals inrichting ICT-riskfunctie; toewijzing van budget; periodieke evaluaties en rapportagelijnen; en een intern ICT audit plan.

ICT-risicobeheer (art. 6)

2/10

Heeft u een kader voor ICT-risicobeheer opgesteld, als onderdeel van uw bedrijfsbrede risicobeheersysteem?

Dit dient o.a. te voorzien in; een risico-analyse methodiek, risico-register (inclusief actieplannen) en periodieke evaluaties.

Zie verder RTS15 en 16(3) voor nadere toelichting.

ICT-Asset inventaris (art. 8)

3/10

Heeft u een inventaris van alle informatie- en ICT-activa, incl. alle bedrijfsprocessen die steunen op ICT-diensten van derde aanbieders?

Dit dient te worden bijgehouden in een register waarin duidelijk aangegeven is of de activa kritieke processen ondersteunen.

Zie sectie III van RTS15 en 16(3) voor nadere toelichting.

Vragen

	Nee	Deels	Ja, opgesteld	Ja, opgesteld en geïmplementeerd

Informatiebeveiligingsbeleid (art. 9)

4/10

Heeft u een ICT-beveiligingsbeleid opgesteld, dat voorziet in beleid en procedures die gericht zijn op het waarborgen van de beschikbaarheid, integriteit en veiligheid van ICT-systemen?

Dit dient o.a. beleid en procedures te bevatten voor technische maatregelen, zoals: fysieke en logische toegangscontrole; beheer van ICT changes; encryptie; netwerkbeveiliging; en uitvoeren van patches en updates.

Zie verder RTS15 en 16(3) voor nadere toelichting.

Bedrijfscontinuïteit (art. 11-12)

5/10

Heeft u een ICT-bedrijfscontinuïteitsbeleid (Business Continuity Plan) opgesteld, dat voorziet in een bedrijfscontinuïteitsplan, het uitvoeren van bedrijfsimpactanalyses, een communicatieplan, periodieke testen, en een overzicht van gebeurtenissen?

Dit dient o.a. te worden getest door gebruik te maken van realistische testscenario's die potentiële verstoringen proberen te simuleren. Indien mogelijk, worden ook ICT-services van derde partijen meegenomen in de testwerkzaamheden. De testresultaten worden gedocumenteerd en afwijkingen worden geanalyseerd, opgevolgd en gerapporteerd aan het management.

Zie RTS15 en 16(3) voor nadere toelichting.

Back-up en herstel (art. 12)

6/10

Heeft u back-up beleid en procedures, incl. herstelprocedures en -methodieken?

Zie RTS15 en 16(3) voor nadere toelichting.

Awareness en scholing (art. 13)

7/10

Heeft u bewustmakingsprogramma's op het gebied van ICT-beveiliging en opleidingen ontwikkelt inzake digitale operationele weerbaarheid als verplichte modules in de opleidingsprogramma's in lijn met het takenpakket van medewerkers?

Vragen

	Nee	Deels	Ja, opgesteld	Ja, opgesteld en geïmplementeerd

Incidentenmanagement (art. 17-23)

8/10

Heeft u een beheersproces voor het detecteren en afhandelen van ICT-gerelateerde incidenten vastgesteld, inclusief het gebruik van een incidentenregister en sjablonen ter ondersteuning van de meldplicht?

Zie RTS18(3), RTS20(a) en ITS20(b) voor nadere toelichting.

Testprogramma voor digitale weerbaarheid (art. 24-27)

9/10

Heeft u een risico gebaseerd programma opgesteld voor het testen van digitale operationele weerbaarheid, inclusief beleid en procedures voor het opvolgen van bevindingen?

Zie RTS26(11) voor nadere toelichting.

ICT-risicobeheer van derde aanbieders (art. 28-30)

10/10

Heeft u beleid voor het beheersen van ICT-diensten van derde aanbieders die kritieke en/of belangrijke bedrijfsprocessen ondersteunen?

Dit dient o.a. te voorzien in: een informatieregister voor overeenkomsten met derde aanbieders van ICT-diensten, exitplannen voor kritieke en/of belangrijke functies, en contractsjablonen obv de eisen uit de RTS, zoals service levels en auditrechten.

Zie RTS28(1), RTS30(5) en ITS28(9) voor nadere toelichting.

Publicaties

De AFM deelt in aanloop naar de inwerkingtreding van DORA regelmatig informatieve updates en andere publicaties ter voorbereiding voor ondernemingen.