# Aan de slag met DORA: Beheer, classificatie en rapportage van ICT-gerelateerde incidenten

**In het kort** *Dit is de vierde editie in een reeks AFM-publicaties over de Digital Operational Resilience Act (DORA). Deze reeks is bedoeld voor alle ondernemingen die vanaf 2025 aan de Europese verordening moeten voldoen. In deze editie gaan we in op ICT-gerelateerde incidenten. Op deze manier kunnen ondernemingen analyseren waar ze staan op dit vlak en welke stappen ze eventueel nog moeten zetten om aan de verordening te voldoen.*

## 1. ICT-gerelateerde incidenten in DORA

DORA heeft als doel dat financiële instellingen ICT-risico's beter beheersen en daarmee weerbaarder worden tegen cyberdreigingen en ICT-verstoringen. Hiervoor beschrijft de verordening verschillende vereisten op het gebied van ICT, waaronder voor ICT-gerelateerde incidenten. Ondernemingen kunnen nu al analyseren of ze op dit punt aan de DORA-vereisten voldoen om vervolgens (indien nodig) tot actie over te gaan. Om op 17 januari 2025 aan DORA te voldoen, is het noodzakelijk nu al bezig te zijn met de implementatie.

Om de effecten van ICT-gerelateerde incidenten te kunnen beperken, is het belangrijk dat deze adequaat worden gedetecteerd en afgehandeld. De vereisten voor het beheer van ICT-incidenten en cyberdreigingen worden in de verordening beschreven in artikel 17 (hoofdstuk III). Daarnaast wordt een deel van de vereisten met betrekking tot het detecteren van incidenten en het reageren hierop uitgewerkt in hoofdstuk 3 (artikel 23 en 24) van de *Regulatory Technical Standard* (RTS) voor ICT-risicobeheer[1].

Als onderdeel van het beheerproces moeten ondernemingen hun ICT-incidenten op een consistente manier classificeren, zodat deze zorgvuldig kunnen worden opgevolgd en afgehandeld. In de verordening (artikel 18) staat beschreven hoe ondernemingen ICT-incidenten moeten classificeren en aan de hand van welke criteria zij de impact van het incident kunnen bepalen. Deze criteria worden verder toegelicht in de RTS[2]. Daarnaast wordt in deze technische standaard toegelicht wanneer ICT-incidenten of cyberdreigingen als ernstig (*major*) of significant worden geclassificeerd.

Ondernemingen moeten er verder voor zorgen dat alle ICT-incidenten die zich voor hebben gedaan, worden geregistreerd. Dit biedt hun de mogelijkheid om incidenten te evalueren en analyses uit te voeren om de oorzaak van het incident te achterhalen. DORA schrijft voor dat belangrijke ICT-incidenten moeten worden gemeld aan de toezichthouder (dit is momenteel al verplicht voor incidenten die een ernstige bedreiging vormen voor de integere bedrijfsvoering[3]). In de verordening staan algemene vereisten waar deze rapportages aan moeten voldoen. Zo wordt in artikel 19 beschreven welke rapportages moet

1 https://www.esma.europa.eu/sites/default/files/2023-06/CP_-_Draft_RTSs_ICT_risk_management_tools_methods_processes_and_policies.pdf

2 https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_83_-_Final_Report_on_draft_RTS_on_classification_of_major_incidents_and_significant_cyber_threats.pdf

3 Zie ter referentie voor beleggingsondernemingen en beheerders van beleggingsinstellingen ook https://www.afm.nl/nl-nl/sector/actueel/2023/mei/deep-dive-incidenten-bo

worden gedeeld met de toezichthouder en wanneer klanten van de financiële entiteit op de hoogte moeten worden gebracht van het incident. In de RTS en *Implementing Technical Standard* (ITS)[4] staat in detail beschreven wat ondernemingen moeten opnemen in de rapportages. Hierin is ook een template in opgenomen die kan worden gebruikt voor het rapporteren van *major* incidenten. In deze publicatie zijn wij uitgegaan van de RTS/ITS die zijn gepubliceerd op het moment van schrijven. Aangezien de inhoud van deze RTS/ITS nog niet definitief is, zou het kunnen dat er nog wijzigingen zullen plaatsvinden, al zien we vaak dat de inhoud op hoofdlijnen gelijk blijft.

In de volgende secties staan we stil bij het beheer en de classificatie van ICT-incidenten en cyberdreigingen en waar organisaties nu al mee aan de slag kunnen om aan de vereisten van DORA te voldoen. Ook bespreken we kort hoe ondernemingen ICT-incidenten en cyberdreigingen kunnen melden bij de AFM.

**Tabel 1**

| Aanvullende uitwerkingen | Onderwerp | Afgerond |
|---|---|---|
| RTS voor artikel 15 | Further harmonisation of ICT risk management tools, methods, processes and policies | Inmiddels naar EC verzonden |
| RTS voor artikel 18(3) | Classification of ICT related incidents and cyber threats | Inmiddels naar EC verzonden |
| RTS voor artikel 20(a) | Reporting content and templates | Uiterlijk 17 juli 2024 |
| ITS voor artikel 20(b) | ITS to establish the reporting details for major ICT related incidents | Uiterlijk 17 juli 2024 |

4 JC_2023_70_-_CP_on_draft_RTS_and_ITS_on_major_incident_reporting_under_DORA.pdf (europa.eu)

# 2. Aan de slag met ICT-incidenten

### Beheer van ICT-incidenten

Ondernemingen kunnen nu al aan de slag met:
- Het opstellen en implementeren van een beheerproces voor ICT-gerelateerde incidenten.

Artikel 17 van de verordening beschrijft de vereisten voor het beheerproces voor ICT-incidenten. Het beheerproces helpt ondernemingen bij het adequaat detecteren, melden en afhandelen van ICT-incidenten. Om de impact van deze incidenten tot een minimum te beperken, moeten organisaties een passend beleid en geschikte procedures opstellen en implementeren. In hoofdstuk III (artikel 22 en 23) van de RTS voor ICT-risicobeheer staat verder toegelicht wat instellingen moeten opnemen in hun ICT-incidentenbeleid en welke mechanismen zij moeten implementeren om incidenten te detecteren en hierop te reageren.

Het ICT-incidentenbeleid moet de onderneming in staat stellen om technische, organisatorische en operationele mechanismen te implementeren die het beheerproces voor ICT-incidenten ondersteunen, zoals technieken die nodig zijn om afwijkende activiteiten en gedrag te identificeren. Daarnaast moeten ondernemingen in het ICT-incidentenbeleid vastleggen welke medewerkers en (externe) stakeholders direct betrokken zijn bij de beveiliging van ICT-systemen. Hieronder vallen de personen die verantwoordelijk zijn voor het detecteren en monitoren van cyberdreigingen, afwijkende activiteiten en voor vulnerability management. Voor significante of terugkerende ICT-incidenten moeten ondernemingen processen en methodes inrichten om deze te analyseren.

Het beheerproces voor ICT-incidenten ziet erop toe dat alle ICT-incidenten worden geregistreerd en op een consistente manier worden gemonitord, behandeld en opgevolgd. Hierdoor kunnen de onderliggende oorzaken worden opgespoord, gedocumenteerd en opgelost. Door dit op een juiste manier in te richten kunnen organisaties de kans dat een incident zich vaker voordoet zo veel mogelijk verkleinen. Een ander doel van het beheerproces is om plannen op te stellen voor de communicatie richting het eigen personeel, externe stakeholders en de media, in overeenstemming met het communicatiebeleid (zie hiervoor ook artikel 14 in de verordening) en te garanderen dat ernstige ICT-incidenten aan het desbetreffend leidinggevend personeel worden gemeld.

Om op een effectieve manier ICT-incidenten en afwijkingen te detecteren en hierop te reageren, is het belangrijk dat de rollen en verantwoordelijkheden op dit gebied duidelijk worden vastgelegd en gecommuniceerd binnen de organisatie. Daarnaast dienen instellingen detectiemechanismen te implementeren die hen in staat stellen om:
- interne en externe factoren, waaronder informatie uit systeemlogging, te verzamelen, te monitoren en te analyseren;
- potentiële interne en externe cyberdreigingen te verzamelen, te monitoren en te analyseren, waaronder veelvoorkomende scenario's;
- informatie over ICT-incidenten van derde partijen te verzamelen, te monitoren en te analyseren;
- afwijkende activiteiten en gedrag te identificeren en instrumenten te implementeren voor het genereren van alerts voor afwijkingen;
- relevante informatie over alle afwijkende activiteiten vast te leggen, te analyseren en te evalueren.

Aangezien er belangrijke (en vaak vertrouwelijke) informatie in de incidentverslagen staat, is het belangrijk dat deze en andere relevante informatie over het incident veilig worden opgeslagen en dat deze niet ongeautoriseerd kunnen worden aangepast. Daarnaast moet de belangrijkste informatie over het incident, zoals de datum en tijd van de afwijking en het type incident, worden vastgelegd in een logbestand. Tot slot moet de ICT-incidentprocedure worden geïnitieerd

wanneer er indicaties zijn van ongeautoriseerde activiteiten op een ICT-systeem of netwerk of wanneer er aanwijzingen zijn dat een ICT-systeem of netwerk niet meer veilig is. Andere gevallen waarbij de ICT-incidentprocedure moet worden gevolgd, zijn in het geval van gegevensverlies en wanneer systemen of netwerken niet beschikbaar zijn. Hierbij moet rekening worden gehouden met het belang van de getroffen diensten.

### Classificatie van ICT-incidenten

Ondernemingen kunnen nu al aan de slag met:
- Procedures opstellen (en implementeren) waarin wordt beschreven hoe incidenten worden geclassificeerd.

Voor een effectief beheerproces is het belangrijk dat ICT-incidenten en cyberdreigingen juist worden geclassificeerd. Dit helpt ondernemingen bij het bepalen van de middelen die nodig zijn om het incident op te lossen. Daarnaast helpt dit om de status en verwachtingen te communiceren naar stakeholders binnen de organisatie. Voor het classificeren kunnen instellingen zelf bepalen hoe zij de incidenten indelen. Hierbij moet wel onderscheid kunnen worden gemaakt tussen ernstige (*major*) incidenten, cyberdreigingen en alle overige incidenten (low impact, medium impact, etc.).

Voor het classificeren van ICT-incidenten moeten ondernemingen een aantal criteria hanteren die helpen bij het bepalen van de impact van het incident op de organisatie en externe stakeholders. Deze criteria zijn:
- Het aantal en de relevantie van klanten die door het incident zijn getroffen. Hierbij gaat het om de klanten die gebruik maken van de diensten van de onderneming of de financiële tegenpartijen waar de onderneming een contractuele overeenkomst mee heeft. Daarnaast moeten ondernemingen vaststellen in hoeverre de impact van het incident dat de klant getroffen heeft, ook effect heeft op de doelstelling van de eigen onderneming. Tot slot wordt de relevantie van de klant bepaald door te kijken naar het effect van de klant op het vermogen van de instelling om haar doelstellingen te behalen;
- Het verlies van gegevens als gevolg van het incident. Hiervoor moeten ondernemingen bepalen of gegevens nog toegankelijk zijn (beschikbaarheid), of de gegevens onjuist of onvolledig zijn (integriteit) en of de gegevens zijn benaderd of openbaar zijn gemaakt door ongeautoriseerde gebruikers (vertrouwelijkheid);
- De mate waarin de getroffen diensten als cruciaal voor de onderneming kunnen worden aangemerkt. Dit is het geval wanneer het incident invloed heeft gehad op ICT-diensten die belangrijke of kritieke bedrijfsfuncties ondersteunen;
- De reputatieschade die het incident heeft veroorzaakt. Om de reputatieschade vast te stellen, kijken ondernemingen hoeveel aandacht het incident heeft gekregen in de markt. Hierbij kan onder andere worden onderzocht of het incident in de media is gekomen, of er klachten zijn binnengekomen vanuit klanten of dat de onderneming als gevolg van het incident niet kan voldoen aan wettelijke eisen;
- De duur van het incident. Om dit te bepalen meet de onderneming de tijd tussen het moment dat het incident plaatsvindt en het moment dat het incident is opgelost. Wanneer het startmoment niet kan worden vastgesteld, kan de onderneming het moment gebruiken wanneer het is vastgesteld of wanneer het is vastgelegd in logbestanden of andere databronnen. Als de precieze oplostijd niet bekend is, mogen instellingen een schatting maken om het einde van het incident te bepalen;
- De geografische spreiding van de gebieden die door het incident zijn getroffen. Om de geografische spreiding te bepalen, beoordelen instellingen onder andere de impact van het incident op de klanten, andere kantoren of instellingen binnen de groep in tenminste twee EU-lidstaten;
- De economische effecten van het incident in absolute en relatieve termen. Hierbij gaat het om directe en indirecte kosten en verliezen als gevolg van het incident.

In het geval dat een of meer van de criteria niet met zekerheid kan worden bepaald, moet een schatting worden gemaakt met behulp van de beschikbare data.

Om te bepalen of het gaat om een ernstig (*major*) incident, moet de onderneming kijken naar het aantal criteria waar het incident een materiële impact op heeft gehad. In de bovenstaande lijst worden het aantal getroffen klanten, het verlies van gegevens en het aantal getroffen kritieke diensten als primaire criteria gezien. De overige criteria worden als secundaire criteria beschouwd. Op het moment dat een ICT-incident een materiële impact heeft op twee primaire criteria óf meer dan drie criteria waarvan minstens één primair criterium, moet deze als ernstig worden geclassificeerd. De toelichting over wanneer de impact materieel is, wordt per criterium nader toegelicht in de RTS[5]. Wanneer ICT-incidenten zich vaker herhalen, maar individueel niet als ernstig worden geclassificeerd, kunnen deze alsnog als ernstig worden geclassificeerd wanneer ze vaker voorkomen in een periode van drie maanden. Hiervoor moet het incident vaker dan twee keer plaatsvinden, dezelfde oorzaak hebben en een vergelijkbare impact hebben. Voor cyberdreigingen geldt dat deze als significant kunnen worden aangemerkt wanneer de dreiging invloed heeft op de kritische of belangrijke bedrijfsfuncties van de onderneming, andere financiële instellingen, derde partijen of klanten. Daarnaast moet er een grote kans zijn dat de cyberdreiging zich daadwerkelijk manifesteert. Tot slot moet de cyberdreiging een materiële impact hebben op twee primaire criteria óf meer dan drie criteria waarvan minstens één primair criterium, wanneer de dreiging zich materialiseert. Wanneer de cyberdreiging aan alle voorwaarden voldoet moet deze worden geclassificeerd als significant.

Tabel 2

| Aanvullende uitwerkingen | Beschrijving | Afgerond |
|---|---|---|
| RTS voor artikel 18(3) | Classification of ICT related incidents and cyber threats | Inmiddels naar EC verzonden |

## Rapportage van ernstige ICT-incidenten en significante cyberdreigingen

Ondernemingen kunnen nu al aan de slag met:
- Voorbereidingen treffen om tijdig te kunnen rapporteren over ernstige ICT-incidenten

Wanneer een ICT-incident wordt geclassificeerd als ernstig (*major*), moet deze worden gemeld bij de toezichthouder. De toezichthouder kan op basis van de melding, passende opvolgacties nemen en voorkomen dat het incident een negatieve invloed heeft op de rest van de sector. In het geval dat het incident ook gevolgen heeft voor de financiële belangen van hun klanten, moeten ondernemingen hen hier op de hoogte van brengen. Hierbij moeten zij ook aangeven welke maatregelen zijn genomen om de negatieve effecten van het incident te beperken. Ondernemingen hebben naast het verplicht melden van ICT-incidenten, ook de mogelijkheid om significante cyberdreigingen op vrijwillige basis te melden bij de toezichthouder. Dit kunnen zij doen wanneer zij van mening zijn dat de dreiging relevant is voor de rest van de financiële sector, gebruikers van financiële diensten of hun klanten. De vereisten voor het melden van ICT-incidenten en cyberdreigingen staan in artikel 19 van de verordening en de RTS/ITS voor incidenten rapportage (artikel 20(a) en 20(b)). Hierin wordt daarnaast beschreven wat instellingen moeten opnemen in het incidentenrapport.

### *Eerste kennisgeving*

Op het moment dat een onderneming (op basis van de criteria in het vorige hoofdstuk) bepaald dat een *major* ICT-incident heeft plaatsgevonden, moet een eerste kennisgeving worden gedeeld met de toezichthouder. Hiervoor hebben instellingen 4 uur de tijd vanaf het moment dat het incident als ernstig wordt geclassificeerd, maar dit mag niet langer zijn dan 24 uur nadat het incident is gedetecteerd. In de eerste kennisgeving leggen ondernemingen de algemene informatie over het incident vast, zoals de beschrijving van het incident, wanneer het incident is gedetecteerd en de classificatie van het incident (inclusief de beoordeling van de eerdergenoemde criteria).

5 https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_83_-_Final_Report_on_draft_RTS_on_classification_of_major_incidents_and_significant_cyber_threats.pdf

Verder is het belangrijk dat de onderneming vermeldt hoe het incident is ontdekt, of het incident vaker voorkomt en wat de oorzaak is van het incident. Indien mogelijk, geeft de instelling ook een indicatie of het *business continuity plan* is geactiveerd als gevolg van het incident en of het incident impact heeft gehad op andere financiële instellingen en derde partijen.

***Tussentijds verslag***

Na de eerste kennisgeving moeten instellingen bij ernstige ICT-incidenten ook een tussentijds verslag aanleveren bij de toezichthouder. Het tussentijds verslag moet binnen 72 uur na de classificatie van het incident worden ingediend of zodra de reguliere activiteiten zijn hersteld. Net als in de eerste kennisgeving moeten ondernemingen hierin vermelden wanneer het incident is vastgesteld en op basis van welke criteria is bepaald dat het om een *major* incident gaat. Daarnaast beschrijft de onderneming het type incident en geeft ze informatie over de getroffen onderdelen van de organisatie, zoals bedrijfsprocessen en infrastructuur-componenten. Verder moet in het tussentijds verslag worden aangegeven of het incident is gecommuniceerd naar klanten en welke tijdelijke maatregelen de onderneming heeft genomen om te herstellen van het incident. Tot slot is het belangrijk dat instellingen aangeven wat de gevolgen zijn van het incident. Hiervoor moeten ondernemingen kijken of er kwetsbaarheden zijn misbruikt en of er een indicatie is dat IT-systemen of de IT-infrastructuur niet meer veilig kunnen worden gebruikt.

***Eindverslag***

Uiterlijk een maand na de classificatie van het incident dient de onderneming een eindverslag te delen met de toezichthouder. Wanneer het incident op dat moment nog niet is opgelost, moet het eindverslag uiterlijk een dag nadat het incident definitief is opgelost worden ingediend. Het eindverslag bevat de datum wanneer het incident is opgelost, informatie over de oorzaak van het incident en informatie over het onvermogen van de onderneming om te voldoen aan wettelijke eisen en contractuele overeenkomsten/SLA's (indien van toepassing). In het eindverslag moet ook worden beschreven welke maatregelen de onderneming heeft genomen om het incident op te lossen en om te voorkomen dat het incident zich vaker voordoet. Verder is het belangrijk dat de onderneming informatie geeft over de directe en indirecte kosten die zijn gemaakt als gevolg van het incident.

***Melden significante cyberdreigingen***

Naast het (verplicht) melden van *major* ICT-incidenten, hebben instellingen ook de mogelijkheid om significante cyberdreigingen op vrijwillige basis te melden bij de toezichthouder. Wanneer zij ervoor kiezen om dit te melden, is het belangrijk dat de belangrijkste informatie over de cyberdreiging wordt gedeeld met de toezichthouder. Deze informatie bestaat uit de datum waarop de dreiging is geconstateerd, een beschrijving van de cyberdreiging en de status van de cyberdreiging. Daarnaast is het belangrijk dat de instelling de potentiële impact van de dreiging op de instelling vermeldt en aangeeft welke acties zijn ondernomen om te voorkomen dat de dreiging materialiseert. In het geval dat klanten mogelijk zijn getroffen door de cyberdreiging, zijn ondernemingen wel verplicht om hen op de hoogte te brengen van passende beschermingsmaatregelen die zij kunnen nemen.

De AFM is momenteel bezig met het ontwikkelen van een online omgeving waar instellingen hun ICT-gerelateerde incidenten en geïdentificeerde cyberdreigingen kunnen melden. Deze online omgeving zal onderdeel zijn van het AFM Portaal[6] (waar onder toezicht staande instellingen toegang tot hebben). Instellingen die onder DORA gaan vallen én onder toezicht staan van de AFM zullen vanaf 17 januari 2025 in het AFM Portaal meldingen kunnen plaatsen over uitbestedingen, significante ICT-incidenten en cyberdreigingen. Voor ICT-gerelateerde incidenten kunnen instellingen de eerste kennisgeving delen met de AFM via het portaal. Zodra de eerste kennisgeving is gedeeld komt het incident in het overzicht te staan met alle eerdere meldingen van de instelling. Het tussentijdse verslag en het eindverslag worden vervolgens automatisch gekoppeld aan het incident zodra de instelling de benodigde stukken indient. Tot slot zal het portaal een overzicht weergeven van de openstaande acties. Wanneer aanvullende stukken moeten worden ingediend, zal de organisatie hier een melding van krijgen.

6 https://portaal.afm.nl/

Tabel 3

| Aanvullende uitwerkingen | Beschrijving | Afgerond |
|---|---|---|
| RTS voor artikel 20(a) | Reporting content and templates | Uiterlijk 17 juli 2024 |
| ITS voor artikel 20(b) | ITS to establish the reporting details for major ICT related incidents | Uiterlijk 17 juli 2024 |

# 3. Vooruitblik

Momenteel zijn zowel de eerste als de tweede batch van RTS'en en ITS'en gepubliceerd. De eerste batch (waaronder die voor artikel 18(1)) is inmiddels voorgelegd aan de Europese Commissie die deze zal beoordelen en hier in juli 2024 een beslissing over zal nemen. De tweede batch is door de ESA's voorgelegd aan ondernemingen in de financiële sector ter consultatie. Deze zal naar waarschijnlijkheid in het derde kwartaal van 2024 worden voorgelegd aan de Europese commissie.

De AFM bereidt zich in de tussentijd verder voor op het uitvoeren van DORA-toezicht. In de volgende publicatie uit deze reeks zal dieper worden ingegaan op testen van digitale operationele weerbaarheid. De volgende editie zal in het derde kwartaal van 2024 worden gepubliceerd.

Voor een verdere uitwerking over ICT-incidenten in DORA kunnen de volgende pagina's worden geraadpleegd: www.afm.nl/nl-nl/sector/themas/belangrijke-europese-wet--en-regelgeving/dora/incidenten en www.afm.nl/nl-nl/sector/themas/belangrijke-europese-wet--en-regelgeving/dora/melden

Verdere vragen? Neem contact op met het ondernemersloket van de AFM.