Aan de slag met DORA: ICT-risicobeheer

In het kort Dit is de derde editie in een reeks AFM-publicaties over de Digital Operational Resilience Act (DORA). Deze reeks is bedoeld voor alle ondernemingen die vanaf 2025 aan deze Europese verordening moeten voldoen. In deze editie gaan we in op het ICT-risicobeheer. Door voldoende aandacht te besteden aan ICT-risicobeheer, kunnen organisaties een goed beeld schetsen van hun ICT-risico's en hoe zij de effecten hiervan tot een minimum kunnen beperken. 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 Risk Management 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 het ICT-risicobeheer (ofwel *ICT Risk Management*). 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 17 januari 2025 aan DORA te voldoen, is het raadzaam zo vroeg mogelijk te beginnen.

Een belangrijk onderdeel in DORA is het ICT-risicobeheer. Goed ICT-risicobeheer helpt organisaties om op gestructureerde wijze ICT-risico's te detecteren en beheersen. De vereisten worden in de verordening beschreven in hoofdstuk II (artikel 5 t/m 16). In deze artikelen wordt onder andere ingegaan op het *ICT Risk Management framework, Business Continuity Management* (BCM) en de scholing en ontwikkeling van medewerkers op het gebied van ICT-beveiliging en digitale operationele weerbaarheid.

Naast de beschreven vereisten in de verordening, worden een aantal onderwerpen verder uitgewerkt in een *Regulatory Technical Standard* (RTS)[1]. In deze RTS worden de ICT-risicobeheerinstrumenten, -methoden, -processen en -beleidslijnen (artikel 15) en het vereenvoudigd kader voor ICT-risicobeheer (16, lid 3) uitgewerkt. Hierbij is artikel 15 voor alle ondernemingen, zoals beschreven in artikel 2, lid 1 van toepassing, terwijl in artikel 16 een vereenvoudigd kader voor ICT-risicobeheer wordt beschreven voor een aantal specifieke typen ondernemingen.[2]

In de volgende secties worden de genoemde artikelen uit de DORA-verordening toegelicht. Ook staan we stil bij een aantal onderwerpen die verder zijn uitgewerkt in de RTS. Belangrijk om hierbij te vermelden is dat de RTS-teksten in januari 2024 naar de Europese Commissie (EC) zijn gestuurd. Het zou kunnen dat er nog wijzigingen zullen plaatsvinden in de tekst van de RTS, al zien we vaak dat de tekst op grote lijnen gelijk blijft.

1 RTS on *ICT Risk Management framework* and on simplified *ICT Risk Management framework*

2 Het gaat hier om kleine en niet-verweven beleggingsondernemingen, betalingsinstellingen die krachtens Richtlijn (EU) 2015/2366 zijn vrijgesteld; instellingen die krachtens Richtlijn 2013/36/EU zijn vrijgesteld en waarvoor de lidstaten hebben besloten de in artikel 2, lid 4, van deze verordening bedoelde optie niet toe te passen; instellingen voor elektronisch geld die krachtens Richtlijn 2009/110/EG zijn vrijgesteld, en kleine instellingen voor bedrijfspensioenvoorziening.

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 16(3)	Simplified ICT risk management framework	Inmiddels naar EC verzonden

2. Aan de slag met *ICT-risicobeheer*

Risk Management in DORA (artikelen 6 tot en met 14)

Ondernemingen kunnen nu al aan de slag met:
- Het opstellen van een kader voor ICT-risicobeheer (waaronder op het gebied van uitbestedingen);
- Het controleren of wordt voldaan aan de vereisten op het gebied van Business Continuity Management (BCM).

Artikel 6 van de verordening beschrijft de vereisten voor het kader voor ICT-risicobeheer (ofwel het *ICT Risk Management framework*). Om ICT-risico's snel, efficiënt en zo volledig mogelijk aan te pakken, is het van belang dat ondernemingen over een solide, goed gedocumenteerd *ICT Risk Management framework* beschikken. In dit framework worden onder meer de strategieën, beleidslijnen, procedures, ICT-instrumenten vastgelegd die nodig zijn om alle ICT-activa (*ICT assets*)[3] en relevante fysieke elementen te beschermen.

Het *ICT Risk Management framework* dient minimaal één keer per jaar (of periodiek voor micro-ondernemingen) te worden geëvalueerd en aanpassingen moeten aan het framework moeten worden gedocumenteerd. Hierbij wordt het framework continu verbeterd op basis van de lessen die uit de uitvoering en monitoring naar voren zijn gekomen. Tot slot moet het *ICT Risk Management framework* periodiek worden onderworpen aan een onafhankelijke audit. De uitkomsten van de audit moeten worden opgevolgd.

Om de stabiliteit van dienstverlening van een onderneming te kunnen waarborgen, stelt DORA vereisten op het gebied van *Business Continuity Management* (BCM). Deze vereisten worden in artikel 8 t/m 12 van de verordening beschreven:
- Ondernemingen moeten hun ICT-landschap overzichtelijk in kaart brengen. Hiervoor is het van belang dat alle bedrijfsfuncties, taken en verantwoordelijkheden die door ICT worden ondersteund worden geïdentificeerd, geclassificeerd en gedocumenteerd. Hetzelfde geldt voor de ICT-activa en applicaties die deze bedrijfsfuncties ondersteunen.
- Instellingen moeten continu de beveiliging en werking van ICT-systemen[4] controleren. Dit heeft een positieve uitwerking op de bescherming van de ICT-systemen en vermindert de kans op cyberincidenten.
- Ondernemingen kunnen hun ICT-risico's op ICT-systemen verder beperken door ICT-beveiligingsinstrumenten, -beleidslijnen en -procedures in te zetten die erop gericht zijn de weerbaarheid, continuïteit en beschikbaarheid van ICT-systemen te waarborgen. Aangezien niet alle incidenten kunnen worden voorkomen, is het van belang dat financiële instellingen over detectiemechanismen beschikken om afwijkende activiteiten zo snel mogelijk te detecteren en om zwakke (fysieke) punten te identificeren. Zodra een afwijking is gedetecteerd, dienen instellingen hier op gepaste wijze te reageren.
- Ondernemingen moeten een ICT-bedrijfscontinuïteitsbeleid opstellen en uitvoeren. In dit beleid zijn regelingen, plannen, procedures en mechanismen opgenomen die er onder andere op toe zien dat de continuïteit van kritieke functies wordt gewaarborgd, ICT-incidenten op een goede manier en met minimale schade worden opgelost en dat alle betrokken interne en externe stakeholders op de hoogte worden gebracht van het incident dat zich heeft voorgedaan.

In de RTS worden enkele onderwerpen rondom BCM, zoals het testen van het BCP en het respons- en herstelplan, verder uitgewerkt. Hier komen wij in het volgende onderdeel op terug.

3 Alle software of hardware in de netwerk- en informatiesystemen die door de financiële entiteit worden gebruikt.

4 Alle ICT-activa die samenwerken om een bepaalde bedrijfsfunctie uit te voeren.

De laatste twee artikelen in de verordening over ICT-risicobeheer (artikel 13 en 14) gaan over scholing en ontwikkeling en communicatie. Wat betreft scholing en ontwikkeling is het van belang dat ondernemingen over voldoende capaciteiten en personele middelen beschikken om informatie te verzamelen over kwetsbaarheden, cyberdreigingen en ICT-gerelateerde incidenten. Hierbij dienen financiële entiteiten rekening te houden met technologische ontwikkelingen, de resultaten van uitgevoerde tests op digitale operationele weerbaarheid en ICT-incidenten die zich hebben voorgedaan.

In het geval dat een ICT-gerelateerd incident plaatsvindt, is het belangrijk dat wordt onderzocht wat de verstoring heeft veroorzaakt en welke verbeteringen moeten worden doorgevoerd om herhaling van de verstoring te voorkomen. Daarnaast is het belangrijk dat ondernemingen over crisiscommunicatieplannen beschikken om in het geval van ernstige ICT-incidenten adequaat te handelen. Hieronder valt onder meer het op verantwoorde wijze kenbaar maken van het kwetsbaarheden aan het personeel, cliënten en ander direct betrokkenen.

Verdere uitwerking van ICT-risicobeheer in de RTS (artikel 15)

Ondernemingen kunnen nu al aan de slag met:

- Beleid en procedures ontwikkelen/implementeren op het gebied van onder andere het beheer van ICT assets, netwerkbeveiliging en encryptie en cryptografie.

In dit onderdeel zullen wij een aantal onderwerpen uit de RTS toelichten. Deze onderwerpen zijn een verdere uitwerking van artikel 15 in de verordening. Hierbij is voor het overzicht gekozen voor een selectie van onderwerpen uit de RTS. Het feit dat niet alle onderwerpen uit de RTS worden besproken in deze publicatie betekent niet dat de andere onderwerpen minder belangrijk zijn. Ondernemingen dienen per 17 januari 2025 te voldoen aan alle eisen die in de RTS zijn uitgewerkt.

Business Continuity Management

In hoofdstuk IV (artikel 24 t/m 26) van de RTS zijn een aantal onderwerpen rond BCM verder uitgewerkt. Hierin gaat het onder meer over het testen van het *Business Continuity Plan* (BCP) om de continuïteit van kritieke en belangrijke bedrijfsfuncties te waarborgen. Tijdens het testen van het BCP moeten ondernemingen gebruik 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.

Naast het testen van het BCP moeten ondernemingen een respons- en herstelplan opstellen om de impact van verstoringen te minimaliseren. Hierbij moeten organisaties rekening houden met de *Business Impact Analysis* (zie ook artikel 11(5) in de verordening). In het ICT-respons- en herstelplan wordt onder andere opgenomen in welke situaties het plan van toepassing is (en wanneer niet), de acties die worden ondernomen om de beschikbaarheid, integriteit, vertrouwelijkheid van kritische en belangrijke systemen te waarborgen en in welke gevallen de uitvoering van het respons- en herstelplan als succesvol kan worden bestempeld.

ICT Asset Management

Als onderdeel van het beheer van ICT-activa, moeten ondernemingen een beleid en procedures opstellen (en implementeren) om de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens te waarborgen. In het beleid staat hoe de organisatie de *life cycle* van haar ICT-activa monitort en beheert. Daarnaast dienen instellingen een overzicht te maken van alle ICT-activa, inclusief de locatie, classificatie, systeemeigenaar en de bedrijfsfunctie die door de ICT-activa wordt ondersteund. Tot slot, moet er een procedure zijn waarin wordt beschreven hoe de onderneming bepaalt of een ICT-asset of applicatie kritiek of belangrijk is.

Encryptie en cryptografie

Net als voor het beheer van ICT-activa, moeten ondernemingen een beleid opstellen en implementeren waarin de encryptie van gegevens en het beheer van cryptografische sleutels wordt beschreven. In dit beleid worden onder meer de criteria beschreven om cryptografische technieken en gebruikspraktijken te selecteren. Ook moet worden beschreven in welke situaties een onderneming overstapt naar een

nieuwe cryptografische techniek om de weerbaarheid tegen cyber-aanvallen te vergroten. Voor het beheer van cryptografische sleutels is het van belang dat ondernemingen eisen stellen voor elke fase in de *life cycle* van cryptografische sleutels. Hieronder valt het genereren, vernieuwen, opslaan, maken van *back-ups*, archiveren, ophalen, verzenden, buiten gebruik stellen, intrekken en vernietigen van sleutels.

Netwerkbeveiliging
Voor de beveiliging van netwerken binnen de organisatie is het belangrijk dat ondernemingen een beleid en procedure opstellen en implementeren waarin maatregelen worden beschreven die ongewenste toegang tot het netwerk en gegevensmisbruik tegengaan. Door een overzicht te maken van de verschillende netwerkverbindingen en datastromen binnen de organisatie krijgen instellingen een goed beeld van het netwerk. Verder is het van belang dat netwerkverbindingen die over bedrijfsnetwerken, openbare netwerken, binnenlandse netwerken, netwerken van derden en draadloze netwerken gaan, worden beveiligd en versleuteld om ongewenste toegang tot de gegevens te voorkomen. Tot slot kunnen instellingen de beveiliging van hun netwerk waarborgen door regelmatig de ingestelde regels voor de firewall te herzien en de netwerkarchitectuur en netwerkbeveiliging periodiek te beoordelen.

Vulnerability en patch management
Om de netwerken van ondernemingen verder te beveiligen, dienen instellingen procedures te beschrijven voor zowel *vulnerabillity* als *patch management*. In de *vulnerability management* procedure staat onder meer beschreven hoe de instelling ervoor zorgt dat regelmatig een (geautomatiseerde) *vulnerability* scan wordt uitgevoerd en hoe de geïdentificeerde kwetsbaarheden worden opgevolgd en gemonitord. Tegelijkertijd ziet de *patch management* procedure erop toe dat software en hardware patches automatisch worden geïdentificeerd en getest in een omgeving los van de productieomgeving (indien mogelijk) en dat er een termijn wordt gesteld aan de installatie van patches en updates.

Logging
Naast *vulnerability* en *patch management* en netwerkbeveiliging, dienen instellingen zich te beveiligen tegen indringers en gegevensmisbruik door de handelingen van gebruikers te loggen. Hierbij moeten ondernemingen voor zichzelf bepalen welke handelingen worden bijgehouden, hoe lang de logbestanden worden bewaard en maatregelen om de gegevens veilig te bewaren en verwerken. Om de juistheid van de logbestanden te waarborgen is het ook belangrijk dat maatregelen worden genomen om de logbestanden te beschermen tegen ongeautoriseerde toegang, manipulatie/verwijdering en storingen in het *logging* systeem.

Change management
Om de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens te waarborgen, is het belangrijk dat instellingen een *ICT change management* procedure hebben opgesteld en geïmplementeerd. In deze procedure wordt beschreven hoe de organisatie verifieert dat er wordt voldaan aan de ICT-veiligheidseisen, dat wijzigingen worden aangevraagd, getest, goedgekeurd en geïmplementeerd door de juiste medewerkers en hoe *emergency changes* moeten worden doorgevoerd. Verder is het belangrijk dat ondernemingen nadenken over de evaluatie en monitoring van wijzigingen na de implementatie en welke stappen moeten worden doorlopen wanneer een wijziging voortijdig wordt afgebroken of niet kan worden geïmplementeerd.

Logische toegangsbeheer
Voor het logische toegangsbeheer is het eveneens belangrijk dat er een beleid en procedures wordt opgesteld (en geïmplementeerd). Hierin moet worden beschreven hoe personen en systemen met toegang tot gegevens van de instelling, worden geïdentificeerd en geautoriseerd. Hiervoor is het belangrijk dat alle (externe) medewerkers een unieke identiteit toegewezen krijgen die is gekoppeld aan het gebruikersaccount van de medewerker. Deze identiteiten/gebruikersaccounts moeten worden bijgehouden en periodiek worden gecontroleerd. Onder het controleren van de identiteit valt het aanmaken, wijzigen, (tijdelijk) deactiveren en verwijderen van accounts. Naast de identificatie van gebruikers, is het van belang dat de toegang van medewerkers tot gegevens juist wordt beheerd door de organisatie.

Hierbij moeten instellingen de toegang van medewerkers tot gegevens zoveel mogelijk proberen te beperken (*least privililege principles*), functiescheidingsconflicten voorkomen en ervoor zorgen dat handelingen in ICT-systemen kunnen worden herleid naar medewerkers (met name wanneer gedeelde accounts worden gebruikt). Tot slot is het belangrijk dat mutaties van toegangsrechten juist en tijdig worden doorgevoerd.

Tabel 2

Aanvullende uitwerkingen	Beschrijving	Afgerond
RTS voor artikel 15	Further harmonisation of ICT risk management tools, methods,processes and policies	Inmiddels naar EC verzonden

Vereenvoudigd kader voor ICT-risicobeheer (artikel 16)

In artikel 16 van de verordening worden de vereisten voor het vereenvoudigd kader voor ICT-risicobeheer beschreven welke van toepassing zijn op een aantal uitgezonderde instellingen.[5] Hierbij is een deel van de vereisten voor het framework in de verordening beschreven, terwijl een ander deel in de RTS wordt uitgewerkt.

Als er wordt gekeken naar het kader voor ICT-risicobeheer, geldt dat het vereenvoudigd kader in grote lijnen gelijk is aan het "reguliere" kader voor ICT-risicobeheer. Net als voor het reguliere *ICT Risk Management framework*, geldt dat de vereenvoudigde variant wordt gedocumenteerd en periodiek (en in het geval van ernstige ICT-incidenten) geëvalueerd. De frequentie van de periodieke evaluatie is afhankelijk van het risicoprofiel van de instelling.

Het grootste verschil is het aantal vereisten waar het vereenvoudigd framework aan moet voldoen. Deze vereisten zijn daarnaast vaak minder gedetailleerd. De gedachte hierachter is dat het vereenvoudigd framework de elementen bevat die minimaal nodig zijn om de beschikbaarheid, intgriteit en vertrouwelijkheid van gegevens te waarborgen, terwijl rekening wordt gehouden met het risico, de omvang en de complexiteit van de onderneming. Instellingen waarvoor het vereenvoudigd kader van toepassing is, hoeven daarom enkel een informatiebeveiligingsbeleid op te stellen waarin algemene, overkoepelende richtlijnen en regels staan beschreven die de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens moeten waarborgen. Naast dit informatiebeveiligingsbeleid, moeten instellingen echter wel voldoende veiligheidsmaatregelen treffen voor onder meer logische toegangsbeheer, netwerkbeveiliging, beheer van ICT-systemen en wijzigingsbeheer (*change management*).

Om het risico van ongeautoriseerde toegang tot een minimum te beperken, moeten instellingen bijvoorbeeld procedures opstellen en implementeren waarmee de rechten van medewerkers zoveel mogelijk worden beperkt en handelingen op ICT-systemen kunnen worden herleid naar individuele gebruikers. Verder moeten organisaties een vast proces inrichten voor het toekennen, wijzigen en intrekken van rechten en dienen deze rechten periodiek te worden gecontroleerd.

Voor change management dienen organisaties eveneens een procedure op te stellen. De eisen hiervoor zijn echter beknopter dan de eisen die worden gesteld voor instellingen waar artikel 15 op van toepassing is. De vereenvoudigde change management procedure moet erop toezien dat elke wijziging aan ICT-systemen worden geregistreerd, getest, beoordeeld, goedgekeurd, geïmplementeerd en geëvalueerd.

5 Dit geldt voor kleine en niet-verweven beleggingsondernemingen, betalingsinstellingen die krachtens Richtlijn (EU) 2015/2366 zijn vrijgesteld; instellingen die krachtens Richtlijn 2013/36/EU zijn vrijgesteld en waarvoor de lidstaten hebben besloten de in artikel 2, lid 4, van deze verordening bedoelde optie niet toe te passen; instellingen voor elektronisch geld die krachtens Richtlijn 2009/110/EG zijn vrijgesteld, en kleine instellingen voor bedrijfspensioenvoorziening.

Op het gebied van netwerkbeveiliging moeten ondernemingen het netwerk zo inrichten dat systemen die verbonden zijn met het interne en/of externe netwerk voldoende zijn beschermd tegen ongewenste toegang en gegevensmisbruik. Hiervoor is het belangrijk dat maatregelen worden genomen om gegevens te beschermen (in gebruik, tijdens overdracht en in rust) en de authenticiteit, integriteit en vertrouwelijkheid te waarborgen tijdens gegevensoverdracht. Daarnaast moet worden nagedacht over hoe ongeautoriseerde toegang tot het netwerk wordt voorkomen en tijdig wordt gedetecteerd en dient er een proces te zijn voor het veilig verwijderen van gegevens.

Tot slot, dienen instellingen in het kader van het beheer van ICT-activa, alle ICT-systemen te identificeren die een belangrijke of kritische bedrijfsfunctie ondersteunen. Daarnaast moeten organisaties een procedure ontwikkelen en implementeren voor de aanschaf, ontwikkeling en onderhoud van ICT-systemen. In deze procedure is onder meer opgenomen welke eisen op het gebied van informatiebeveiliging worden gesteld en hoe ICT-systemen worden getest voordat deze in gebruik worden genomen. Hierbij is het ook belangrijk dat de *life cycle* van het ICT-systeem wordt gemonitord om ervoor te zorgen dat deze ten alle tijden voldoen aan de eisen van de organisatie.

De eisen die in de RTS voor het vereenvoudigd kader voor ICT-risicobeheer zijn opgenomen, komen dus in grote lijnen overeen met de vereisten voor het reguliere kader voor ICT-risicobeheer. Voor het vereenvoudigd *ICT Risk Management framework* zijn de gestelde eisen echter minder uitgebreid. Op deze manier wordt er rekening gehouden met de omvang van de instellingen waar artikel 16 op van toepassing is.

Tabel 3

Aanvullende uitwerkingen	Beschrijving	Afgerond
RTS voor artikel 16(3)	Simplified ICT risk management framework	Inmiddels naar EC verzonden

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 15 en 16(3)) is inmiddels voorgelegd aan de Europese Commissie ter beoordeling en besluitvorming. De tweede batch is door de ESA's voorgelegd aan ondernemingen in de financiële sector ter publieke consultatie. Deze batch zal waarschijnlijk 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 publicaties uit deze reeks zal worden ingegaan op andere onderwerpen uit de verordening. De volgende editie zal in het tweede kwartaal van 2024 worden gepubliceerd.

Voor een verdere uitwerking over *ICT Risk Management* in DORA kunnen de volgende pagina's worden geraadpleegd:
Nieuwsbericht over de eerste reeks regels voor onder andere ICT-risicobeheer (RTS) (esma.europa.eu)

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