Aftellen naar DORA, nog 1 jaar te gaan!

De Digital Operational Resilience Act (DORA) heeft als doel de digitale operationele weerbaarheid binnen de financiële sector te bevorderen. Financiële ondernemingen moeten vanaf 17 januari 2025 DORA-proof zijn. Het aftellen is dus begonnen!

Door *Joyce Kerkvliet*

DORA is van toepassing op nagenoeg alle soorten financiële ondernemingen, op een aantal kleine financiële ondernemingen na, zoals AIFMD light-beheerders en bepaalde kleine verzekeraars. Hoewel de meeste financiële ondernemingen tot op zekere hoogte bekend zijn met de regels en de verwachtingen omtrent het beheer van ICT-risico's, zal DORA verderstrekkend zijn.

Welke belangrijke vereisten vloeien voort uit DORA en wat kunnen we als voorbereiding al doen?

ICT risk management framework

Financiële ondernemingen dienen een ICT risk management framework op te stellen dat ten minste de strategieën, beleidslijnen, procedures, ICT-protocollen en instrumenten bevat die nodig zijn om alle ICT-systemen, met inbegrip van computersoftware, hardware en servers alsmede de bijbehorende fysieke infrastructuur (zoals datacentra), te beschermen tegen ICT-risico's. In dat kader zullen financiële ondernemingen aandacht moeten besteden aan de identificatie van ICT-risico's, de bescherming tegen en voorkoming van dergelijke risico's, de reactie en het herstel nadat een ICT-risico zich heeft voorgedaan, het back-up- en herstelbeleid, de scholing en ontwikkeling, alsmede de interne en externe communicatie omtrent ICT-risico's. DORA hanteert een ruime definitie van ICT-risico's: 'iedere redelijkerwijs aan te wijzen omstandigheid met betrekking tot het gebruik van ICT-systemen die, indien zij zich voordoet, de beveiliging van het ICT-systeem of afhankelijke instrumenten of processen of van de levering van de diensten in gevaar kan brengen'.

'Financiële ondernemingen moeten een strategie vaststellen met betrekking tot de risico's van ICT-dienstverleners.'

Het ICT risk management framework moet ten minste eenmaal per jaar alsmede na een ernstig ICT-gerelateerd incident of op instructie van de toezichthouder geëvalueerd worden en regelmatig worden onderworpen aan een interne audit.

ICT-incidenten

Er is sprake van een ICT-gerelateerd incident indien een gebeurtenis de beveiliging van ICT-systemen in gevaar brengt en een nadelig effect heeft op de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van gegevens, of op de door de financiële onderneming verleende diensten.

Een financiële onderneming dient deze incidenten te detecteren, te beheren en te melden aan de toezichthouder (AFM of DNB).

Bovendien zullen alle ICT-geregistreerde incidenten en cyberdreigingen moeten worden geclassificeerd en geregistreerd, mede om vast te kunnen stellen of het gaat om ernstige ICT-gerelateerde incidenten of significante cyberdreigingen. Van een ernstig ICT-gerelateerd incident is sprake indien zich grote nadelige gevolgen voordoen voor de ICT-systemen die de kritieke of belangrijke functies van de financiële onderneming ondersteunen. Deze ernstige incidenten moeten worden gerappor-

ILLUSTRATIE: SHUTTERSTOCK

‘DORA hanteert een ruime definitie van ICT-risico’s.’

teerd aan de toezichthouder. DORA schrijft een gedetailleerd rapportageproces voor: van een eerste kennisgeving tot aan een eindverslag, steeds binnen een voorgeschreven termijn.

Testen van operationele weerbaarheid

Financiële ondernemingen moeten naast een ICT risk management framework een programma opstellen voor het testen van de digitale operationele weerbaarheid van ICT-systemen. De inhoud van dit programma is afhankelijk van het vastgestelde risicoprofiel van een onderneming. Er zijn verschillende soorten tests denkbaar, waaronder kwetsbaarhedenscans, penetratietests en red teaming. Ten minste eenmaal per jaar zullen deze tests moeten worden uitgevoerd op alle ICT-systemen die kritieke of belangrijke functies ondersteunen.

De grotere financiële ondernemingen die daartoe zullen worden aangewezen, dienen bovendien ten minste om de drie jaar zogenoemde Threat-Led Penetration Tests (kort gezegd: nagebootste hacks) uit te voeren op de ICT-systemen die de kritieke of belangrijke functies van de financiële onderneming ondersteunen. De tests kunnen steeds worden uitgevoerd door interne of externe onafhankelijke personen.

Beheer van ICT-risico van derde aanbieders

Een belangrijk element van DORA heeft betrekking op de risico’s die financiële ondernemingen lopen door gebruik te maken van ICT-diensten van derden. DORA verplicht een degelijk beheer van dergelijke risico’s, ook als de ICT-dienstverlener onderdeel uitmaakt van dezelfde groep als de financiële onderneming.

De verplichtingen uit DORA richten zich op alle diensten die doorlopend (dus niet eenmalig) via ICT-systemen worden verleend.
Opvallend daarbij is dat DORA zich niet beperkt tot ICT-diensten die als uitbesteding kwalificeren, maar zich richt op alle diensten die door ICT-dienstverleners worden aangeboden. Wel maakt DORA bij deze diensten onderscheid tussen kritieke of belangrijke functies en overige functies.

Financiële ondernemingen moeten een strategie vaststellen met betrekking tot de risico’s van ICT-dienstverleners. Als onderdeel daarvan moeten financiële ondernemingen een register bijhouden met betrekking tot alle contractuele overeenkomsten met deze dienstverleners.
Ook daarbij wordt onderscheid gemaakt tussen diensten die dienen ter ondersteuning van kritieke of belangrijke functies en die dienen ter ondersteuning van overige functies. Bovendien moet de financiële onderneming ten minste jaarlijks over deze overeenkomsten rapporteren aan de toezichthouder en die vooraf informeren over het geplande gebruik van ICT-diensten die kritieke of belangrijke functies ondersteunen en wanneer functies kritiek of belangrijk zijn geworden.
De overeenkomsten met de ICT-dienstverleners moeten de in DORA voorgeschreven bepalingen bevatten, bijvoorbeeld over audits. Dit houdt ook in dat bestaande overeenkomsten met ICT-dienstverleners mogelijk moeten worden herzien.

Aanbevelingen voor de praktijk

Zoals gezegd zal DORA vanaf 17 januari 2025 van toepassing zijn. Het aftellen is nu dan ook echt begonnen en het verdient aanbeveling om voortvarend aan de slag te gaan. Ook AFM en DNB roepen hiertoe op in een reeks publicaties.

Het moment voor actie lijkt des te actueler nu begin dit jaar de eerste batch met definitieve ‘technische reguleringsnormen’ (RTS) en ‘technische uitvoeringsnormen’ (ITS) met aanvullende verplichtingen is gepubliceerd.

Ter voorbereiding op DORA kan een financiële onderneming aan de slag gaan met het ICT risk management framework, het kennisniveau bijspijkeren van bestuurders en toezichthouders (voorzover nodig), en processen, procedures en ICT-rollen evalueren. Zij kunnen in gesprek gaan met ICT-dienstverleners over de komende aanscherping van de wettelijke vereisten gericht op de overeenkomst.

ICT-dienstverleners zullen hun werkwijze ook moeten aanscherpen. Daarnaast kunnen zij afspraken maken met derde partijen over het ontvangen van de juiste assurance-rapportages voor de kritieke uitbestedingsketen. ■

Joyce Kerkvliet
Counsel bij Orange Clover

IN HET KORT

DORA heeft als doel ICT-risico’s te ondervangen voor financiële ondernemingen en zo de digitale operationele weerbaarheid te bevorderen.

DORA is van toepassing op nagenoeg alle financiële ondernemingen en richt zich op het aanscherpen van ICT risk management, ICT-incidentbeheersing, testen en toezicht op ICT-dienstverleners.

Financiële ondernemingen moeten vanaf 17 januari 2025 DORA-proof zijn.

Het is verstandig om snel aan de slag te gaan met de implementatie en het gesprek aan te gaan met ICT-dienstverleners.

FOTO: ARCHIEF ORANGE CLOVER