Auteur: Michiel Herrebrugh is Security & privacy consultant bij MichielH Services. Michiel is te bereiken via: info@michielh.nl

Hoe invulling te geven aan de eisen vanuit DORA

Grip krijgen op leveranciersrisico's

Vanaf 17 januari 2025 moeten financiële instellingen aan DORA (Digital Operational Resilience Act) voldoen. Eén van de kernpunten van DORA is het grip krijgen en houden op de volledige uitbestedingsketen. Maar wat schrijft de wet voor en hoe geeft een kleine of middelgrote financiële instelling op een praktische manier invulling aan het managen van leveranciersrisico's?

DORA bestaat uit vijf pijlers, waarvan het beheer van ICT-risico van derde aanbieders er één is. Dit laat het belang van het managen van uitbestedingsrisico's zien. De specifieke eisen zijn vastgelegd in artikelen 28 t/m 30. Artikelen 31 t/m 44 bevatten de regels rondom het overzichtskader, maar die zijn op dit moment voor financiële instellingen minder relevant.

Om aan DORA te voldoen moet een instelling de wettekst naleven (de zogenaamde level 1-eisen). Er zijn echter voor verschillende onderwerpen verdiepende technische reguleringsnormen (level 2-eisen) waar ook aan voldaan moet worden. Deze level 2-eisen zijn op het moment van schrijven nog niet goedgekeurd door de Europese Commissie, maar de (Engelstalige) conceptversies zijn wel al gepubliceerd. Op het gebied van leveranciersrisico's zijn dit:

- RTS (regulatory technical standard): Policy on ICT services performed by third parties
- ITS (implementing technical standard): Templates for the register of information
- RTS: Elements when sub-contracting critical or important functions en
- RTS: Information on oversight conduct.

Hoe invulling wordt gegeven aan de eisen vanuit DORA verschilt per toezichthouder. De Autoriteit Financiële Markten heeft in 2019 'Principes voor Informatiebeveiliging' gepubliceerd, maar deze principes zijn dusdanig generiek dat ze weinig handvatten bieden voor de implementatie van DORA. Nuttiger is de 'Good Practice Informatiebeveiliging' van De Nederlandsche Bank (DNB). In deze Good Practice staan redelijk gedetailleerde eisen waarmee aangetoond kan worden dat informatiebeveiliging op een goede manier is ingericht. Door te voldoen aan de versie uit 2023 wordt tegemoetgekomen aan een groot gedeelte van de level 1-eisen vanuit DORA.

Implementatie van de DORA-eisen

Om invulling te geven aan de eisen vanuit DORA/de Good Practice van DNB, moeten in elk geval de punten uit de onderstaande afbeelding geïmplementeerd zijn. Dit is echter geen uitputtende lijst: vanuit andere wetgeving, normenkaders of bedrijfseisen kunnen additionele activiteiten nodig zijn, zoals het uitvoeren van een Data Protection Impact Assessment (DPIA) of het aanmelden van een (ICT-)uitbesteding bij de toezichthouder.

1. Uitbestedingsbeleid

Elke financiële instelling moet een uitbestedingsbeleid – oftewel een strategie inzake ICT-risico van derde aanbieders hebben. Hierin staan de beleidsregels voor het uitbesteden van ICT-diensten. Ook moet het algemene risicoprofiel van deze ICT-diensten beoordeeld worden. Om aantoonbaar te voldoen aan de gestelde eisen, is het belangrijk om het gehele proces rondom uitbesteding te beschrijven: wat zijn de stappen die genomen moeten worden bij welk type leverancier. Dit kan onderdeel zijn van het uitbestedingsbeleid, maar kan ook in een aparte procesbeschrijving staan.

2. BIA/BIV-classificatie

Binnen de organisatie is het van belang dat er duidelijkheid is

over hoe kritisch welke bedrijfsprocessen zijn. Met een business impact analyse (BIA) of materialiteitsassessment wordt dit in kaart gebracht. Voor leveranciersmanagement is dit van belang, omdat er onderscheid gemaakt wordt tussen ICT-diensten ter ondersteuning van kritieke of belangrijke functies (hierna: kritieke ICT-diensten) en alle andere ICT-diensten (zie kader).

De BIA is ook nodig om te bepalen wat de BIV-classificatie van het systeem is of gaat worden: hoe belangrijk zijn de beschikbaarheid, integriteit en vertrouwelijkheid van het systeem en de data? Deze BIV-classificatie is nodig om in de volgende stap de securityvereisten op te stellen.

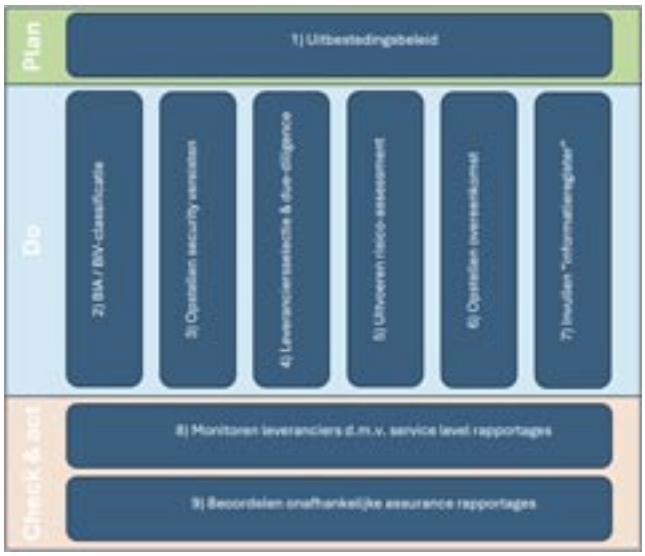
Wat zijn kritieke of belangrijke functies?
De definitie binnen DORA (artikel 2) omschrijft dit als 'een functie waarvan de verstoring wezenlijk afbreuk zou doen aan de financiële prestaties van een financiële entiteit of aan de soliditeit of de continuïteit van haar diensten en activiteiten, of waarvan de beëindiging of gebrekkige of mislukte uitvoering wezenlijk afbreuk zou doen aan de permanente naleving door een financiële entiteit van de voorwaarden en verplichtingen uit hoofde van haar vergunning of haar andere verplichtingen uit hoofde van het toepasselijke recht inzake financiële diensten.'

3. Opstellen securityvereisten

Het is belangrijk om passende securitymaatregelen te implementeren: niet te veel, maar ook niet te weinig. Om te voorkomen dat bij elke uitbesteding ad hoc bepaald wordt welke securityrequirements van toepassing zijn, helpt het hebben van een vooraf gedefinieerde maatregelenset. Hierbij kunnen de maatregelen gedifferentieerd worden naar BIV-classificatie, zoals in tabel 2 is weergegeven. De BIV-classificatie bepaalt uiteindelijk welke beheersmaatregelen contractueel afgesproken worden met de leverancier, zodat de maatregelen passen bij het risicoprofiel van de uitbestede dienst.

4. Leverancierselectie & due diligence

Wanneer de (security)requirements duidelijk zijn, kan gezocht worden naar een geschikte leverancier. DORA schrijft niet voor hoe de meest geschikte leverancier geselecteerd moet worden, maar er wordt wel van de financiële instelling verwacht dat er passend (due diligence)onderzoek gedaan wordt. Ook moet



Figuur 1: DORA verplichtingen leveranciersmanagement.

beoordeeld worden of aan de toezichtvoorwaarden voor het sluiten van het contract is voldaan en of er eventueel belangenconflict kan voortkomen uit de overeenkomst.

5. Uitvoeren risico-assessment

De wetgever stelt specifieke eisen aan het uitvoeren van een risico-assessment voorafgaand aan het uitbesteden van ICT-diensten. Alle relevante risico's met betrekking tot de overeenkomst moeten in kaart gebracht worden, waarbij in het geval van kritieke ICT-diensten tenminste een aantal specifieke risico's moeten terugkomen:

- Concentratierisico: in hoeverre is de leverancier vervangbaar; en ontstaat er geen kritische afhankelijkheid door te veel diensten bij dezelfde leverancier af te nemen?
- Onderuitbesteding: wat betekent het voor de instelling als de dienstverlener bepaalde ICT-diensten verder uitbesteedt, met name naar onderaannemers in het buitenland? Wat is de impact van potentieel lange of complexe uitbestedingsketens op het vermogen van de financiële instelling om de contractuele afspraken te monitoren?
- Insolventie & faillissement: wat is het risico als een ICT-dienstverlener niet meer aan zijn financiële verplichtingen kan voldoen en kan de instelling dan nog zijn gegevens herstellen?
- Privacy: worden de Europese privacyregels nageleefd bij uitbesteding naar het buitenland?

Om de risico's te kunnen mitigeren, moeten potentiële leveranciers hun volledige onderuitbestedingsketen inzichtelijk maken,

Hoe geeft een kleine of middelgrote financiële instelling invulling aan het managen van leveranciersrisico's?

Beschikbaarheid	**Laag**	**Midden**	**Hoog**
- Beschikbaarheidspercentage	80%	90%	99,9%
- Uitwijkbaarheid	N.v.t.	Cold standby	Hot standby
- Uitwijktesten	Geen	Tweejaarlijks	Jaarlijks
Vertrouwelijkheid	**Laag**	**Midden**	**Hoog**
- Encryptie	Encryption in transit	Encryption in transit + rest	Encryption in transit + rest
- Authenticatie	Username + password	Username + password	MFA
- Authenticatie beheerders	Username + password	MFA	MFA

Tabel 1: Voorbeeld beveiligingsmaatregelen per classificatieniveau voor beschikbaarheid en vertrouwelijkheid.

inclusief de wijze waarop zij de relevante risico's beheersen die aanwezig zijn bij die onderleveranciers.

Na het bepalen van de risico's kunnen mitigerende maatregelen bepaald en afgesproken worden. Ook kan blijken dat de uitbesteding toch niet door mag gaan, omdat het een onacceptabel risico oplevert voor de instelling.

6. Opstellen overeenkomst

Wanneer duidelijk is of een ICT-dienst een kritieke of belangrijke functie ondersteunt, de BIV-classificatie en bijbehorende beheersmaatregelen duidelijk zijn, de leverancier is geselecteerd en de gedefinieerde risico's beheersbaar zijn, kan overgegaan worden tot het opstellen van de overeenkomst. DORA stelt expliciete eisen aan deze overeenkomst: er wordt een negental punten beschreven die in elke uitbestedingsovereenkomst van ICT-diensten moeten terugkomen. Daarnaast zijn er zes verplichtingen voor contracten met leveranciers van kritieke ICT-diensten.

Twee punten die het benadrukken waard zijn: (1) het hebben van een exitstrategie en (2) het uitvoeren van threat led penetration testing.

1) Een financiële instelling moet een redelijke mate van zekerheid hebben dat het beëindigen van een overeenkomst kan gebeuren zonder dat dit leidt tot een verstoring van de bedrijfsactiviteiten of de dienstverlening naar klanten. Hiervoor moet een exitstrategie zijn beschreven in de afspraken met de leverancier en moet deze periodiek geëvalueerd worden.
2) Threat led penetration testing, of dreigingsgestuurde penetratietest, gaat verder dan normale penetratietesten. Hierbij worden realistische aanvalsscenario's van bestaande actoren nagebootst, waarbij de test zich niet beperkt tot één specifiek systeem. Artikelen 26 en 27 beschrijven de eisen rondom deze testen.

7. Invullen informatieregister

Elke financiële instelling is verplicht om een informatieregister te hebben met daarin informatie over alle contractuele overeenkomsten rondom uitbestede ICT-diensten en de ICT-leveran-

Eisen voor elke overeenkomst rondom uitbestede ICT-diensten	Aanvullende eisen aan contracten met leveranciers van kritieke ICT-diensten
1. Beschrijving van alle te leveren functies en diensten, inclusief eisen en voorwaarden aan onderuitbesteding van een kritieke ICT-dienst 2. De locatie waar de diensten moeten worden geleverd en waar de gegevens moeten worden verwerkt. De financiële instelling moet geïnformeerd worden voorafgaand aan het veranderen van de locatie 3. Beveiligingsbepalingen rondom de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid 4. Afspraken over de toegang tot, het herstel van en de teruggave van data in het geval de overeenkomst -om wat voor reden dan ook- wordt beëindigd (inclusief bij insolventie/faillissement) 5. Beschrijvingen van het dienstenniveau 6. De verplichting dat de ICT-dienstverlener bij een incident kosteloos, of tegen een vooraf bepaalde prijs, bijstand verleent 7. De verplichting dat de ICT-dienstverlener volledige medewerking verleent aan de toezichthouder(s) van de financiële entiteit 8. Het recht om een dienst te beëindigen en de bijbehorende minimumopzegtermijn 9. Afspraken over deelname aan bewustwordingsactiviteiten van de financiële instelling door medewerkers van de ICT-dienstverlener (waar relevant)	a. Nauwkeurige kwantitatieve en kwalitatieve prestatiecriteria, zodat de financiële instelling monitoringsactiviteiten kan uitvoeren (ter aanvulling op punt 5) b. De verplichting van de ICT-leverancier om de financiële instelling te informeren over ontwikkelingen die impact kunnen hebben op de naleving van de Service Level Agreements c. De verplichting van de ICT-leverancier om bedrijfscontinuïteitsplannen te hebben en te testen; en om beveiligingsmaatregelen te hebben geïmplementeerd die passend zijn d. De verplichting van de ICT-leverancier om deel te nemen aan threat led penetration testing (TLPT) e. Het recht om de prestaties van de ICT-leverancier te monitoren, inclusief: i. Het recht op onbeperkte toegang, inspectie en audit door zowel de financiële instelling als de toezichthouder, inclusief het recht om ter plaatse kopieën te maken van relevante documentatie en de plicht van de ICT-dienstverlener om daaraan mee te werken ii. Het recht om andere garantieniveaus af te spreken indien de rechten van andere klanten worden aangetast iii. De verplichting voor de ICT-dienstverlener om gedetailleerde informatie te verstrekken over waar, hoe en hoe vaak de audits plaatsvinden f. Er moet een exitstrategie afgesproken zijn

Tabel 2: DORA eisen aan contracten.

ciers. Dit register moet voldoen aan de eisen zoals beschreven in de ITS Templates for the register of information. Er is een Excel-template beschikbaar gesteld die gebruikt kan worden voor het informatieregister (1).

In het template valt op dat er relatief veel informatie gevraagd wordt, zeker voor een kleine of middelgrote financiële instelling. Het document correct invullen is echter van belang, omdat het register opgevraagd mag worden (en naar verwachting zál worden) door de toezichthouder. Het template helpt daarnaast om invulling te geven aan alle level-2 eisen die gesteld worden vanuit de bovengenoemde ITS.

8. Monitoren d.m.v. service level rapportages

Zoals onder punt 6 beschreven staat, moeten er in contracten afspraken gemaakt worden over service levels (eis 5) en moeten er – in geval van kritieke ICT-diensten – kwalitatieve en kwantitatieve prestatiecriteria worden opgesteld (eis a). Het is van belang om deze prestatiecriteria breder te formuleren dan enkel de beschikbaarheidseisen en operationele reactietijden bij incidenten en problemen: specifiek op het vlak van informatiebeveiliging en cyberweerbaarheid kunnen prestatiecriteria over analyse en reactietijden op Indicators of Attack of Indicators of Compromise bijdragen aan het vaststellen of een leverancier de benodigde volwassenheid heeft.
De financiële instelling moet – mede door middel van service

level rapportages – grip houden op de dienstverlening door de leverancier van kritieke ICT-diensten. Daarnaast helpt het periodiek overleggen met leveranciers om het vermogen om effectief samen te werken regelmatig te evalueren en een goede relatie op te bouwen: deze relatie is misschien wel het belangrijkste middel om risico's te mitigeren.
De rapportages moeten worden geanalyseerd en over de uitkomsten hiervan moet worden gerapporteerd aan het verantwoordelijke lijnmanagement. Op deze manier houdt de financiële instelling toezicht op (de betrouwbaarheid van) de volledige uitbestedingsketen van kritieke ICT-diensten.

9. Beoordelen onafhankelijke assurancerapportages

Elke financiële instelling is verantwoordelijk voor het voldoen aan de eisen vanuit DORA, ook wanneer ICT-diensten uitbesteed worden. Daarbij is het niet voldoende om te vertrouwen op beloftes van een leverancier: naleving van de eisen moet aantoonbaar zijn. De meest gebruikelijke en efficiënte manier om dit te doen is door onafhankelijke assurancerapportages op te vragen bij de leverancier en deze te beoordelen. Hierbij is een ISO 27001 certificering niet voldoende: er moet aangetoond worden dat beveiligingsmaatregelen effectief werken over een langere periode, bijvoorbeeld door middel van een ISAE 3402 type 2 of een SOC-2 type 2 verklaring. Deze vereiste geldt ook voor onderleveranciers.
Bij het beoordelen van een assuranceverklaring zijn twee aandachtspunten van belang:

1. Zijn alle subcontractors in scope van de verklaring?
Vaak worden onderleveranciers niet meegenomen bij de uitspraken over effectieve beheersmaatregelen (carve-out). Aangezien elke financiële instelling de gehele uitbestedingsketen moet monitoren, is het – als onderleveranciers niet in scope zijn – nodig om assuranceverklaringen bij de onderleveranciers op te vragen en te beoordelen. Het is dus effectiever om met een ICT-leverancier af te spreken dat ook de onderleveranciers meegenomen worden in de rapportage.

2. Zijn alle relevante beveiligingsmaatregelen in scope van de verklaring?
Niet elke assuranceverklaring heeft dezelfde scope. Een financiële instelling moet de zekerheid hebben dat alle relevante beveiligingsmaatregelen getest en effectief bevonden zijn. Welke beveiligingsmaatregelen relevant zijn, kan verschillen per type leverancier (zie onderstaande tabel). Door hier van tevoren over na te denken, kunnen vergelijkbare ICT-leveranciers op een vergelijkbare manier beoordeeld worden. Het is aan te bevelen om ruimte te houden om, wanneer nodig, af te wijken van de standaardmapping, waarbij afwijkingen naar een lager niveau wel eerst voorgelegd moeten worden aan een (C)ISO of tweedelijns riskfunctionaris.

	SaaS leverancier	Data-center	Software-ontwikkelaar
Screening (DNB 08.4)	X	X	X
Secure coding (DNB 10.1)	X	-	X
Uitwijktesten (DNB 11.2)	X	X	-
Fysieke beveiliging (DNB 21.1 & 21.2)	-	X	-

Tabel 3: Voorbeeld mapping DNB normen - type leverancier.

Vervolgens kan voor elk van de relevante maatregelen vastgesteld worden of de assuranceverklaring een uitspraak doet over de effectiviteit van de maatregel. Leg deze beoordeling, inclusief eventuele afwijkingen/uitzonderingen en verbeteracties, vast om aan te tonen dat de financiële instelling invulling geeft aan deze wettelijke verplichting.

Naderende deadline

Vanaf 17 januari 2025 moet elke financiële instelling voldoen aan DORA. Wacht dus niet te lang met de implementatie van de vereisten. Dit artikel draagt er hopelijk aan bij om duidelijk te krijgen wat gedaan moet worden om aan artikelen 28 t/m 30 van DORA te voldoen. De wetgeving is echter breder dan alleen die artikelen en dusdanig uitgebreid en specifiek dat het onmogelijk is om alle verplichtingen in één artikel te beschrijven. Neem dus ook de tijd om zelf de wetgeving en de onderliggende technische reguleringsnormen erop na te slaan om goed in kaart te brengen wat er moet gebeuren om aan deze nieuwe wetgeving te voldoen.

Referentie

(1) https://www.eiopa.europa.eu/publications/set-rules-under-dora-ict-and-third-party-risk-management-and-incident-classification_en