TOEZICHT DORA UPDATE 5

Aan de slag met DORA: Testen van de digitale operationele weerbaarheid

In het kort Dit is de vijfde 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 testen van de digitale operationele weerbaarheid. 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. Inleiding

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 testen van de digitale operationele weerbaarheid. 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.

In de vorige edities zijn de DORA-vereisten behandeld voor het beheren van ICT-risico's (waaronder van derde aanbieders) en het beheer van ICT-incidenten. DORA verwacht van financiële instellingen dat zij hiervoor voldoende maatregelen nemen en processen inrichten die de informatiebeveiliging en cyberweerbaarheid helpen te verbeteren. Om te waarborgen dat deze maatregelen voldoen, is het belangrijk dat de ICT-instrumenten en -systemen regelmatig worden getest om eventuele kwetsbaarheden en gebreken bloot te leggen. Door regelmatig de weerbaarheid van ICT-instrumenten en -systemen te testen, kunnen ondernemingen de continuïteit van belangrijke en kritieke functies waarborgen in het geval van een verstoring. De vereisten voor het testen van de digitale operationele weerbaarheid worden beschreven in artikel 24 tot en met 27 (hoofdstuk IV) van de verordening. Artikel 24 beschrijft de algemene vereisten die gelden voor het uitvoeren van tests. Hierin wordt onder meer beschreven hoe organisaties een testprogramma moeten opstellen, hoe vaak de tests moeten worden uitgevoerd en hoe bevindingen moeten worden opgevolgd. Deze vereisten gelden voor alle ondernemingen die onder DORA vallen, met uitzondering van micro-ondernemingen[1]. Van micro-ondernemingen wordt verwacht dat zij een risicogebaseerde aanpak hanteren. In artikel 25 wordt beschreven welke tests kunnen worden gebruikt voor het testen van ICT-instrumenten en -systemen.

Artikel 26 en 27 van de verordening beschrijven de vereisten van geavanceerde tests op basis van *threat-led penetration test* (TLPT), waarbij meerdere belangrijke of kritieke functies worden getest (in de productieomgeving). Deze artikelen beschrijven onder andere de scope van deze tests, de rol van de toezichthouders en hoe wordt bepaald welke financiële instellingen TLPT moeten uitvoeren. Daarnaast

1 Een financiële entiteit die geen handelsplatform, centrale tegenpartij, transactieregister of centrale effectenbewaarinstelling is, en waar minder dan 10 personen werkzaam zijn en waarvan de jaaromzet en/of het jaarlijkse balanstotaal niet hoger liggen dan €2 miljoen

AFM

worden de vereisten voor de testers beschreven voor het uitvoeren van TLPT. De vereisten voor TLPT zijn verder uitgewerkt in de *Regulatory Technical Standard* (RTS)[2]. Hierin staat in meer detail beschreven op basis van welke criteria ondernemingen kunnen worden aangewezen voor TLPT en welke vereisten er gelden voor het gebruik van interne testers. Daarnaast wordt in de RTS het proces van TLPT uitgelegd. Dit proces is gebaseerd op het TIBER-EU framework. De AFM begeleidt al sinds 2021, in samenwerking met DNB, TIBER-tests bij financiële ondernemingen[3].

In deze DORA-update gaan we dieper in op de algemene vereisten voor het testen van de digitale operationele weerbaarheid en waar organisaties nu al mee zouden starten om aan DORA te kunnen voldoen. Ook bespreken we de vereisten rond TLPT en het proces van zulke tests.

Tabel 1

Aanvullende uitwerkingen	Onderwerp	Afgerond
RTS voor artikel 26 (11)	Advanced testing of ICT tools, systems and processes based on TLPT	Inmiddels naar EC verzonden

2 Zie Regulatory Technical Standards (RTS) en Implementing Technical Standards (ITS)

3 Zie TIBER-NL-programma (afm.nl)

2. Aan de slag met het testen van de digitale operationele weerbaarheid

Testen van ICT-instrumenten en -systemen

Ondernemingen kunnen nu al aan de slag met:
- Het opstellen van een risicogebaseerd programma voor het testen van de digitale operationele weerbaarheid;
- Het uitvoeren van het testprogramma.

In artikel 24 van de verordening staan de algemene vereisten voor het testen van de digitale operationele weerbaarheid beschreven. Om op een structurele manier de weerbaarheid van de ICT-systemen en -diensten te kunnen beoordelen, moeten ondernemingen een testprogramma opstellen, uitvoeren en regelmatig evalueren. Dit testprogramma dient onderdeel te zijn van het I*CT risk management framework*[4] en bevat de tests, praktijken, methodologieën en instrumenten die regelmatig worden uitgevoerd om de ICT-systemen, -instrumenten en -processen van de organisatie te beoordelen. Bij de beoordeling wordt gekeken naar de processen die zijn ingericht om ICT-gerelateerde incidenten tijdig te detecteren en af te handelen. Daarnaast moeten ondernemingen zelf beoordelen in hoeverre zij in staat zijn om kwetsbaarheden en gebreken in de digitale weerbaarheid te herkennen. Tot slot geven de tests inzicht in hoeverre de organisatie tijdig herstellende maatregelen kan implementeren die de duur en impact van een verstoring tot een minimum beperken. Bij het bepalen van de tests moet de onderneming onder meer rekening houden met het (veranderende) landschap van ICT-risico's, specifieke ICT-risico's voor de onderneming en de kritieke aard van de ICT-systemen en -diensten.

Van organisaties wordt verwacht dat zij minimaal één keer per jaar hun ICT-systemen en -toepassingen testen die kritieke of belangrijke functies ondersteunen. Deze tests kunnen zowel door interne als externe testers worden uitgevoerd. Hierbij is het belangrijk dat (potentiële) belangenconflicten gedurende de ontwerp- en uitvoeringfase van de test worden voorkomen. Wanneer gebruik wordt gemaakt van interne testers, treffen de ondernemingen voldoende maatregelen om te waarborgen dat de testers geen belang hebben bij het resultaat van de tests. Verder moeten financiële instellingen beleid en procedures opstellen om alle tekortkomingen, die tijdens de uitvoering van de tests naar voren zijn gekomen, te classificeren, te prioriteren en op te volgen. Hierbij moeten zij ook nagaan of alle vastgestelde kwetsbaarheden en gebreken volledig zijn aangepakt.

Artikel 25 van de verordening beschrijft de tests die ondernemingen kunnen uitvoeren om hun ICT-systemen en -toepassingen te testen. Hierbij bepalen ondernemingen overeenkomstig het evenredigheidbeginsel[5] welke tests relevant zijn. Voorbeelden van tests zijn:
- *Vulnerability scans*. Hierbij wordt de beveiliging van ICT-systemen en -instrumenten beoordeeld en worden kwetsbaarheden (vaak via geautomatiseerde scans) geïdentificeerd;
- *Gap analyses*, waarbij de huidige staat van de ICT-systemen en -instrumenten wordt vergeleken met de gewenste staat. Op basis van deze analyses kan worden bepaald welke systemen wel en niet voldoen aan de vereisten;
- Beoordelingen van de fysieke beveiliging. Denk hierbij aan tests om vast te stellen of mensen ongeautoriseerd toegang kunnen krijgen tot bepaalde locaties (zoals kantoren, datacenters, etc.);
- Beoordelingen van broncodes waarbij ontwikkelaars, die de code niet zelf hebben geschreven, de broncode controleren voordat deze

4 Voor meer informatie over het ICT risk management framework, zie DORA update 3 (Publicaties (afm.nl))

5 De vereisten in hoofdstuk IV van de verordening moeten worden toegepast in verhouding tot de omvang en algehele risicoprofiel van de onderneming en tot de aard, schaal en complexiteit van hun diensten, activiteiten en verrichtingen.

naar de productieomgeving gaat;
- Compatibiliteitstests: een vorm van testen waarbij de werking van de software wordt getest in verschillende omgevingen (software/hardware platforms, netwerken, browsers, etc.);
- *End-to-end testing*: een vorm van testen waarbij de applicatie van begin tot eind wordt getest om te verifiëren dat alle componenten ook werken in realistische scenario's;
- Penetratietests: tests waarbij de (vaak externe) tester gebruik probeert te maken van kwetsbaarheden om toegang te krijgen tot het systeem.

Bovenstaande vereisten zijn niet van toepassing op micro-ondernemingen. Voor micro-ondernemingen geldt een op risico's gebaseerde aanpak waarbij enerzijds rekening wordt gehouden met de hoeveelheid middelen en tijd die nodig zijn voor het uitvoeren van de tests en anderzijds de urgenties, het soort risico, de kritieke aard van het ICT-systeem en eventuele andere relevante factoren.

Geavanceerde tests van ICT-instrumenten, -systemen en -processen

Voor een aantal ondernemingen gelden, naast de (algemene) vereisten voor het testen van ICT-systemen en -instrumenten, extra vereisten met betrekking tot het testen van de digitale operationele weerbaarheid. Deze instellingen moeten één keer in de drie jaar[6] een geavanceerde test uitvoeren door middel van *threat-led penetration test* (TLPT). TLPT betreft een uitgebreide test waarin de tactieken, technieken en procedures die in de praktijk worden gebruikt door dreigingsactoren (zoals hackers), worden nagebootst[7]. Hierdoor wordt op een gecontroleerde, instellingsspecifieke en door inlichtingen gestuurde wijze, de cyberweerbaarheid van de financiële instelling getoetst. Een dergelijke test vormt een uitgebreidere vorm van *red-teaming*, mede door de betrokkenheid van de toezichthouder.

Om TLPT succesvol te kunnen uitvoeren, is het belangrijk dat de onderneming deze test ziet als een mogelijkheid om te leren en eventuele kwetsbaarheden bloot te leggen. Daarnaast is TLPT veeleisend, waardoor het belangrijk is dat ondernemingen voldoende middelen en personeel vrijmaken gedurende de verschillende fases van de test.

Elke TLPT dient betrekking te hebben op de kritieke of belangrijke bedrijfsfuncties van de onderneming en moet worden uitgevoerd op de (live) productiesystemen die deze bedrijfsfuncties ondersteunen. Hiervoor is het belangrijk om eerst de ICT-systemen, -processen, -instrumenten en (uitbestede) -diensten te identificeren die kritieke of belangrijke functies ondersteunen. Vervolgens bepaalt de onderneming welke kritieke of belangrijke functies onderdeel moeten zijn van de test. Voordat de reikwijdte van de test definitief kan worden gemaakt, moet deze worden gevalideerd door de TLPT-autoriteit die de test begeleidt. In Nederland zal dit, afhankelijk van de toezichthouder die de vergunning verleent, worden gedaan door de AFM of DNB.

Wanneer derde aanbieders van ICT-diensten binnen de reikwijdte van een TLPT vallen, neemt de onderneming voldoende maatregelen om deelname van de derde aanbieders aan TLPT te waarborgen. In het geval dat deelname aan TLPT een negatief effect zal hebben op de kwaliteit van de dienstverlening van de derde aanbieder aan organisaties die niet onder DORA vallen, kan de externe dienstverlener buiten scope van de TLPT van de onderneming worden gelaten. In dat geval moet de derde aanbieder zelf een externe tester aanwijzen die een gebundelde TLPT (of *pooled test*) uitvoert, waarbij meerdere financiële instellingen, waaraan ICT-diensten worden verleend, betrokken zijn. Deze gebundelde test dient alle ICT-diensten te dekken die zijn uitbesteed aan de derde partij en kritieke of belangrijke functies van de verschillende financiële entiteiten ondersteunen.

Om te kunnen waarborgen dat de TLPT correct wordt uitgevoerd, gelden er een aantal vereisten voor de testers (of *red team*). Ondernemingen moeten gebruik maken van testers die in een lidstaat zijn gecertificeerd door een certificeringsorgaan en/of formele gedragscodes/ethische kaders naleven. Daarnaast moeten testers over

6 De toezichthouder heeft de bevoegdheid deze frequentie te verhogen of te verlagen.

7 Voor het opstellen van de TLPT-vereisten in DORA, is het TIBER-EU raamwerk als basis gebruikt (zie ook What is TIBER-EU? (europa.eu)).

voldoende technische en organisatorische capaciteiten beschikken en kunnen laten zien dat zij relevante kennis hebben op het gebied van inlichtingen over dreigingen, penetratietests en *red-teaming*. Tot slot moeten testers de onafhankelijke uitvoering van de test en de vertrouwelijkheid van informatie (zoals testresultaten) kunnen waarborgen. In het geval dat interne testers worden gebruikt, zet de onderneming bovendien voldoende middelen in om belangenconflicten tegen te gaan en moet het gebruik van interne testers worden goedgekeurd door de TLPT-autoriteit die de test begeleidt. De vereisten voor het gebruik van interne testers zijn verder uitgewerkt in hoofdstuk IV van de RTS.

Voor de aanwijzing van ondernemingen die TLPT moeten uitvoeren, bepaalt de TLPT-autoriteit welke financiële entiteiten aangewezen worden om TLPT te verrichten. Afhankelijk van de vergunningsverlening zal de AFM of DNB verantwoordelijk zijn voor de aanwijzing (en begeleiding) van TLPT. Sommige financiële instellingen kunnen door zowel de AFM als DNB worden aangewezen. In dat geval kan worden besloten dat een gezamenlijke test wordt uitgevoerd, waarbij beide toezichthouders zijn betrokken. De criteria voor het aanwijzen van ondernemingen zijn beschreven in hoofdstuk II van de RTS. De TLPT-autoriteit houdt hierbij rekening met proportionaliteit. Instellingen kunnen worden aangewezen voor TLPT op basis van 'harde (of kwantitatieve) criteria'. Hieronder vallen bijvoorbeeld handelsplatformen met een bepaald marktaandeel op nationaal of Europees niveau. Deze harde criteria zijn beschreven in artikel 2, lid 1 van de RTS. Instellingen die niet op basis van de kwantitatieve criteria worden aangewezen, kunnen alsnog worden aangewezen om verplicht TLPT uit te voeren op basis van hun ICT-risicoprofiel, systemisch karakter en impact op de stabiliteit van de financiële sector. Meer concreet kunnen instellingen worden aangewezen op basis van de volgende (overwegend kwalitatieve) factoren:

- Systemisch karakter en impact gerelateerde factoren:
  - De omvang van de instelling;
  - De mate en aard van de verwevenheid van de instelling met andere financiële instellingen in de financiële sector;
  - Het belang van de diensten die worden aangeboden;
  - De vervangbaarheid van de diensten die worden aangeboden;
  - De complexiteit van het businessmodel van de instelling;
  - Of de instelling onderdeel is van een groep waarbij gedeelde ICT-systemen worden gebruikt.

- ICT-risico gerelateerde factoren:
  - Het risicoprofiel en dreigingslandschap van de instelling;
  - De mate van afhankelijkheid van kritische, belangrijke of ondersteunende bedrijfsfuncties van ICT-systemen en processen;
  - De complexiteit van de ICT-architectuur van de instelling;
  - Uitkomsten van eventuele toezichtonderzoeken die relevant zijn voor de beoordeling van de ICT-volwassenheid van de financiële entiteit;
  - De volwassenheid van *ICT business continuity plans* en ICT-herstel- en responsplannen;
  - De volwassenheid van de operationele ICT-beveiligingsdetectie- en mitigatiemaatregelen;
  - Of de instelling onderdeel is van een groep waarbij gedeelde ICT-systemen worden gebruikt.

Tot slot kunnen micro-ondernemingen en ondernemingen waarvoor het vereenvoudigd *ICT risk management framework*[8] geldt, niet worden aangewezen voor TLPT. In de volgende sectie zullen we dieper ingaan op het proces rond TLPT en de verschillende rollen van de betrokken partijen.

Tabel 2

Aanvullende uitwerkingen	Beschrijving	Afgerond
RTS voor artikel 26 (11)	Advanced testing of ICT tools, systems and processes based on TLPT	Inmiddels naar EC verzonden

8 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 DORA bedoelde optie niet toe te passen; instellingen voor elektronisch geld die krachtens Richtlijn 2009/110/EG zijn vrijgesteld, en kleine instellingen voor bedrijfspensioenvoorziening.

TLPT-proces

Om te kunnen waarborgen dat elke TLPT correct wordt uitgevoerd, zijn er een aantal vereisten met betrekking tot de testmethodologie en het TLPT-proces uitgewerkt in hoofdstuk III van de RTS. Om te beginnen, beoordelen ondernemingen de risico's die gepaard gaan met de uitvoering van TLPT. Er moeten voldoende maatregelen worden genomen om te voorkomen dat deze risico's zich materialiseren als gevolg van de uitvoering van de testwerkzaamheden. Hierbij gaat het om risico's met betrekking tot:

- het verlenen van toegang aan externe partijen tot gevoelige gegevens;
- het niet voldoen aan de vereisten rond TLPT;
- *crisis/incident management*;
- verstoringen in kritische activiteiten en processen;
- het verlies van data als gevolg van de testwerkzaamheden;
- het niet volledig herstellen van systemen die zijn getroffen door de test.

Voordat de testwerkzaamheden kunnen worden uitgevoerd, moet duidelijk zijn wat de rol is van iedereen die betrokken is bij de uitvoering van de TLPT. Vanuit de autoriteit die de TLPT begeleidt (bijvoorbeeld de AFM of DNB), dient er een testmanager te worden aangewezen die de testwerkzaamheden begeleidt en zorgt dat tijdens de uitvoering wordt voldaan aan alle vereisten. Daarnaast wordt ten minste één plaatsvervanger aangewezen die de taken van de testmanager kan overnemen indien dit nodig is. Van de autoriteit die de TLPT begeleidt, wordt verwacht dat deze bij alle fasen van de testwerkzaamheden betrokken is en tijdig feedback, validatie of goedkeuring geeft wanneer dit nodig is.

De onderneming moet zelf zorgen dat zij beschikt over een team met medewerkers die betrokken zijn bij de uitvoering van de test (het *control team* of *white team*), waarvan één iemand is aangewezen als teamleider. Het control team wordt op de hoogte gehouden van elke bevinding die uit de TLPT voortkomt. Dit geldt voor bevindingen van zowel de personeelsleden binnen de eigen organisatie als door de externe dienstverleners. Eventuele opvolgacties voor incidenten die voortkomen uit de test, worden door het team zelf opgepakt en informatie over de voortgang van de testwerkzaamheden moet worden gedeeld met de testmanagers wanneer hierom wordt gevraagd.

Tot slot moeten voldoende maatregelen worden genomen om de geheimhouding van de TLPT te waarborgen. Zo wordt de toegang tot informatie over de TLPT worden beperkt tot het *control team*, het bestuursorgaan van de onderneming, de TLPT-autoriteit, de aanbieders van *threat intelligence* en de testers. Hierbij zijn de aanbieders van *threat intelligence* externe specialisten die data verzamelen en analyseren over actuele dreigingen en op basis hiervan realistische scenario's ontwikkelen. De testers bestaan uit (externe) ethische hackers (of *red team*) die toegang tot de productiesystemen van de onderneming proberen te krijgen. Het *blue team* zijn medewerkers van de onderneming zelf, die het netwerk en de ICT-systemen proberen te beschermen tegen aanvallen van buitenaf. Het *blue team* wordt niet betrokken bij de test en is daarom niet op de hoogte van de test.

Voorbereidingsfase

Zodra de onderneming een notificatie ontvangt van de TLPT-autoriteit, kan de onderneming beginnen met de voorbereiding van de test. Tijdens de voorbereidingsfase voert de onderneming de risicobeoordeling uit, waarbij wordt gekeken naar de naar de risico's die gepaard gaan met het uitvoeren van een test op de productieomgeving van systemen die belangrijke en kritische bedrijfsfuncties ondersteunen. Daarnaast moeten voor de aanvang van de test een projectcharter[9], de contactgegevens van de teamleider van het *control team* en informatie over het gebruik van interne of externe testers worden aangeleverd bij de TLPT-autoriteit. Verder wordt informatie gedeeld met de TLPT-autoriteit over de communicatiekanalen tijdens de uitvoering van de testwerkzaamheden en de codenaam die wordt gebruikt voor de test. Deze informatie moet uiterlijk drie maanden na de notificatie van de TLPT-autoriteit worden gedeeld met de testmanagers. Ondernemingen die door de AFM zijn aangewezen voor TLPT, kunnen de benodigde rapportages indienen via het AFM-portaal [10]. Zodra deze

9 Zie de Annex I van de RTS voor de inhoud van het projectcharter

10 In DORA update 4 staat beschreven hoe ondernemingen vanaf 17 januari 2025 toegang kunnen krijgen tot het AFM-portaal

documentatie is goedgekeurd door de testmanagers, kan de onderneming het *control team* opzetten die de teamleider ondersteunt met het voorbereiden van de test.

Wanneer de samenstelling van het *control team* is goedgekeurd door de TLPT-autoriteit, bepaalt de onderneming welke kritische en belangrijke bedrijfsfuncties worden meegenomen in de uitvoering van de testwerkzaamheden. Hierbij wordt onder meer rekening gehouden met het belang van de functie voor de onderneming en de stabiliteit van de financiële sector, de vervangbaarheid van de functie, de verwevenheid met andere functies en de geografische locatie van de functie. Wanneer de reikwijdte van de test is bepaald, moet deze worden goedgekeurd door het bestuursorgaan en worden gedeeld met de testmanagers[11]. Deze rapportage wordt uiterlijk zes maanden na de notificatie van de TLPT-autoriteit gedeeld. Wanneer de ingediende rapportages zijn goedgekeurd door de testmanagers, kunnen deze worden gedeeld met de testers en aanbieders van *threat intelligence*. De onderneming zorgt ervoor dat zowel het *red team* als de aanbieders van *threat intelligence*, zijn gecontracteerd voor de aanvang van de testfase.

Testfase

De testfase kan worden onderverdeeld in twee onderdelen: *threat intelligence* en *red-teaming*. Wanneer de scope van de test is goedgekeurd door de TLPT-autoriteit, moet de aanbieder van de *threat intelligence* onderzoek doen naar de onderneming en dreigingen en kwetsbaarheden die relevant zijn voor de onderneming. Tijdens dit onderzoek verzamelen zij data door cyberdreigingen in de sector te identificeren en te analyseren en bestaande en potentiële kwetsbaarheden te identificeren die kunnen worden uitgebuit tijdens de test. Voor deze stap kunnen de aanbieders van *threat intelligence* overleggen met het *control team* en de testmanagers die de test begeleiden.
Op basis van deze analyse zal de aanbieder van de *threat intelligence* een aantal scenario's opstellen die kunnen worden gebruikt bij de uitvoering van de test. Vervolgens selecteert de teamleider van het *control team* ten minste drie van deze scenario's op basis van de aanbeveling van de aanbieder van de threat intelligence, de input van de testmanagers, de haalbaarheid van de voorgestelde scenario's tijdens de uitvoering en de grootte, complexiteit en risicoprofiel van de onderneming. De analyse van de aanbieder van threat intelligence moet worden opgenomen in een rapport en worden gedeeld met de testmanagers[12].

Wanneer het *threat intelligence* rapport is goedgekeurd door de testmanagers, kunnen de testers (*red team*) beginnen met het opstellen van hun testplan[13]. Het testplan bevat onder meer de tactieken, technieken, procedures en communicatiekanalen die worden gebruikt tijdens de uitvoering van de test. Wanneer het testplan is opgesteld, moet deze worden besproken met het *control team*, de testmanagers en de aanbieder van *threat intelligence*, voordat het *control team* en de testmanagers het plan kunnen goedkeuren. Na deze goedkeuring kunnen de testers starten met hun testwerkzaamheden. De duur van deze testwerkzaamheden is onder andere afhankelijk van de scope, de schaal en de activiteiten. De test duurt echter minimaal twaalf weken. Tijdens de uitvoering van het testplan komen de testers, testmanagers en het *control team* ten minste wekelijks bijeen om de voortgang te bespreken. Wanneer de testwerkzaamheden worden opgemerkt door medewerkers van de onderneming, neemt het *control team*, in overleg met de testers, maatregelen om de geheimhouding van de test te waarborgen. Deze maatregelen moeten vervolgens ook met de testmanagers worden gedeeld. In het geval dat de testers het punt bereiken dat doorgaan met de test kan leiden tot ernstige verstoringen in kritische of belangrijke bedrijfsfuncties, kan de teamleider van het *control team* besluiten om de test stop te zetten.

11 Zie Annex II van de RTS voor de inhoud van het *scope specification* rapport
12 Zie Annex III van de RTS voor de inhoud van het *threat intelligence rapport*
13 Zie Annex IV van de RTS voor de inhoud van het red team test plan

Afsluiting

Wanneer de testers alle testwerkzaamheden hebben afgerond, worden de medewerkers van het blue team ingelicht over de TLPT die heeft plaatsgevonden. Uiterlijk vier weken na het einde van de test deelt het red team een rapport met het *control team* met informatie over de test en de bevindingen[14]. Dit rapport moet vervolgens worden gedeeld met het *blue team* en de testmanagers.

Uiterlijk tien weken na de testwerkzaamheden van de testers, deelt het *blue team* een rapport met het *control team* waarin een lijst is opgenomen met de gedetecteerde aanvallen tijdens de test (inclusief de logbestanden)[15]. Dit bestand wordt ook weer met de testmanagers gedeeld. In dezelfde periode moet een kleinere test worden uitgevoerd, waarbij de testers, samen met het *blue team*, de aanvallen op de ICT-systemen en -infrastructuur herhalen (dit wordt ook wel *purple teaming* genoemd). Tijdens deze test kunnen ook aanvullende onderdelen worden getest die tijdens de TLPT niet konden worden getest. Aan het einde van deze kleinere test, krijgen alle betrokkenen de mogelijkheid om elkaar feedback te geven op het TLPT-proces.

Nadat de TLPT-autoriteit de rapportage van zowel het *blue team* als het *red team* heeft gecontroleerd en goedgekeurd, moet de onderneming binnen acht weken de opgestelde samenvatting van bevindingen en de correctieplannen delen met de TLPT-autoriteit[16]. In deze periode levert de onderneming ook een verbeterplan aan waarin de geïdentificeerde tekortkomingen worden beschreven, verbeteracties (inclusief prioritering) worden voorgesteld, een *root cause analysis* wordt uitgevoerd, de verantwoordelijke medewerkers van de verbeteracties worden geïdentificeerd en de risico's worden beschreven die verbonden zijn aan het niet opvolgen van de bevindingen. Tot slot verstrekt de TLPT-autoriteit, na ontvangst van de benodigde stukken, een attest aan de onderneming waarmee wordt bevestigd dat de TLPT in overeenstemming met de vereisten is uitgevoerd.

Tabel 3

Aanvullende uitwerkingen	Beschrijving	Afgerond
RTS voor artikel 26 (11)	Advanced testing of ICT tools, systems and processes based on TLPT	Inmiddels naar EC verzonden

14 Zie Annex V van de RTS voor de inhoud van het red team test report
15 Zie Annex VI van de RTS voor de inhoud van het blue team test report
16 Zie Annex VII van de RTS voor de inhoud van het test summary report

3. Vooruitblik

Momenteel is zowel de eerste als de tweede batch van RTS'en en ITS'en gepubliceerd. De eerste batch en tweede batch zijn inmiddels voorgelegd aan de Europese Commissie die deze zal beoordelen, waarna zij naar verwachting in het derde kwartaal van 2024 een besluit neemt over de teksten.

De AFM bereidt zich in de tussentijd verder voor op het uitvoeren van DORA-toezicht. Dit is de laatste editie waarin wij inhoudelijk op de vereisten van DORA ingaan. In de volgende publicatie zal worden vooruitgeblikt op het toezicht op DORA vanaf 17 januari 2025 en andere ontwikkelingen. De volgende editie zal in het vierde kwartaal van 2024 worden gepubliceerd.

Voor een verdere uitwerking over TLPT in DORA kunnen de volgende pagina's worden geraadpleegd:
- Digital Operational Resilience Act (DORA) (afm.nl) en
- TIBER-NL-programma (afm.nl)

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