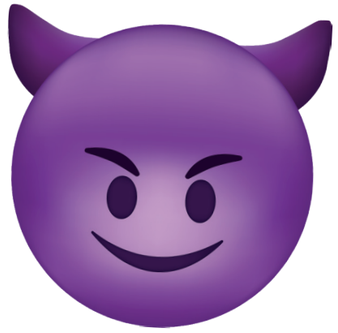
DORA en haar duiveltjes

Waarschijnlijk heeft u het zelf ook wel eens ervaren: "The devil is in the detail". Bij de implementatie van DORA is het niet anders. Betrekkelijk eenvoudige acties als 'informeer de toezichthouder bij ernstige ICT-incidenten' wordt al snel een hele opgave als de Europese regelgevers daar standaarden voor gaan ontwikkelen. In dit artikel gaan we u helpen door u een eerste rondleiding te geven langs de 'regulatory technical standards' en de andere detaillering van de DORA.



Regulatory en Implementing Technical Standards
Op verschillende plaatsen in de DORA-verordening staat dat de Europese Commissie de bevoegdheid krijgt om de voorstellen voor 'technische reguleringsnormen' vast te stellen. Daarmee wordt verder invulling gegeven aan de regelgeving. Bij de implementatie van de DORA is het dus zinvol om deze technische uitwerking er meteen bij te pakken en mee te nemen in het plan van aanpak.

Deze technische standaarden verschijnen in drie vormen namelijk:
- 'regulatory technical standards' (RTS),
- de 'implementing technical standards' (ITS),
- Guidelines (in het Nederlands vertaald als 'richtsnoeren').

Over het algemeen geldt dat de RTS wat concreter is dan de DORA verordening zelf en de ITS is doorgaans erg voorschrijvend qua detail.

Bij de DORA horen tien aanvullende documenten (RTS, ITS en Guidelines). Deze zijn verschenen in twee sets, namelijk fase 1 en fase 2. Zolang deze regelgeving nog de status consultatie heeft, zijn de teksten alleen in het Engels beschikbaar. Bij de definitieve vaststelling verschijnen de documenten in het Nederlands. Maar u kunt er in de voorbereiding nu al mee aan de slag en wij zetten alvast wat aandachtspunten voor u op een rijtje.

Fase 1: de voorstellen aan de Europese Commissie
In de eerste fase zijn vier documenten geconsulteerd. De consultatiefase is inmiddels beëindigd en de geconsulteerde documenten zijn thans als voorstel gepresenteerd aan de Europese Commissie. Het betreft de volgende vier documenten:
1. Draft RTS on the ICT Risk Management Framework and on Simplified ICT Risk Mgt Framework;
2. Draft RTS on the classification of major incidents and significant cyber threats;
3. Draft RTS to specify the policy on ICT services supporting critical or important functions;
4. Draft ITS on the Register of Information.

Fase 2: in consultatie
In de tweede fase worden zes documenten geconsulteerd. De consultatiefase is inmiddels gestart en deze loopt tot 4 maart 2024. Uiterlijk 17 juli moeten deze voorstellen, na verwerking van de feedback uit de consultatie, worden gepresenteerd aan de Europese Commissie. Het betreft de volgende zes documenten:
5. Draft RTS on subcontracting ICT services supporting critical or important functions;
6. Draft joint guidelines on the estimation of aggregated annual costs and losses caused by major ICT-related incidents;
7. Draft RTS on the harmonisation of conditions enabling the conduct of the oversight activities
8. A: Draft RTS on the content of the notification and reports for major incidents;
   B: Draft ITS on the standard forms, templates and procedures for financial entities to report a major incident;
9. Draft joint guidelines on the oversight cooperation and information exchange;
10. Draft RTS specifying elements related to threat led penetration tests.

We hebben deze documenten doorgenomen. Het gaat te ver om alles te bespreken, want het zijn stevige documenten met veel details. Hierbij een overzicht met een korte toelichting. Elk document bevat tevens de link naar de EBA-website.

1. Draft RTS on the ICT Risk Management Framework and on Simplified ICT Risk Mgt Framework
Deze technische standaard heeft betrekking op de eerste pijler en is vrij omvangrijk. Een proportionele benadering is wellicht mogelijk en de RTS biedt ook een onderdeel (titel 2) over een vereenvoudigde aanpak, maar voor de meeste organisaties zullen de voorschriften van titel 1 gelden.

De kern van de RTS is opgedeeld in vijf hoofdstukken: (1) Governance, (2) Human resources en logische toegangsbeveiliging, (3) ICT incidentmanagement, (4) ICT Business Continuity en (5) Review rapportage.

Het eerste hoofdstuk is omvangrijk en de volledige implementatie zal een flinke klus zijn die mogelijk ook niet in 2024 kan worden afgerond. Onze visie is dat het goed is om hier te denken in termen van stapsgewijze toenemende volwassenheid door middel van de PDCA-aanpak. De hoofdstukken die volgen betreffen onderwerpen die ook op basis van het Good Practice document al zijn ingericht. Maar de regels zijn wel gedetailleerder dan het Good Practice document dat in beginsel meer principle based is.

Een belangrijk sluitstuk van deze RTS is hoofdstuk 5, het jaarlijkse evaluatierapport. De RTS schrijft de vorm en inhoud voor en daarin komen alle onderdelen van het ICT risicobeheer wel in terug. De toezichthouder mag dit document opvragen en onze verwachting is dat u er rekening mee moet houden dat de toezichthouder dat ook gaat doen.

Dit document zal zich nog gaan ontwikkelen en mogelijk gaan toezichthouders ook terugkoppeling en wellicht nog wat guidance geven over hun verwachtingen. Eenvoudig beginnen is een goed idee, maar met 12 verplichte onderdelen bent u al snel onderweg richting een stevig rapport. Sommige elementen zijn overigens erg eenvoudig, zoals de datum van goedkeuring van het rapport. Andere elementen zijn omvangrijk, zoals een omschrijving van alle genomen maatregelen om de geconstateerde zwaktes en tekortkomingen op te lossen.

Naar onze verwachting zal de implementatie van deze standaard een behoorlijke klus worden, maar naar onze inschatting kan dit ook gefaseerd worden opgepakt.

2. Draft RTS on the classification of major incidents and significant cyber threats
Deze technische standaard heeft betrekking op de tweede pijler van DORA. Een belangrijk onderdeel van deze tweede pijler is dat u onderscheid moet gaan maken tussen:
- (gewone) ICT-incidenten en ernstige ICT-incidenten en
- (gewone) cyberdreigingen en significante cyberdreigingen.

Ernstige ICT-incidenten moeten (onverwijld) worden gemeld bij de bevoegde autoriteit en significante cyberdreigingen op vrijwillige basis. Deze technische standaard gaat met name in op de criteria om ICT-incidenten en Cyberdreigingen als "ernstig" of "significant" te classificeren. Daarvoor worden zeven criteria uitgewerkt waarbij deels kwalitatieve criteria worden meegegeven, maar deels ook heel concrete kwantitatieve criteria, zoals bijvoorbeeld voor de economische impact (> €100.000), de duur van het incident (24 uur) of de downtime van kritische of belangrijke systemen (2 uur).

Deze RTS biedt een nadere uitwerking van de criteria en hoe deze onderling moeten worden gewogen om te kunnen concluderen of er sprake is van een ernstig ICT-incident dat moet worden gemeld.

De wijze waarop moet worden gemeld is uitgewerkt in een separate RTS en ITS (zie document 8). In dat document worden ook de tijdslijnen en de inhoud van de rapportage toegelicht.

Op zichzelf zijn de regels best concreet en duidelijk, maar pas als je aan de slag gaat, bijvoorbeeld in een door InAudit gefaciliteerde workshop, blijkt pas echt hoe lastig het zal zijn en welke voorbereidingen je moet treffen om te voorkomen dat je in tijden van grote stress (als gevolg van een ernstig ICT-incident) het wiel moet gaan uitvinden. Naar onze verwachting zijn workshops en 'table top exercises' de beste methode om deze regelgeving eigen te maken.

3. Draft RTS to specify the policy on ICT services supporting critical or important functions
Deze technische standaard heeft betrekking op de vierde pijler van DORA en gaat over de risicobeheersing met betrekking tot ICT-serviceproviders. De vierde pijler van DORA is een hele pittige opgave die zich ook nog eens lastig laat plannen omdat medewerking van leveranciers nodig zal zijn. Ook is er nog best wel wat onduidelijkheid over de mate waarin je mag steunen op de 'oversight' werkzaamheden van de grote 'third-party providers'. Als individuele verzekeraar zal het namelijk lastig onderhandelen zijn met Microsoft, Google of AWS.
Inhoudelijk bestaat deze RTS op zichzelf eigenlijk maar uit tien artikelen, waarbij het met name gaat over de risico-analyse rondom uitbesteding van ICT diensten, due diligence vooraf, contractuele bepalingen en de monitoring. Uit dit RTS volgt wel dat het wellicht zinvol is om het ICT-uitbestedingsbeleid als separaat beleidsdocument uit te werken. Hierdoor voorkom je dat het reguliere uitbestedingsbeleid te zeer wordt belast met ICT-specifieke vereisten.

Vervolg pagina 19

Naar onze verwachting is de invoering van deze RTS een logisch en samenhangend onderdeel van de werkzaamheden van hoofdstuk vijf van de DORA verordening zelf. In dit document wordt op het eerste gezicht weinig extra complexiteit toegevoegd.

4. Draft ITS on the Register of Information

Ook het informatieregister is onderdeel van de vierde pijler. Op zichzelf klinkt het heel logisch: namelijk een overzicht van ICT serviceproviders, de dienstverlening en het soort contracten. Toch zijn de ESA's erin geslaagd om er een complex geheel van te maken. Probeer het zelf maar eens.

Een lastig onderdeel is dat het informatieregister meerdere lagen kan hebben. Als er belangrijke of kritieke functies worden uitbesteed kan het zijn dat ook de serviceprovider van de serviceprovider van de serviceprovider moet worden gerapporteerd, ergo twee of drie lagen diep. Binnen InAudit hebben we een Excel tool (pagina 11 punt 4 in dit magazine) gemaakt waarin we alle informatie bij elkaar hebben gebracht en u op een iets vriendelijkere wijze proberen naar de juiste invulling te leiden met vertalingen, drop down menu's en instructies.

Het informatieregister moet er in beginsel liggen als DORA van kracht wordt op 17 januari 2025. De bevoegde autoriteiten mogen het ook opvragen en onze verwachting is ook dat dit misschien al in 2025 zal gebeuren. Dit kan dus uitdrukkelijk niet worden uitgesteld naar 2025.

Onze verwachting is dat de eerste invulling van deze templates erg zal tegenvallen. Neem hier voldoende tijd voor, of overweeg een door InAudit gefaciliteerde workshop.

5. Draft RTS on subcontracting ICT services supporting critical or important functions

Waar document 3 gaat over het beleid met betrekking tot ICT uitbesteding, gaat het in dit document met name over de vraag: "Mag je deze (kritieke of belangrijke) functie eigenlijk wel uitbesteden?" Het document kent eigenlijk maar 8 artikelen en is daarom vrij overzichtelijk. Het centrale artikel van de RTS is artikel 4 waarin een soort checklist-achtige opsomming wordt gegeven van de specifieke eisen waaraan de SLA met de serviceprovider moet voldoen. Uiteraard beschrijft deze RTS ook de verplichting om de risico's te analyseren, maatregelen te treffen om de naleving te bewaken en om de overeenkomst te beëindigen bij materiële veranderingen.

Net zoals document 3 is dit RTS een logisch en integraal onderdeel van de implementatie van de op zichzelf lastige vierde pijler over ICT-risicomanagement over uitbestedingen.

6. Draft joint guidelines on the estimation of aggregated annual costs and losses caused by major ICT-related incidents

Zowel in het evaluatieverslag over het boekjaar (zie document 1) als in de meldingen van 'ernstige ICT-incidenten' moet de (geschatte) schade als gevolg van ICT incidenten worden gerapporteerd. Deze kosten kunnen op verschillende manieren worden bepaald en de vraag zal vaak zijn of kosten nu incident-gerelateerd zijn of wellicht gewoon 'vervroegde investeringen' danwel 'achterstallig onderhoud'. Ook het toerekenen van schades aan een boekjaar (afgrenzen) kan wellicht complexiteit geven. Deze guidelines geven daartoe nadere duiding. Ook wordt een template meegegeven (pagina 16 van deze RTS) van de te rapporteren (geschatte) schade in het boekjaar.

Deze RTS moet zeker enige aandacht krijgen. Mogelijk zal iedere organisatie hier ook zelf weer vuistregels voor ontwikkelen, maar op zichzelf lijken deze guidelines niet erg complex.

7. Draft RTS on the harmonisation of conditions enabling the conduct of the oversight activities

Terwijl wij meestal spreken over 'vijf pijlers' spreken de toezichthouders meestal over zes focus areas. Het verschil is het 'oversight' kader. Daarin worden de bevoegdheden van de bevoegde autoriteiten vastgelegd met betrekking tot het (rechtstreekse) toezicht op ICT-serviceproviders.

Wij hebben ons hier vooralsnog niet nader in verdiept omdat we ervan uitgaan dat dit niet tot werkzaamheden voor financiële instellingen zal leiden.

De 5 pijlers van DORA

8. A: Draft RTS on the content of the notification and reports for major incidents
B: Draft ITS on the standard forms, templates and procedures for financial entities to report a major incident

Bij de tweede pijler van DORA horen twee documenten, namelijk de RTS die gaat over de classificatie van incidenten en cyberdreigingen (document 2) en een RTS (en ITS) die gaat over de tijdslijnen en de inhoud van de melding van ICT-incidenten (document 8).

Document 8 bestaat uit twee delen, namelijk een RTS en een ITS. De ITS betreft een gedetailleerde uitwerking van de te rapporteren velden in de vier templates die van toepassing worden op de incidentenrapportage aan de bevoegde autoriteiten, inclusief data glossary etc.

Het informeren van de autoriteiten over ernstige ICT-incidenten vindt plaats met drie verschillende rapportages (en templates):

- Eerste kennisgeving: Deze moet plaatsvinden binnen vier uur na het classificeren van het incident als 'ernstig', maar niet later dan 24 uur na eerste vaststelling. De classificatie moet dus min of meer binnen 20 uur zijn afgerond.
- Tussentijds verslag: Zodra de situatie is teruggekeerd naar normaal, maar anders na 72 uur na classificatie als 'ernstig'.
- Eindverslag: Niet later dan één maand na classificatie, maar als het incident dan nog niet gesloten is, dan de dag na de definitieve afwikkeling van het incident.

Voor de drie verschillende verslagen zijn afzonderlijke templates gedefinieerd. Deze zijn in de ITS uitgewerkt. Om deze templates te kunnen invullen moet u in uw incidentenproces heel wat informatie vastleggen. Zo moet u bijvoorbeeld na afloop rapporteren over de totale kosten van het incident. Ook daar bestaan weer guidelines voor (document 6).

Binnen InAudit hebben we een Excel tool (pagina 11 punt 3 in dit magazine) ontwikkeld waarmee kan worden geoefend om op tijd te zijn voorbereid op deze meldingsplicht. In geval van ernstige ICT incidenten is het namelijk geen goed moment om die last er ook nog bij te krijgen. Ons advies is om hiertoe één of meerdere workshops te plannen zodat er een goed draaiboek ligt en er alvast enige bekendheid zal zijn met betrekking tot alle vragen en bepalingen en hetgeen rondom het incident moet worden vastgelegd.

9. Draft joint guidelines on the oversight cooperation and information exchange

Net als document 7 gaat ook dit document over de samenwerking tussen bevoegde autoriteiten als het gaat om het toezicht op met name serviceproviders. Dit document biedt een wettelijk kader om informatie te delen. Verder beschouwen wij dit niet als een document waarmee financiële instellingen aan de slag moeten gaan.

10. Draft RTS specifying elements related to threat led penetration tests

De 'threat led penetration test' (TLPT) is een belangrijk onderdeel van de derde pijler van DORA. Bevoegde autoriteiten kunnen daarin een belangrijke rol spelen als het gaat om validatie van de scope vooraf en het delen van de uitkomsten achteraf. Eisen worden gesteld aan diverse elementen, waaronder ook expliciet de testers. In het RTS wordt dit allemaal netjes uitgewerkt met onder andere ook een duiding van de 'red, white and blue teams' in het TLPT proces.

Maar voordat we enthousiast de diepte ingaan maakt artikel 2 duidelijk dat deze verplichting voor veel financiële instellingen niet zal gelden. Voor verzekeraars bijvoorbeeld gaat het om organisaties met meer dan €500 miljoen premievolume. Hoewel we graag onze enthousiaste beschouwing over de verschillende fases van het TLPT willen delen, kunnen we dat wellicht beter alleen doen met de organisaties die het betreft. Voor de meeste organisaties kan invoering van de TLPT en deze RTS achterwege blijven, al is het opdoen van inspiratie voor het reguliere pentest programma geen slecht idee.

We zijn er om u te helpen!

De hele stapel regelgeving (DORA plus tien RTS/ITS documenten) is een hele klus. Zelfs als u redelijk goed bent ingevoerd is het wellicht zinvol om te kunnen sparren. Binnen InAudit hebben we tools en workshops ontwikkeld die u wellicht op een efficiënte wijze op weg kunnen helpen. Daarover hebben we ook een artikel opgesteld. Dat vindt u op pagina 10. Verder houden we u graag op de hoogte via de themapagina op onze website. Maar u mag natuurlijk ook gewoon bellen!

Ronald van de Langenberg
Algemeen Directeur InAudit
06-24 48 68 92