Deloitte.

Positieve impact serviceorganisaties op eigen operationele weerbaarheid

In dit artikel leest u hoe serviceorganisaties, oftewel derdepartijdienstverleners, een cruciale rol vervullen in de operationele weerbaarheid van financiële instellingen. We bespreken de impact van relevante standaarden op het beheer en toezicht van deze dienstverleners. Daarnaast gaan we in op de verschillen tussen ICT- en non-ICT-dienstverleners, de uitdagingen die financiële instellingen ondervinden bij het beheersen van deze ketens, en bieden we praktische tips om hier effectief mee om te gaan. Tot slot belichten we hoe Deloitte financiële instellingen kan ondersteunen bij het voldoen aan de complexe eisen rondom third-party risk management.

Aanleiding

Financiële instellingen zijn steeds afhankelijker geworden van externe ICT-diensten, zoals cloudopslag, betalingsverwerking en data-analyse. Dit heeft het belang van serviceorganisaties aanzienlijk vergroot. Serviceorganisaties leveren vaak essentiële diensten voor de dagelijkse bedrijfsvoering en innovatie binnen de financiële sector. Deze toenemende afhankelijkheid brengt nieuwe risico's met zich mee, zoals concentratierisico, verlies van controle over kritieke processen en een verhoogde kwetsbaarheid voor cyberdreigingen.

Om deze risico's te beheersen en de digitale weerbaarheid van de sector te vergroten, heeft de Europese Unie de Digital Operational Resilience Act (DORA)[1] geïntroduceerd. DORA legt de nadruk op het identificeren, beheersen en monitoren van risico's die ontstaan door het inschakelen van serviceorganisaties. Daarnaast beoogt DORA de transparantie en het toezicht op kritieke ICT-dienstverleners te versterken. Een goed begrip van de rol van en het toezicht op serviceorganisaties is daarom essentieel om te voldoen aan de eisen van DORA en de continuïteit van de financiële dienstverlening te waarborgen.

RTS Subcontracting (update juli 2025)
De Regulatory Technical Standard (RTS) over subcontracting[2] is recentelijk gepubliceerd. Deze standaard bevat specifieke eisen en voorwaarden voor het gebruik van uitbestede ICT-diensten die kritieke of belangrijke functies of materiële onderdelen ondersteunen. Financiële instellingen dienen de risico's van uitbesteding al in de precontractuele fase te beoordelen, onder andere via het due-diligenceproces. De standaard stelt eisen aan het implementeren, monitoren en beheren van contractuele ICT-uitbestedingsafspraken. Dit waarborgt dat financiële instellingen de gehele keten van ICT-uitbesteding kunnen monitoren en beheersen.

Verantwoordelijkheden serviceorganisaties

Serviceorganisaties dienen incidenten, kwetsbaarheden en operationele afwijkingen proactief te rapporteren, zodat tijdige en doeltreffende maatregelen kunnen worden genomen (art. 22). Het vertrouwen in het digitale fundament van financiële diensten hangt immers af van deze openheid en snelle communicatie. Financiële instellingen stellen niet alleen business continuity- en disaster recovery-plannen op, maar testen en monitoren deze plannen ook regelmatig (art. 25). Toezicht op deze plannen verzekert dat bij onverwachte gebeurtenissen de dienstverlening kan doorgaan zonder dat klanten daar (ernstige) hinder van ondervinden.

De governance van serviceorganisaties speelt hierin een bepalende rol. Toezichthouders eisen een heldere structuur met duidelijke verantwoordelijkheden en voldoende middelen om risico's effectief te beheersen. Dit voorkomt dat operationele blindheid of gebrekkige middelen leiden tot onvoorziene kwetsbaarheden. Kortom, DORA transformeert serviceorganisaties van louter leveranciers naar actieve partners in het veiligstellen van de digitale toekomst van de financiële sector.

Consultation draft Guidelines on the sound management of third-party risk (update juli 2025)
Uit de lopende consultatie over de nieuwe EBA-richtlijn voor third-party risk[3] blijkt een duidelijk onderscheid tussen ICT-dienstverleners en non-ICT-dienstverleners. Dit onderscheid is essentieel vanwege het verschillende regelgevingskader en de specifieke risico's die aan beide typen diensten verbonden zijn. Het beheer van risico's rondom ICT-dienstverleners valt onder DORA en niet onder de nieuwe EBA-richtlijnen. Non-ICT-dienstverleners vallen binnen het toepassingsgebied van de EBA-richtlijnen. De EBA stelt eisen aan het beheer van risico's, governance, due diligence, contractuele auditrechten, continuity-plannen en exitstrategieën.

1 Regulation—2022/2554—EN—DORA—EUR-Lex
2 Final report on Draft Regulatory Technical Standards to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions as mandated by Article 30(5) of Regulation (EU) 2022/2554
3 Consultation on draft Guidelines on the sound management of third-party risk | European Banking Authority

Monitoring serviceorganisaties

Financiële instellingen moeten zorgen voor solide contractuele afspraken waarin niet alleen verantwoordelijkheden en serviceniveaus zijn vastgelegd, maar ook essentiële elementen zoals audit- en toegangsrechten (art. 28 en 30), incidentrapportage (art. 22), continuïteitsplannen en exitstrategieën (art. 25). Deze contracten vormen het fundament waarop financiële instellingen effectief toezicht bouwen. Toegang tot systemen, data en personeel van dienstverleners is cruciaal. Hiermee kunnen financiële instellingen eigen audits uitvoeren en verifiëren dat de dienstverlening voldoet aan wettelijke en contractuele eisen (art. 28). Regelmatige due diligence vooraf én voortdurende risicobeoordelingen zorgen ervoor dat potentiële kwetsbaarheden tijdig worden gesignaleerd en aangepakt (art. 26). Monitoring vindt plaats via prestatie-indicatoren, rapportages en een actief incidentmanagement (art. 22 en 27). Hierdoor kunnen financiële instellingen snel reageren op operationele verstoringen.

Het is essentieel om de continuity- en disaster recovery-plannen van dienstverleners te toetsen en te zorgen voor heldere exitplannen, zodat diensten zonder haperingen kunnen worden overgenomen of opnieuw intern worden ingericht (art. 25). Samenwerking met toezichthouders vormt een belangrijke schakel. Financiële instellingen faciliteren inspecties en delen informatie, waardoor het toezicht transparant en doeltreffend blijft (art. 29).

Kortom, door strikte contracten, volledige toegang, grondige risicobeoordeling, constante monitoring en nauwe samenwerking vorm te geven aan het toezicht, behouden financiële instellingen hun operationele veerkracht en betrouwbaarheid.

Uitdagingen

Op basis van DORA ondervinden financiële instellingen verschillende uitdagingen bij het beheersen van serviceorganisaties. De vier belangrijkste uitdagingen zijn:

- **Toegang tot relevante informatie en transparantie**
  Financiële instellingen moeten volledige en tijdige toegang hebben tot data, systemen en rapportages van serviceorganisaties om audits en controles effectief uit te voeren (art. 28). In de praktijk blijkt het verkrijgen van deze informatie, zeker bij buitenlandse dienstverleners, vaak een uitdaging.
- **Incidentmanagement en rapportageverplichtingen**
  DORA vereist een snelle en proactieve melding van ICT-incidenten door serviceorganisaties (art. 22). Financiële instellingen moeten deze incidenten adequaat managen, maar het coördineren en interpreteren van meldingen van diverse dienstverleners kan complex zijn.
- **Beheersen van operationele en cyberrisico's**
  DORA legt nadruk op een holistisch risicobeheer (art. 9), maar de steeds evoluerende aard van cyberdreigingen en operationele risico's vereist een continu bijstellen van beheer- en monitoringsprocessen. Dit vergt veel middelen en expertise.
- **Capaciteits- en kennisvraagstukken**
  Om effectief te voldoen aan de DORA-eisen moeten financiële instellingen beschikken over voldoende gekwalificeerde medewerkers met expertise in ICT-risicomanagement, contractuele verplichtingen en compliance.

RTS Register of Information (november 2024)/ verplichte uitvraag informatieregister (april 2025)
In april 2025 zijn De Nederlandsche Bank (DNB) en de Autoriteit Financiële Markten (AFM) gestart met de verplichte uitvraag van het informatieregister (art. 28 lid 3). Dit register biedt een gedetailleerd en gestandaardiseerd overzicht van alle contractuele afspraken over ICT-diensten met derden—inclusief intragroepsleveranciers en belangrijke subcontractors—die cruciaal zijn voor de operationele veerkracht van financiële instellingen.

Financiële instellingen dienen het informatieregister te rapporteren via uniforme templates die onder meer:

- Alle contractuele ICT-arrangementen en hun onderlinge relaties in de ICT-serviceketen inzichtelijk maken;
- Gebruikmaken van unieke identificaties zoals LEI en EUID voor heldere en eenduidige herkenning van dienstverleners;
- Het rangschikken van ICT-dienstverleners in de keten (directe partijen en subcontractors) voorschrijven;
- Uitgebreide informatie bevatten over de aard van ICT-diensten, risico-inschattingen, relevantie van functies en mogelijke impact van uitval;
- En waarborgen dat data consistent, accuraat en compleet worden vastgelegd op entiteit-, subgeconsolideerd- en geconsolideerd niveau binnen groepen.

DORA vergroot de transparantie en zorgt ervoor dat toezichthouders, zoals DNB en AFM, kunnen sturen op digitale weerbaarheid om de risico's rondom externe ICT-dienstverlening te beheersen.

Tips

Om de vier genoemde uitdagingen die financiële instellingen ondervinden bij het beheersen van serviceorganisaties onder DORA effectief aan te pakken, kunnen de volgende tips als leidraad dienen:

- **Sluit heldere en uitgebreide contracten af (zie uitdaging I)**
  Om te voldoen aan art. 28 van DORA, waarin volledige en tijdige toegang tot data, systemen en rapportages van serviceorganisaties wordt vereist, is het cruciaal dat financiële instellingen heldere contractuele afspraken maken met hun dienstverleners, inclusief buitenlandse partijen. Deze afspraken moeten expliciete rechten tot toegang en audit bevatten, zodat audits en controles effectief kunnen worden uitgevoerd. Daarnaast is het van belang gestandaardiseerde rapportage- en communicatieprocessen te implementeren om de beschikbaarheid en betrouwbaarheid van informatie te waarborgen. Door nauwe samenwerking met dienstverleners kunnen praktische belemmeringen worden weggenomen, waardoor wordt voldaan aan de DORA-eisen en de integriteit van audit- en controleprocessen wordt versterkt.
- **Implementatie geïntegreerd en gestandaardiseerd incidentmanagementproces (zie uitdaging II)**
  Om te voldoen aan de snelle en proactieve meldplicht van ICT-incidenten zoals voorgeschreven in art. 22 van DORA, is het essentieel om een geïntegreerd en gestandaardiseerd incidentmanagementproces te implementeren. Dit proces omvat het centraal verzamelen en monitoren van incidentmeldingen van alle serviceorganisaties, waarbij uniforme rapportageformaten worden gehanteerd. Daarnaast dienen duidelijke communicatieprotocollen en regelmatige afstemmingen met dienstverleners te worden vastgesteld, zodat meldingen tijdig en eenduidig worden geïnterpreteerd en opgevolgd.
- **Implementeer een robuust risicobeheerraamwerk (zie uitdaging III)**
  DORA benadrukt het belang van holistisch risicobeheer (art. 9), wat vraagt om een continu aanpassingsproces van beheer- en monitoringsprocessen vanwege de snel evoluerende cyberdreigingen en operationele risico's. Dit vergt een proactieve benadering waarbij financiële instellingen investeren in gespecialiseerde kennis, geavanceerde technologieën en flexibele processen. Door het integreren van realtime threat intelligence, regelmatige risicoassessments en het gebruik van geautomatiseerde monitoringtools kunnen risicobeheersing en detectie worden geoptimaliseerd. Daarnaast is het essentieel om samen te werken met externe experts en dienstverleners om up-to-date te blijven en de benodigde middelen efficiënt in te zetten, zodat het risicomanagement continu effectief en toekomstbestendig blijft. Hierbij kan onder meer worden gedacht aan het DORA in control framework van NOREA[4].
- **Investeer in sterke governance en interne capaciteit (zie uitdaging IV)**
  Effectieve naleving van de DORA-eisen vereist dat financiële instellingen beschikken over voldoende gekwalificeerde medewerkers met diepgaande expertise op het gebied van ICT-risicomanagement, contractuele verplichtingen en compliance. Dit betekent dat organisaties moeten investeren in gerichte opleidingen, kennisontwikkeling en het aantrekken van specialisten. Daarnaast is het belangrijk om multidisciplinaire teams te vormen waarbij kennis over technologie, juridische aspecten en risicobeheer wordt geïntegreerd. Door het continu ontwikkelen van vaardigheden en het bevorderen van kennisdeling binnen de organisatie kunnen financiële instellingen de complexe eisen van DORA adequaat invullen en de weerbaarheid tegen ICT-risico's versterken.

4 NOREA | Digital Operational Resilience Act—DORA

Wat kan Deloitte betekenen?

Deloitte kan financiële instellingen op diverse manieren ondersteunen bij het effectief beheersen van serviceorganisaties en het voldoen aan de eisen van DORA:

- **Audit Readiness en Assurance (ISAE 3000) (zie tip I/II)**
  Ter ondersteuning van audits voert Deloitte voorbereidingsaudits uit volgens de standaarden van ISAE 3000. Hierbij worden cruciale onderwerpen beoordeeld, zoals incidentmanagement en -rapportage, encryptie, netwerksegmentatie, bewustwordingssessies en de verantwoordelijkheden van het bestuur. Om financiële instellingen succesvol te laten zijn in hun auditproces, biedt Deloitte gerichte ondersteuning bij de voorbereiding, waaronder het samenstellen van een gedegen dossier, het toetsen van controles en het trainen van proceseigenaren op hun rol tijdens de audit. Zodra een organisatie 'audit-ready' is, kan Deloitte tevens assurance verlenen middels een ISAE 3000-rapport. Dit rapport bevestigt de effectiviteit van beheersmaatregelen en processen, waarmee organisaties inzicht krijgen in hun compliance en operationele robuustheid.
- **Risicobeoordeling en gap-analyse (plus second opinion) (zie tip I/II)**
  Deloitte voert diepgaande assessments uit om de huidige governance, risicobeheerprocessen en contractuele kaders rondom serviceorganisaties grondig te beoordelen. Hiermee worden eventuele lacunes ten opzichte van de DORA-vereisten helder in kaart gebracht. Deloitte biedt ook second opinion-diensten aan waarbij een onafhankelijke en kritische herbeoordeling wordt uitgevoerd van eerder uitgevoerde assessments, zowel intern als extern. Deze second opinion helpt organisaties om de kwaliteit, volledigheid en objectiviteit van eerdere analyses te verifiëren en eventuele blinde vlekken of risico's te identificeren. Op basis van deze inzichten adviseert Deloitte over de meest urgente prioriteiten en passende verbetermaatregelen, zodat organisaties hun third-party risk management effectief kunnen versterken en voldoen aan de nieuwe regelgeving.
- **Ontwikkeling en implementatie van governance- en beheerskaders (zie tip III)**
  Deloitte ondersteunt organisaties bij het ontwerpen en implementeren van robuuste interne governance-structuren, beleid en procedures die de volledige levenscyclus van third-party relaties bestrijken. Van grondige due diligence en continue monitoring tot effectief incidentmanagement en strategische exit-planning—Deloitte zorgt ervoor dat elke fase zorgvuldig wordt beheerd.
- **Training en bewustwording (zie tip IV)**
  Deloitte biedt maatwerkworkshops en trainingen aan voor management-, risicomanagement-, compliance- en IT-teams, gericht op de inhoud en impact van DORA. Hierbij ligt de focus op best practices voor het beheersen van third-party risks en het effectief toepassen van het proportionaliteitsbeginsel. Deze trainingen zijn zorgvuldig afgestemd op de eisen die DORA stelt, waardoor organisaties niet alleen voldoen aan de regelgeving, maar ook hun kennis en vaardigheden versterken om risico's proactief en efficiënt te managen.
- **Capaciteitsopbouw en kennisontwikkeling (zie tip IV)**
  Door het (tijdelijk) inzetten van ervaren experts versterkt Deloitte de interne capaciteit van financiële instellingen op het gebied van IT-risicomanagement, contractbeheer en compliance. Deze ondersteuning zorgt ervoor dat toezicht en governance stevig en duurzaam worden verankerd binnen de organisatie, waardoor financiële instellingen beter zijn uitgerust om complexe risico's effectief te beheersen en te voldoen aan steeds strengere regelgeving.

Voor meer informatie en om te ontdekken hoe wij u kunnen ondersteunen, nodigen wij u uit contact op te nemen met Shahil Kanjee, Jesper de Boer, Bas Freriks of Rick Vissers.

De auteurs

Shahil Kanjee
Partner—IT Audit & Assurance
shkanjee@deloitte.nl

Jesper de Boer
Director—IT Audit & Assurance
JedeBoer@deloitte.nl

Bas Freriks
Senior Manager—IT Audit & Assurance
bafreriks@deloitte.nl

Rick Vissers
Manager—IT Audit & Assurance
RVissers@deloitte.nl

Deloitte.

Designed by CoRe Creative Services. RITM2191468