DORA.

Op tijd compliant zijn met de
Digital Operational Resilience Act (DORA)
Wij helpen u graag!

Kennisdag voor betaalinstellingen, 10 oktober 2024

InAudit

DORA: niet alleen een uitdaging, maar ook een kans om uw bedrijfsvoering te versterken!

DORA, hoe zit het ook alweer?
De Digital Operational Resilience Act (hierna: DORA) bestaat uit een pakket maatregelen om de digitale weerbaarheid van de financiële sector te versterken. Dit betekent voor u dat u aantoonbaar compliant moet zijn met wat DORA stelt. In de praktijk komt dit erop neer dat u moet kunnen aantonen dat u weerstand kunt bieden tegen, kunt reageren op en kunt herstellen van alle vormen van aan IT gerelateerde verstoringen en bedreigingen. DORA is daardoor een mooi instrument om uw beheersing te versterken.

Aan welke tijdlijnen moet u denken?
DORA is in werking getreden op 17 januari 2023. Vanaf 17 januari 2025 moet u aantoonbaar compliant zijn. Dit betekent dat u niet alleen moet kunnen aantonen dat u op papier heeft beschreven hoe u voldoet, maar ook moet kunnen aantonen dat u in de praktijk *in control* bent.

Wat raden wij u aan?
Wij adviseren u om zo snel mogelijk in beeld te hebben in hoeverre u voldoet aan DORA en daarna eventuele *gaps* te implementeren. Nadat u de eisen uit DORA een halfjaar heeft geïmplementeerd kunt u dan in 2025 een audit laten uitvoeren. Op deze manier kunt u aantonen dat u compliant en in control bent.

In Audit

De verschillende pijlers van DORA

ICT risico management

- Governance
- Risicomanagement raamwerk
- Preventie & detectie
- Respons en herstel
- Communicatie
- Etc.

ICT incident rapportage

- Classificatie van incidenten
- Classificatie van dreigingen
- Criteria en drempels
- Verplichte melding
- Geanonimiseerde EU-brede rapportages

Testen van digitale weerbaarheid

- Testprogramma
- Interne of externe onafhankelijke partijen
- (TLPT) - Threat-Led penetration testing (dreigingsgestuurd)
- Eens in de drie jaar (extern)
- Rapportage aan toezichthouder

ICT risicobeheer ketenpartners

- Kritieke of belangrijke functies
- Pre-contract toetsing
- Realistische exit opties
- Centraal toezicht op de ICT-reuzen
- Bevoegdheden en boetebepalingen

ICT informatie uitwisseling

- Juridisch kader om informatie over dreigingen en kwetsbaarheden te delen
- Vertrouwens-gemeenschappen (Trusted communities)

In Audit

De pijlers van DORA in vogelvlucht:

I: ICT risico management

DORA Chapter II - ICT Risk management

Artikel 5: Governance en organisatie	Artikel 6: Kader voor ICT risico beheer	Artikel 7: ICT systemen, protocollen en instrumenten	Artikel 8: Identificatie	Artikel 9: Bescherming en preventie	Artikel 10: Detectie	Artikel 11: Reactie en herstel	Artikel 12: Backup, herstel-procedures en methodes	Artikel 13: Verbeter-potentieel	Artikel 14: Communi-catie	Artikel 15: Verbeter-potentieel	Artikel 16: Communi-catie

RTS over
Artikel 15 die verwijst naar:
Artikel 6(5)
Artikel 9(2)
Artikel 9(4)c
Artikel 10(1)
Artikel 10(2)
Artikel 11(1)
Artikel 11(3)
Artikel 11(6)

RTS over
Artikel 16(3) die verwijst naar:
Artikel 16(1) a, c, f, g
Artikel 16(2)

In Audit

De pijlers van DORA in vogelvlucht:

II: ICT incident rapportage (1/2)

DORA - ICT incident rapportage

Artikel 17: Beheerproces voor ICT-gerelateerde diensten	Artikel 18: Classificatie van ICT-gerelateerde incidenten en cyberdreigingen	Artikel 19: Rapportage van ernstige ICT-gerelateerde incidenten en vrijwillige melding van significante cyberdreigingen	Artikel 20: Harmonisatie van inhoud en modellen van rapportage	Artikel 21: Centralisatie van meldingen van ernstige ICT-gerelateerde incidenten	Artikel 22: Feedback van toezichthouders	Artikel 23: Betalingsgerelateerde operationele of beveiligingsincidenten die kredietinstellingen, betalingsinstellingen, aanbieders van rekeninginformatie-diensten en instellingen voor elektronisch geld betreffen
	RTS over Artikel 18(3) die verwijst naar: Artikel 18(1) Artikel 18(2)		**RTS over** Artikel 20 die verwijst naar: Artikel 18(1) Artikel 19(4) Definitief op 17 juli 2024			

InAudit

De pijlers van DORA in vogelvlucht:

II: ICT incident rapportage (2/2)

Omvang	Defi-nitie	Toelichting
ICT gerelateerd incident	Artikel 3 lid 8	Een gebeurtenis of een reeks gekoppelde gebeurtenissen die: • niet door de financiële entiteit zijn gepland en • die de beveiliging van de netwerk- en informatiesystemen in gevaar brengen en • een nadelig effect hebben op de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van gegevens of • op de door de financiële entiteit verleende diensten
Betalingsgerelateerd operationeel of beveiligingsincident	Artikel 3 lid 9	Een gebeurtenis of een reeks gekoppelde gebeurtenissen die niet door de [...] bedoelde financiële entiteiten zijn gepland, die al dan niet ICT-gerelateerd zin, en [een negatief effect heeft op betalingsgelateerde activiteiten
Ernstig ICT-gerelateerd incident	Artikel 3 lid 10	Een ICT-gerelateerd incident met grote nadelige gevolgen voor de netwerk- en informatiesystemen die kritieke of belangrijke functies van de financiële entiteit ondersteunen
Ernstig betalingsgerelateerd operationeel of beveiligingsincident	Artikel 3 lid 11	Een betalingsgerelateerd operationeel of beveiligingsincident dat een groot negatief effect heeft op verleende betalingsgerelateerde diensten

Omvang	Defi-nitie	Toelichting
Cyberdreiging	Artikel 3 lid 12	Cyberdreiging in de zin van [...] van Verordening (EU) 2019/881 (lees: De CyberSecurity Act - ENISA) "elke potentiële omstandigheid, gebeurtenis of actie die Netwerk- en informatiesystemen, de gebruikers, van dergelijke systemen en andere personen kan schaden, verstoren of op andere wijze negatief kan beïnvloeden"
Significante cyberdreiging	Artikel 3 lid 13	Een cyberdreiging waarvan de technische kenmerken erop wijzen dat zij kan leiden tot een ernstig ICT-gerelateerd incident of een ernstig betaling gerelateerd operationeel of beveiligingsincident.
Cyberaanval	Artikel 3 lid 14	Cyberaanval: "een kwaadwillig ICT-gerelateerd incident dat het gevolg is van een door een dreigingsactor gepleegde poging om een actief te vernietigen, bloot te stellen, te veranderen, buiten werking te stellen, te stelen of er ongeoorloofde toegang toe te verkrijgen of er ongeoorloofd gebruik van te maken."

In Audit

De pijlers van DORA in vogelvlucht:

III: Testen van digitale weerbaarheid (1/2)

DORA - Testen van digitale weerbaarheid

Artikel 24:
Algemene vereisten voor uitvoering van tests van digitale operationele weerbaarheid

Artikel 25:
Testen van ICT-instrumenten en -systemen

Artikel 26:
Geavanceerde tests van ICT-instrumenten, -systemen en -processen op basis van TLPT

Artikel 27:
Vereisten voor testers voor het uitvoeren van TLPT

RTS over
Artikel 26(11)

Definitief op
17 juli 2024

InAudit

De pijlers van DORA in vogelvlucht:

III: Het testen van digitale weerbaarheid (2/2)

- ☑ Eisen aan programma van penetratietesten
- ☑ De dreigingsgestuurde penetratietest (TLPT) – mogelijk al eind 2024 om in 2025 gereed te zijn.
- ☑ Afstemming met toezichthouder vooraf (art 26 lid 2)
- ☑ Rapportage aan de toezichthouder achteraf (art 26 lid 6) – mogelijk gaat het dan om één toezichthouder (art 26 lid 9)
- ☑ Gebundelde tests bij derde-aanbieders
- ☑ Betaalinstellingen moeten een TLPT uitvoeren als zij in elk van de voorgaande twee boekjaren een totale waarde van betaaltransacties van meer dan 150 miljard euro hebben overschreden.

In Audit

De pijlers van DORA in vogelvlucht:

IV: ICT risicobeheer ketenpartners (1/2)

DORA - ICT risicobeheer ketenpartners

Artikel 28:
Algemene beginselen

Artikel 29:
Voorlopige beoordeling van het ICT-concentratierisico op het niveau van de entiteit

Artikel 30:
Belangrijke contractuele bepalingen

RTS over
Artikel 28(9) die verwijst naar 28(3)

Artikel 28(10) die verwijst naar 28(2)

RTS over
Artikel 30(5) die verwijst naar 30(2) a

Definitief op 17 juli 2024

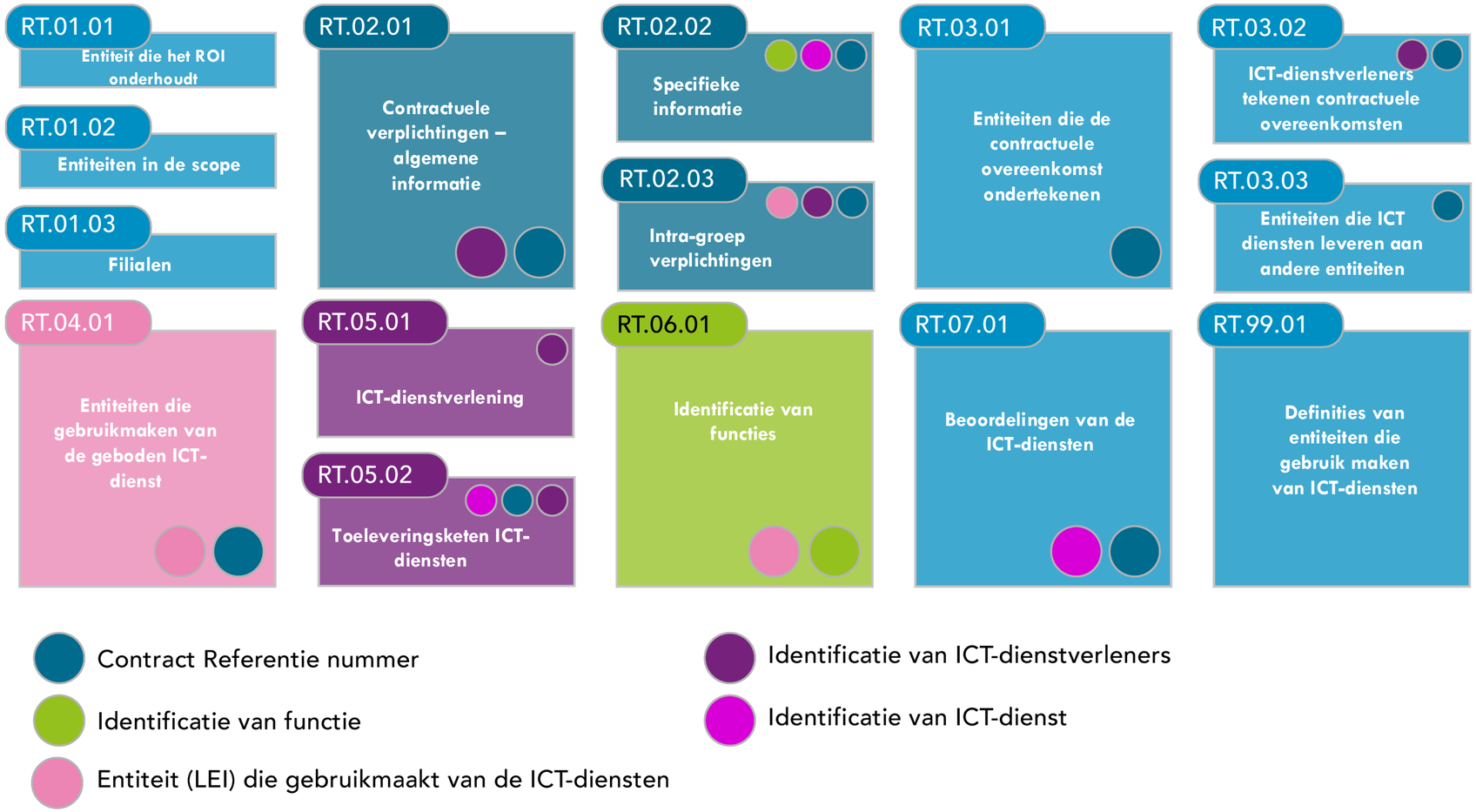
InAudit

De pijlers van DORA in vogelvlucht:

IV: ICT risicobeheer ketenpartners (2/2)

Het registreren van informatie op organisatieniveau gebeurt in 15 templates. Onderstaande afbeelding laat de onderlinge structuur van deze templates zien, waarbij wordt weergegeven hoe deze met elkaar samenhangen.

Afbeelding 1: de structuur van het informatieregister dat op organisatie- of entiteitsniveau wordt onderhouden. Afbeelding komt uit RTS artikel 28(10).



De pijlers van DORA in vogelvlucht:

V: ICT informatie uitwisseling (1/2)

DORA - ICT informatie uitwisseling

Artikel 45:
Regelingen voor uitwisseling van
informatie en inlichtingen over cyberdreiging

In Audit

De pijlers van DORA in vogelvlucht:

V: ICT informatie uitwisseling (2/2)

Informatie-uitwisseling in ‘trusted communities’

Het wordt de bedoeling dat financiële entiteiten onderling informatie en inlichtingen over cyberdreigingen uitwisselen. Het gaat dan om bijvoorbeeld gesignaleerde indicatoren voor aantasting, tactieken, technieken en procedures, cyberbeveiligingswaarschuwingen en configuratie-instrumenten, voor zover deze uitwisseling:

- ☑ Bedoeld is om de digitale operationele weerbaarheid te versterken;
- ☑ Plaatsvindt binnen ’vertrouwensgemeenschappen’ (trusted communities)
- ☑ Gebeurt met inachtname van regelingen om potentieel gevoelige informatie te beschermen

Toezichthouders worden geïnformeerd over de gesignaleerde ontwikkelingen, zodat informatie sectorbreed kan worden gedeeld en iedereen daar dus zijn of haar voordeel mee kan doen.

InAudit

DORA: niet alleen een uitdaging, maar ook een kans om uw bedrijfsvoering te versterken!

Hoe kunt u hiermee (verder) aan de slag gaan?

Om u te helpen bij het tijdig compliant zijn met DORA bieden wij u een viertal producten/ diensten aan:

1
Gap-analyse

Wij voeren voor u een gap-analyse uit om in kaart te bren-gen in hoeverre u compliant ben met DORA

2
Tool

Wij bieden u een tool om zelf een gap-analyse uit te voeren op complian-ce met DORA

3
Geïdentifi-ceerde gaps

Wij helpen u bij het oplossen van de geïdentificeerde gaps naar aanleiding van de door ons of door uzelf uitgevoer-de gap-analyse

4
Audit

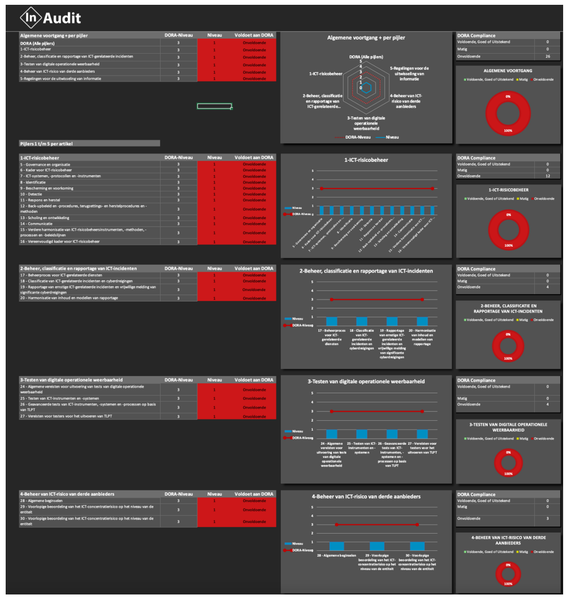
Wij voeren voor u een audit uit om compliance met DORA te toetsen

In Audit

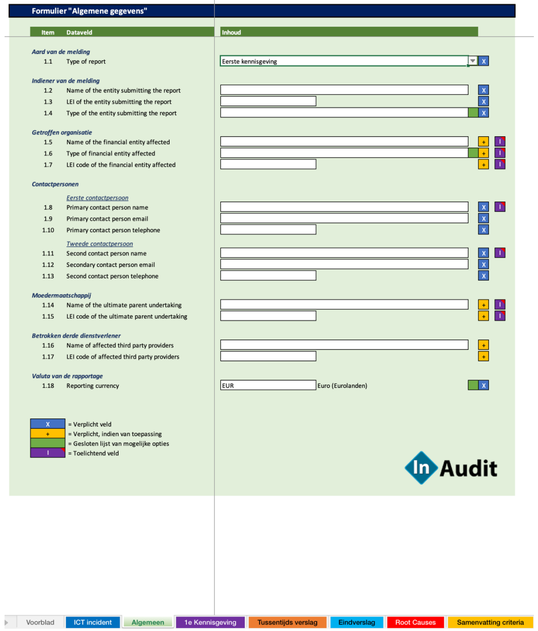
Hoe wij u kunnen helpen ?

Met praktische tools en workshops !

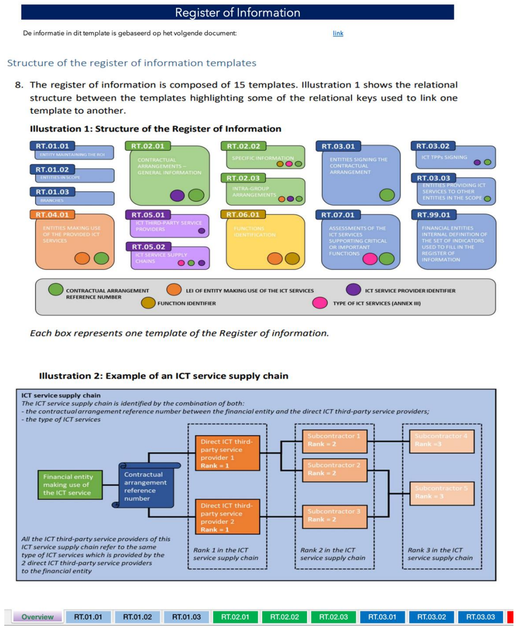
Gap-analyse tooling



Incident report tool



Informatieregister tool



Workshops en inzet

In Audit

Hoe wij u *nog meer* kunnen helpen ?

Wellicht met de uitbesteding rol van security officer/ CISO

Artikel 6 lid 4: de onafhankelijke security officer is verplicht !
"[Instellingen …] wijzen de verantwoordelijkheid voor het beheer van en toezicht op ICT-risico toe aan een **controlefunctie** en waarborgen een passend niveau van **onafhankelijkheid** van die controlefunctie om belangenconflicten te voorkomen."

De Information Security Officer (afgekort: ISO) is een belangrijke spil om DORA (en andere toekomstige regelgeving) te implementeren. De Chief Information Security Officer (afgekort: CISO) kan worden gezien als de hierboven genoemde controlefunctie, en wordt idealiter in de tweede lijn gepositioneerd.

Als de rol van ISO/CISO geen fulltime functie is …
Het benodigde budget voor informatiebeveiliging zal de komende jaren waarschijnlijk alleen hoger worden. Financiële instellingen zijn kwetsbare databedrijven die zonder toegang tot betrouwbare data niet kunnen functioneren. De rol van ISO en CISO zal voor veel organisaties echter geen fulltime functie zijn.

Uitbesteding is een interessante optie
Binnen InAudit Information Security werken specialisten met een uiteenlopend niveau van kennis en ervaring. Ieder van hen is zeer goed bekend met DORA, het Good Practice document van DNB, ISO27001 projecten en andere relevante onderwerpen. Deze expertise kan op schaalbare wijze worden ingezet, waarbij de continuïteit van de dienstverlening en de jaarlijkse investeringen in kennis en ontwikkeling op ons nemen.

InAudit

Meer weten?

Wilt u meer weten over onderstaande producten, weet ons dan te vinden!

1. Uitvoeren gap-analyse DORA
2. Tool om zelf een gap-analyse DORA uit te kunnen voeren
3. Het implementeren van de geïdentificeerde gaps naar aanleiding van de door ons of door u uitgevoerde gap-analyse DORA
4. Audit compliance met DORA

In Audit

Contact

- **InAudit BV**
  Spankerenseweg 16a
  6974 BC Leuvenheim (NL)
  T 055 – 303 2597
  W www.inaudit.nl
  E info@inaudit.nl

- **Ronald van de Langenberg RA CISA**
  Algemeen directeur
  InAudit Information Security BV
  T 06 – 24 48 68 92
  E ronald.vandelangenberg@inaudit.nl

- **Ricardo Henriques**
  Directeur Audit Services
  InAudit Audit Services BV
  T 06 – 21 37 33 66
  E ricardo.henriques@inaudit.nl

Ronald van de Langenberg

Ricardo Henriques

Niels Bokkers

Jens Meuleman

Frederike Gieles

InAudit