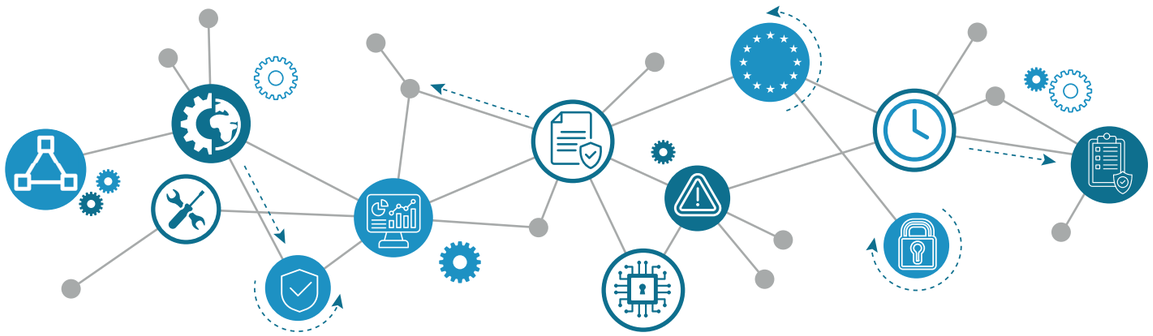
Update DORA Incident management

Hoofdstuk 3 (artikel 17 tot en met 23) van de Digital Operational Resilience Act ("DORA") gaat met name over de verplichting om "ernstige" ICT-incidenten te melden aan de toezichthouder. Met dit hoofdstuk hangen ook twee redelijk omvangrijke RTS en ITS documenten samen en overigens ook de Guidelines voor het bepalen en schatten van de kosten en verliezen als gevolg van ernstige ICT-incidenten. Deze zomer zijn enkele van deze documenten van 'consultation' naar 'final draft' gegaan en hoewel het niet schokkend anders is, is het wel iets om goed in de gaten te houden. In dit artikel brengen we enkele belangrijke veranderingen onder de aandacht.

Final draft voor het rapporteren van 'ernstige ICT-incidenten'
Het verschil tussen de versies van de (concept) DORA regelgeving zorgt wel eens voor verwarring en dat is best begrijpelijk. Veel organisaties zijn dit jaar aan de slag gegaan met DORA, maar pas deze zomer, op 17 juli, verschenen de zes laatste final reports van de ESA's (waaronder EIOPA). De 'final draft' volgt dus op de consultatieversie en de naam impliceert dat de feedback van de consultatie is meegenomen. Overigens betekent het vaak ook dat er weliswaar niets wordt veranderd, maar dat wordt uitgelegd waarom veelgehoorde feedback toch niet is verwerkt. Hoe dan ook, ook de 'final draft' is nog geen definitieve versie. Het is namelijk de versie die de ESA's aan de Europese Commissie hebben voorgelegd ter publicatie. Maar voordat de Europese Commissie dat doet, moeten ook het Europees Parlement en de Europese Raad worden gehoord. Die hebben namelijk het recht om de regelgeving nog tegen te houden. Nu zijn voor DORA de deadlines kort en de materie is behoorlijk technisch, dus het is wel reëel te verwachten dat er geen grote inhoudelijke wijzigingen meer zullen volgen. Maar 'final' betekent dus nog niet dat dit ook daadwerkelijk de regelgeving zal zijn. Let vooral bij de RTS/ITS over de rapportagetemplates op dat je met de versie van 17 juli 2024 werkt. Dat is momenteel de meest recente versie.

Versoepeling van deadlines
Voor het melden van 'ernstige ICT-incidenten' staan buitengewoon strakke deadlines. De eerste kennisgeving moet zelfs al binnen vier uur (!) na het moment van classificatie bij de toezichthouder binnen zijn en het tussentijdse verslag binnen 72 uur. Deze deadlines kunnen buitengewoon vervelend zijn als deze tijdstippen in de nacht of in het weekeinde vallen. Dat zou bijna vereisen dat iedere organisatie over een 24/7 service moet kunnen beschikken, alleen al voor rapportagedoeleinden. Het is immers niet aannemelijk dat de 'incident resolvers' deze rapportageplicht erbij kunnen nemen tijdens het beheersen van de crisis. Hierin zijn de toezichthouders de financiële industrie tegemoet gekomen. In het weekeinde en tijdens officiële vrije dagen mag de rapportageplicht worden opgeschort tot 12:00 uur op de eerstvolgende werkdag. Voor het eindrapport geldt dat de deadline niet langer ligt op een maand na classificatie, maar een maand na het laatst ingediende tussentijdse rapport.

Minder datavelden in de templates
Het rapporteren over 'ernstige ICT-incidenten' moet verplicht via voorgeschreven templates. In deze templates moeten veel gedetailleerde datavelden worden ingevuld. Veelgehoorde en ook begrijpelijke kritiek op de consultatie over de voorgeschreven templates was dat het allemaal te veel was. Daar lijkt naar geluisterd te zijn, namelijk het aantal datavelden is teruggebracht van 84 naar 59.
Maar zoals wel vaker lijkt het ook wat mooier dan het daadwerkelijk is. Zo is bijvoorbeeld het aantal velden over de kosten en verliezen van het ernstige incident teruggebracht van elf naar twee. Maar ja, in het veld 'amount of gross direct and indirect costs and losses' moet nog steeds de som worden gerapporteerd van de velden die voorheen uitgesplitst werden gevraagd.
Een ander voorbeeld is dat het veld waarmee je een reclassificatie van 'ernstig' naar 'niet-ernstig' kon invullen is verdwenen van het template. Maar de reclassificatie moet nog steeds worden gerapporteerd.
Al met al klinkt de vereenvoudiging in de zin van het aantal datavelden best significant, maar inhoudelijk hebben we niet de indruk dat alles nu veel eenvoudiger is geworden. Het is en blijft veel werk.



De kosten en verliezen als gevolg van 'ernstige ICT-incidenten'
Het aantal kostensoorten dat moet worden gerapporteerd is weliswaar afgenomen, maar de voorgeschreven opbouw van het bedrag is hetzelfde gebleven en verdient ook best extra aandacht. Overigens lijkt de laatste Guideline over de kosten van incidenten ook weer een template voor te schrijven, maar dat is waarschijnlijk vooral voor de jaarrapportage.

De componenten waaruit de bruto kosten van een incident zijn opgebouwd betreffen:
- Het bedrag aan gestolen geld of de bedragen waarvoor de organisatie aansprakelijk is;
- De kosten van vervanging van hardware, software en infrastructuur;
- De personeelskosten, inclusief extra inhuur, overwerkvergoedingen, kosten van verplaatsing van werkplekken, uitwijk en recovery, alsmede verloren werktijd;
- De kosten van boetes en niet naleving van verplichtingen
- De kosten van compensatie van klanten;
- Het verlies aan gemiste opbrengsten;
- Communicatiekosten, zowel intern als extern
- Kosten van adviseurs, waaronder (forensische) experts en juridische bijstand
- Overige kosten zoals afschrijvingen, reserveringen, overlopende schadelasten.

Veel van deze kostencomponenten zijn wellicht niet altijd eenduidig te bepalen.

InAudit tooling update
De hiervoor genoemde updates hebben we ook verwerkt in het InAudit tool voor rapportage van 'ernstige ICT incidenten'. Klanten die dit voorjaar aan de slag zijn gegaan met de eerdere versie van onze tooling kunnen bij ons de nieuwe versie opvragen. We zijn nog bezig wat laatste aanpassingen te doen, maar de nieuwe tool voor het rapporteren van 'ernstige ICT-incidenten' kunnen we waarschijnlijk snel weer uit leveren.

Oefenen, oefenen en oefenen!
Uw organisatie beschikt vast wel over een incident management procedure, maar als een crisis echt groot is, en deze DORA verplichtingen komen er bij, dan kan de spanning behoorlijk oplopen. Daarom is het ons advies om deze procedure – in elk geval vooraf – goed te oefenen. De hoofdlijnen van de procedure moeten namelijk bij iedereen voldoende in het hoofd zitten. In het geval van een ernstig incident zal de aandacht namelijk vooral uitgaan naar allerlei praktische issues en niet naar de DORA met al haar details. Maar het niet-rapporteren kan wel belangrijke non-compliance opleveren. Om deze reden adviseren we iedereen om – net zoals bij een BHV oefening - de procedure minimaal één keer per jaar te oefenen. Vanuit InAudit kunnen we u daarbij uitstekend ondersteunen.

Belangrijkste opbrengst: minder paniek en stress in het geval een crisis zich in het echt voordoet en bekendheid met deze regelgeving bij mensen die pas jaren later een verantwoordelijkheid krijgen in het proces van crisismanagement.

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