Het ISMS-raamwerk in Confluence

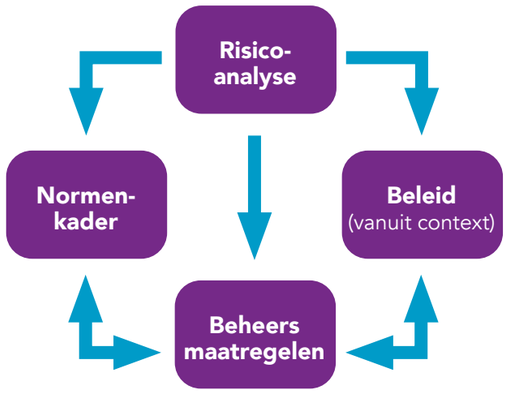
Voor alle financiële organisaties die onder de DORA vallen geldt dat ze 'moeten beschikken over een solide, alomvattend en goed gedocumenteerd kader voor ICT-risicobeheer'. Dit roept de vraag op: 'Wat is een "kader" en hoe doe je dit op een efficiënte wijze?' We hebben verschillende organisaties mogen ondersteunen op dit gebied en daarbij hebben we vaak gebruik gemaakt van het tool 'Confluence' en een opbouw en indeling die is gebaseerd op de logica die je ook in het ISO27001 normenkader terugvindt. Zo is de stap naar eventuele latere certificering ook goed te maken. In dit artikel geven we aan hoe wij dit als InAudit Information Security oppakken.

Een solide, alomvattend en goed gedocumenteerd kader

De eerste vraag is wat onder een 'solide, alomvattend en goed gedocumenteerd kader' valt. Artikel 6 lid 2 van de DORA geeft daarop het antwoord: 'Het kader voor ICT-risicobeheer omvat ten minste strategieën, beleidslijnen, procedures, ICT-protocollen en instrumenten die nodig zijn om alle informatie- en ICT-activa, […] toereikend te beschermen […].' Deze brede formulering schetst een breed scala, maar weinig voorgeschreven structuur. Om deze reden gebruiken we bij voorkeur de logische opbouw van ISO27001. Deze begint immers meer concreet met het schetsen van de context van de organisatie: de doelstelling en strategie van de organisatie, de bedrijfsprocessen, het ICT-landschap etc. Vervolgens gaat het om het identificeren van de functies, rollen, taken en verantwoordelijkheden binnen de organisatie. Vanuit deze context volgen het ICT-beleid en het informatiebeveiligings-beleid ('IB-beleid'). Het IB-beleid zelf is meestal een overkoepelend document, waarna de verschillende onderdelen daarvan, zoals back-upbeleid, patch- en updatebeleid, wachtwoordbeleid etc. separaat worden uitgewerkt. Dat maakt het onderhoud eenvoudiger. Uit het beleid volgen procedures en gezamenlijk moeten we daarmee voldoen aan de wet- en regelgeving ('de opzet').

Risico's en beheersmaatregelen

Om van opzet naar bestaan te komen moeten we over concrete beheersmaatregelen (of 'controls') beschikken. Dat ligt in lijn met het ISO27001 normenkader, maar ook in lijn met artikel 6, lid 3: 'Overeenkomstig hun kader voor ICT-risicobeheer beperken financiële entiteiten de impact van ICT-risico tot een minimum door passende strategieën, beleidslijnen, procedures, ICT-protocollen en instrumenten in te zetten […]'. Daarom is dit veelal het derde onderdeel van ons raamwerk, namelijk een overzicht van ICT-risico's en de assessment van deze risico's. Traditioneel doen we dit meestal door de kans en de impact te analyseren, zowel bruto (zonder controls) als netto (rekening houdend met de risicobeperkende werking van controls).
De beheersmaatregelen dienen primair om IB-risico's tot een acceptabel minimum terug te brengen. Maar soms moeten ze ook separaat worden gedocumenteerd, bijvoorbeeld omdat het DORA-normenkader (voorheen het DNB GPIB-normenkader) daar om vraagt. Hetzelfde geldt voor de normen uit een ISO27001-raamwerk, maar controls kunnen ook logisch volgen uit het beleid, meer dan uit de uitgewerkte risico-analyse. Hoe dan ook: wij stellen de 'eigen' beheersmaatregelen centraal in ons raamwerk. Dat zijn namelijk de controls die we ook qua werking kunnen aantonen omdat we ze werkelijk uitvoeren overeenkomstig de frequentie en op de wijze die we hebben vastgelegd. In ons raamwerk (in de context-sectie) hebben we het normenkader opgenomen en daarbij hoeven we alleen maar te verwijzen naar de interne beheersmaatregel waarmee invulling wordt gegeven aan de norm, ongeacht of dit het DORA of ISO27001 normenkader betreft.



Identify- Protect- Detect- Respond- Recover

Deze vijf stappen in het beheersen van risico's komen uit het Amerikaanse NIST raamwerk en zijn ook geland in het DORA-raamwerk. De betekenis hiervan is dat we bij risico's niet alleen moeten nadenken over hoe we deze kunnen voorkomen (identify & protect), maar dat we ook maatregelen moeten hebben om het optreden van het risico te kunnen constateren (detect) en ongedaan te kunnen maken (respond & recover). In veel raamwerken zien we nog een één-op-één relatie tussen risico's en beheersmaatregelen, maar feitelijk is dat vaak nog onvoldoende. Steeds vaker zullen we naast 'protect' controls ook 'detect, respond en recover' controls moeten opnemen om effectief aan DORA te voldoen.

Plan-do-check-act

Als we deze onderdelen hebben uitgewerkt, dan hebben we de basis gelegd voor het raamwerk, in de terming van de Demming-cyclus: 'Plan'. Nu moeten we het ook gaan doen, en het bewijs dat de controls ook daadwerkelijk zijn uitgevoerd moet worden vastgelegd. We komen daarmee van de 'plan'-fase naar de 'do-fase'. In onze beheersmaatregelen leggen we meestal de details vast, vaak aangeduid als de vijf w-'s: wie, wat, wanneer, waartoe, waar (halen we de evidence op) en geen 'w', maar ook concreet: 'hoe' (en soms 'wat als niet'). Er zijn ongetwijfeld betere tools dan Confluence om de vastlegging van de controls te verzamelen en (geautomatiseerd) te verwerken, maar met een beetje discipline werkt Confluence uitstekend. Door de datum van uitvoering (en eventueel review door de CISO) vast te leggen, kunnen eenvoudig overzichten worden gemaakt van de controls die staan gepland. Als uit de uitvoering van de controls 'acties' voortvloeien (bijvoorbeeld omdat de control een signaal oplevert), dan kan dat eenvoudig op de actielijst worden gezet.

In de 'do' fase kijken we ook naar wijzigingen in het ICT-landschap en/of de bedrijfsstrategie en analyseren we de risico's en formuleren we beheersmaatregelen die effectief zijn.
Na de 'plan' en de 'do' fase volgen de stappen die ervoor zorgen dat de volwassenheid kan stijgen naar een aantoonbaar niveau 3 of 4, namelijk het proces van continue verbetering. Deze begint met de 'check'-fase.

Digitale weerbaarheid

De effectiviteit van de maatregelen die we hebben ingevoerd wordt pas echt op de proef gesteld als we deze ook gaan testen. Dat testen is niet alleen het uitvoeren van jaarlijks dezelfde pentest. Het gaat om een programma van pentesten waarbij alle maatregelen, niet alleen de preventieve, worden getest. Het gaat daarbij ook om audits en andere analyses, bijvoorbeeld rapportages van derden. Dit geheel laat zien dat de beheersmaatregelen ook effectief zijn, of waar afwijkingen of mogelijkheden tot verbetering zijn vastgesteld. In de ISO-systematiek worden deze stelselmatig vastgelegd in een afwijkingenregister en geanalyseerd naar herstel, root-causes en het wegnemen daarvan. Bij audits bewaken we ook altijd de follow-up van de geconstateerde afwijkingen.

Alle lijntjes komen weer terug bij het bestuur

Uiteindelijk draagt het bestuur de eindverantwoordelijkheid voor de effectiviteit van het ISMS, of zoals het in artikel 5 van de DORA is vastgelegd: 'Het leidinggevend orgaan van een financiële entiteit bepaalt alle regelingen met betrekking tot het bedoelde kader voor ICT-risicobeheer, keurt deze goed, houdt toezicht op de uitvoering ervan en is ervoor verantwoordelijk.'
De output van de 'check'-fase, maar ook de kwartaalrapportages van de CISO zijn voor het bestuur van groot belang om inzicht te krijgen in de effectiviteit van het raamwerk dat is opgetuigd om de ICT-risico's te beheersen. Daarbij kan een zeker inzicht in Confluence ook helpen. In Confluence is namelijk het gehele raamwerk gedocumenteerd opgenomen en alles terug te vinden.

Als we kunnen helpen …

Als InAudit hebben we goede ervaringen met het optuigen van een ISMS-raamwerk in Confluence. Confluence is een niet al te dure tool van Atlassian en veel organisaties hebben het al in huis (bijvoorbeeld samen met JIRA). Het is een flexibel en eenvoudig te begrijpen tool dat voldoende mogelijkheden en structuur biedt om snel overzicht te bieden. Ook wijzelf als InAudit gebruiken dezelfde aanpak om onze compliance met ISO27001 te bewaken en aan te kunnen tonen.

Wilt u meer weten, dan vertellen wij er graag over!

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