DATASHEET
MexonInControl en Informatiebeveiliging

Mexon Technology gelooft dat elk bedrijf haar eigen unieke bedrijfsprocessen en business model heeft. Dat betekent dan ook dat elk bedrijf haar eigen specifieke eisen stelt aan services en ICT.

Mexon Technology's visie is dat de services voor het bedrijf en de ondersteunende ICT-systemen 'fit for purpose' en 'fit for future' moeten zijn.

Snelheid in de levering, naadloze integratie, flexibiliteit en de juiste inzet van uw (IT & Security) Service Management oplossing kunnen u aanzienlijk concurrentievoordeel opleveren.

De missie van Mexon Technology is om organisaties te helpen bij het bereiken van 'Excellence in Service Management'.

Uw security uitdaging

Organisaties en de samenleving in het algemeen worden steeds meer informatiegedreven. Gebruik van internet en smartphones, email en webapplicaties, het wordt steeds meer gezien als de meest logische manier om te werken en te communiceren.

Er zijn daardoor steeds meer manieren waarop organisaties informatie delen met de buitenwereld en het datavolume neemt sterk toe. Van sommige van deze datastromen willen we dat deze beschermd worden tegen diefstal, verminking of uitval. Om in security termen te spreken, we willen de Vertrouwelijkheid (Exclusiviteit), Integriteit en Beschikbaarheid van de data beschermen.

Het gaat hier niet alleen om de IT-kant van de informatiestroom. Bedreigingen en kwetsbaarheden doen zich overal voor, zoals bij fysieke inbraak, gladde praatjes van bedriegers, diefstal van laptops etcetera.

Om richting te geven aan beveiligings-inspanningen zijn er algemene (externe) standaarden dan wel normen ontwikkeld. Met deze handreikingen is een doordachte set aan maatregelen beschikbaar welke de beveiliging van informatie sterk kan verbeteren.

Veel organisaties hebben te maken met, of worden geconfronteerd met, een veelvoud aan standaarden.

Om dan over de volle breedte een logische èn samenhangende beveiliging te verkrijgen is geen sinecure. Komt nog bij dat weten wát je moet doen nog geen antwoord geeft op de vraag óf je dit doet en hoe goed je dit doet. In de meeste organisaties bieden de aanwezige beheer en management tools geen antwoord op dit probleem.

Beveiligingsincidenten kunnen leiden tot imago-schade, financiële schade en zelfs de bedrijfs-continuïteit serieus in gevaar brengen.

Om informatiebeveiliging in te richten zijn er algemene (externe) standaarden dan wel normen ontwikkeld die organisaties kunnen of moeten toepassen, zoals de ISO27001, ISO27002, ISO28000, NEN7510 en de hiervan afgeleide branche specifieke normen BIR (Rijksoverheid), BIG (Gemeenten), IBI (Provincies) en BIWA (Waterschappen).

Hierdoor zijn security verantwoordelijken vaak genoodzaakt om zelf nog een eigen informatiesysteem, veelal Excel-spreadsheets, in de lucht te houden om alsnog goed en snel inzicht te krijgen in bijvoorbeeld de actuele status van en de samenhang tussen relevante norm, controls, maatregelen, acties, activiteiten, assets en resources.

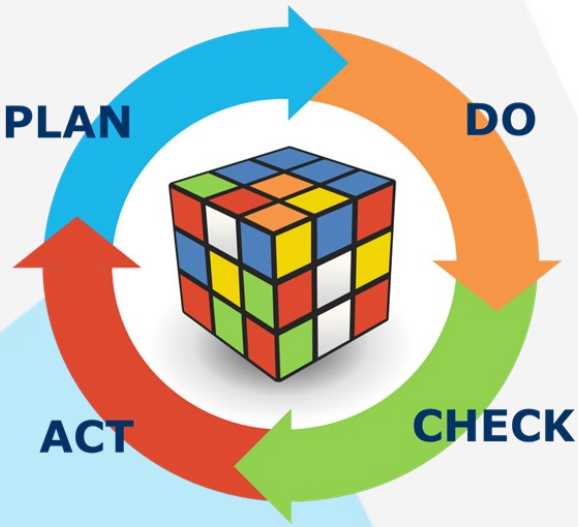
Implementatie, vastlegging en onderhoud van het Information Security Management System (ISMS)

Complexiteit

De complexiteit van het control- en maatregelenstelsel behorende bij een norm is groot en het 'pas-toe-of-leg-uit'-regime is streng. Aanbevolen wordt dan ook om planmatig een zogenaamd Information Security Management System, ofwel ISMS, in te richten, te vullen en te onderhouden.

Een ISMS is de vastlegging en het onderhoud (verbetercyclus) van de complete set van maatregelen, processen en procedures in het kader van informatiebeveiliging. Deze complete set is de manier dan wel methode hoe een organisatie met informatiebeveiliging omgaat.

De kern van het ISMS is de Plan-Do-Check-Act-cyclus (PDCA-cyclus). 'Plan' geeft invulling aan het beleid en de scope ten aanzien van het ISMS, 'Do' geeft invulling aan de uitvoering van het ISMS, 'Check' geeft invulling aan de monitoring van het ISMS en 'Act' geeft invulling aan het onderhouden en verbeteren van het ISMS.



Het ISMS op zich is overigens niet de garantie voor 100% veiligheid maar is een managementsysteem dat organisaties helpt om 'in control' te zijn of te geraken over hun informatiebeveiliging.

Huidige opzet

Veel organisaties en externe adviseurs zijn in het kader van informatiebeveiliging primair gericht op het inventariseren van risico's, het uitvoeren van gap-analyses, het vastleggen en publiceren van processen, procedures, maatregelen, statusbepaling, rapportages, auditing, etcetera.
Aanzienlijk minder aandacht is er voor de initiëring, toewijzing en besturing van acties, activiteiten en resources die benodigd zijn om een security incident op te lossen of een maatregel geïmplementeerd te krijgen en te onderhouden.
Ook het inrichten en initieel vullen van het ISMS gebeurt vaak onvoldoende efficiënt of met gebrekkige samenhang tussen IT-processen en (de veel breder georiënteerde) security raamwerken.

Doorgaans worden de operationele processen gemanaged vanuit de aanwezige IT Service Management (ITSM) tooling. Echter, de samenhang met de informatie die in de GRC- en/of ISMS-tooling zit ontbreekt in de meeste gevallen. Bijkomend probleem is dat de ITSM-database over het algemeen alleen gegevens bevat over IT-assets, zoals applicaties en hardware en niet vanzelfsprekend ook gegevens bevat over de non IT-assets, die zoals aangegeven ook onderdeel zijn van de informatiebeveiligingsketen.

ISMS implementaties zijn van nature meer te zien als een programma dan als een project. Een zeer brede scope, een groot aantal doelgroepen en stakeholders, diversiteit in complexiteit en prioriteit... Het is snel duidelijk dat de gebruikelijke projectmanagementmethodieken snel tekort kunnen schieten.

Een andere uitdaging is dat de van toepassing zijnde norm op zich ook kan veranderen, omdat de externe normen sterk aan elkaar gerelateerd dan wel van elkaar afgeleid kunnen zijn. Een aanpassing van de ene norm kan leiden tot een aanpassing in de andere norm, waardoor een organisatie mogelijk te maken krijgt met andere maatregelen, acties en activiteiten. Deze zogenaamde kruislijsten (met de relaties tussen de van toepassing zijnde normen) vormen in de praktijk grote hoofdbrekens voor de security verantwoordelijken.

Onze oplossing: MexonInControl

Ondersteuning

Onze MexonInControl ISMS-software wordt ontwikkeld om security verantwoordelijken, zoals de Chief Information Security Officer (CISO) of Information Security Officer (ISO), te ondersteunen bij het bewaken van, informeren en rapporteren over de status van de vastgelegde controls en maatregelen.

Vergroot inzicht

Via een cyclische proces (plan/do/check/act) worden een risicobeoordeling, de te treffen maatregelen, het bewaken van de voortgang en beoordelen van de status van de maatregelen aangestuurd. Dit leidt tot inzicht in de status van het traject om compliance te bereiken en te handhaven, alsook tot inzicht in volwassenheid en/of werking van maatregelen (opzet, bestaan en werking).

Procesbenadering
MexonInControl biedt een organisatie een procesbenadering voor het beheersen van de informatiebeveiliging. Dit leidt tot betere controle en verminderde auditlast. Hiervoor is een krachtige workflow engine ingericht.

Integratie met bestaande ITSM-tools
MexonInControl laat bestaande ICT-beheerprocessen intact en kan door slimme integratie met bestaande ITSM-tools relevante data gebruiken voor analyse en rapportage. Dit betreft onder andere informatie over het applicatielandschap, de status van bijvoorbeeld antivirusmaatregelen, de voortgang van IT- projecten of changes.

'In control'
MexonInControl helpt bij het voldoen aan een informatiebeveiligingsnorm, het compliant blijven aan de norm en het volledig en aantoonbaar 'in control' zijn over de informatiebeveiliging. Bovendien maakt het het onderhoud van de norm zelf ook eenvoudig.

Ondersteuning van normen
MexonInControl kan toegepast worden op alle algemene en branche specifieke normen op het gebied van informatiebeveiliging, waaronder: ISO27001, ISO27002, ISO28000, NEN7510, VIR, BIR, BIG, IBI, BIWA, etcetera.

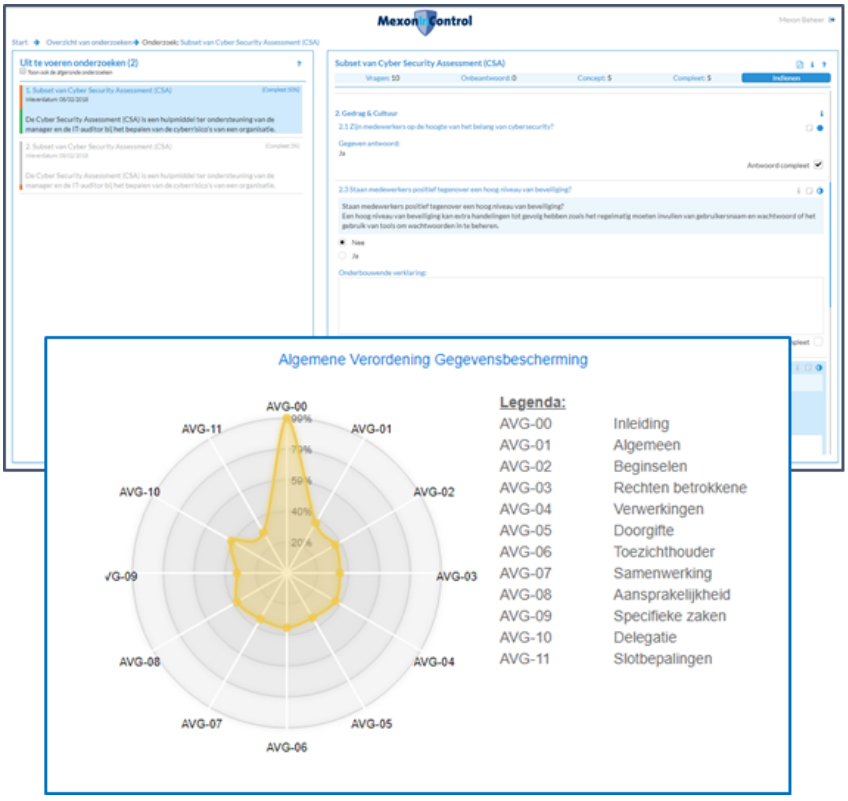
Interne en externe escalatie
Ondanks alle pogingen om privacygevoelige

gegevens van personen en ketenpartners te beschermen zullen er zich toch security incidenten voordoen.

MexonInControl wordt ontwikkeld om incidenten van de categorie die gemeld moeten worden aan de CISO te registeren en af te wikkelen via vooraf ontworpen reacties en eventuele escalatieprocedures.

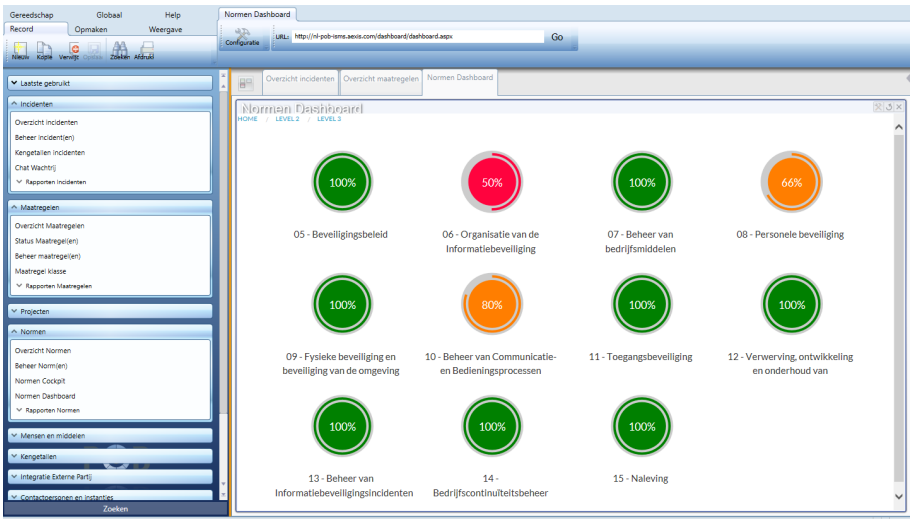
Deze incidenten zullen veelal ook gemeld moeten worden aan bijvoorbeeld Autoriteit Persoonsgegevens en IBD. Het interne en externe escalatieproces wordt volledig door MexonInControl ondersteunt via workflow en koppelingen naar standaard formulieren, etcetera.

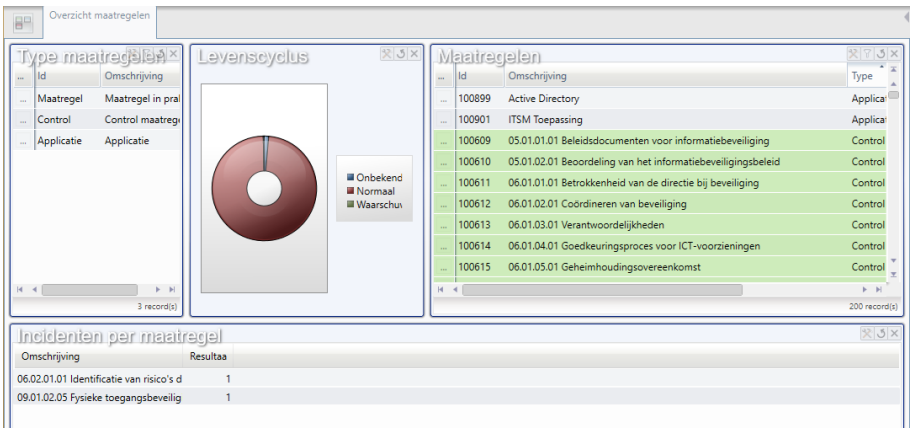
MexonInControl



De voordelen voor u van MexonInControl op een rijtje:

- Voorgedefinieerde en aanpasbare set van controls en maatregelen;
- Eenvoudig inzicht in status en volwassenheid van de controls, inclusief het meten van de opzet, bestaan en werking van de maatregelen bij een control;
- Voorgedefinieerde en aanpasbare workflows en activiteitenplanning voor ad hoc en repeterende acties en activiteiten;
- Eenduidig inzicht in de samenhang tussen risico's, maatregelen, acties, activiteiten, resources (waaronder capaciteit, ICT assets, etcetera);
- Flexibele dashboards en rapportering voor snel overzicht en minimale auditlast;
- Eenvoudig uploaden van kruislijsten en updaten van de norm, controls en maatregelen [op termijn];
- Separate database voor borging vertrouwelijke data;
- Eén gebruikersvriendelijke geïntegreerde applicatie voor alle informatiebeveiligingsprocessen;
- Geïntegreerde, voorgedefinieerde en aanpasbare control plans;
- Slimme integratie met ITSM-tooling voor actuele informatie t.b.v. analyse en rapportage;
- Faciliteren van interne en externe escalatie;
- Een tool dat u voorbereidt op en assisteert bij audits en samenwerking met betrokkenen binnen de security keten optimaliseert;
- In te richten en toepasbaar voor alle informatiebeveiligingsnormen;
- En meer…





Nederland
Plesmanstraat 2
3833 LA Leusden
+31 (0) 33-4321700
www.mexontechnology.nl

België
Leuvensesteenweg 392B
1932 Sint-Stevens-Woluwe
+32 (0) 2-7251644
www.mexontechnology.be

Frankrijk
Immeuble Technologies
84/88 bd de la Mission Marchand
92411 Courbevoie Cedex
+33 (0) 1-49-04-71-71
www.mexontechnology.fr

Neem contact met ons op:
sales@mexontechnology.com

Bezoek onze website op:
www.mexontechnology.com

Mexon Technology
is onderdeel van de Aexis Group