DIGITAAL VLAANDEREN

/// Vo Informatieclassificatieraamwerk

INFORMATIEVEILIGHEID

DE LEIDEND AMBTENAAR AAN ZET

Een handreiking voor leidend ambtenaar en CISO

Versie/// 1.0

Publicatiedatum/// augustus 2023

Vlaamse overheid

www.vlaanderen.be/digitaalvlaanderen

Classificatie: Klasse 1

Documenthistoriek

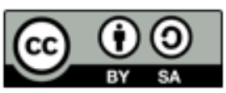
Versie	Opmerking	Datum	Auteur	Status
1.0	Versie ter publicatie	Augustus 2023	Team Informatieveiligheid	Finaal

Classificatie

Dit document valt onder de vertrouwelijkheidsklasse 1 (Publiek) en mag toegankelijk zijn voor iedereen.

Dankwoord

Een speciaal woord van dank gaat uit naar het Centrum Informatiebeveiliging en Privacybescherming in Nederland van wie het bronmateriaal 'De bestuurder aan zet' mocht gebruikt en herwerkt worden bij het opstellen van deze handreiking.



INHOUD

1 INLEIDING

1.1 DOELGROEP

De doelgroep van deze handreiking zijn leidend ambtenaren en security officers (informatieveiligheidsconsulenten). Dit is een informatief instrument om te helpen bij het ontwikkelen en afstemmen van een jaarlijks verbeterplan voor Informatieveiligheid.

In dit document wordt ook het begrip ‘bestuur’ of ‘bestuurder’ gebruikt. Hiermee wordt bedoeld de eindverantwoordelijke die aansprakelijk is. Het is afhankelijk van de politiek-bestuurlijke context wie in een organisatie de eindverantwoordelijke is voor Informatieveiligheid.

1.2 HET BELANG VAN INFORMATIEVEILIGHEID

Het thema Informatieveiligheid is de laatste jaren steeds belangrijker geworden door de toegenomen digitalisering van de maatschappij. We worden afhankelijker van informatietechnologie en de daarmee gepaarde kwetsbaarheden en dreigingen. U kent de voorbeelden vast uit het nieuws. Overheidsinstanties en andere organisaties die gegijzeld worden door hackers en niet meer bij hun gegevens kunnen zonder betaling. Of vertrouwelijke gegevens liggen na een datalek op straat. Die dreigingen worden steeds groter en dat stelt hogere eisen aan de organisatie. En daarmee bent u als leidend ambtenaar aan zet.

De Vlaamse overheid verzamelt en verwerkt meer en meer gevoelige data van burgers, bedrijven en organisaties om haar publieke opdracht te kunnen vervullen. Maar ook om de wensen van gebruikers met een meer gepersonaliseerde en geautomatiseerde dienstverlening te beantwoorden. De samenleving verwacht dat de Vlaamse overheid zorgvuldig met die informatie omgaat en ze voldoende beschermt.

Permanente aandacht voor Informatieveiligheid binnen de Vlaamse overheid is van kritisch belang voor het succes van een veilige digitale samenleving en moet breed gedragen en verankerd worden in de bestuurdersverantwoordelijkheid van leidend ambtenaren en directiecomités.

1.3 VO INFORMATIECLASSIFICATIERAAMWERK

Het Informatieclassificatieraamwerk (ICR) van de Vlaamse overheid is een set van beleidslijnen en minimale maatregelen voor de veilige verwerking van informatie. De basis van het raamwerk wordt gevormd door vijf informatieklassen voor de drie kwaliteitskenmerken: vertrouwelijkheid, integriteit en beschikbaarheid van informatie.

De klasse bepaling is cruciaal, omdat het de basis is voor de selectie en implementatie van beheersmaatregelen. Hoe gevoeliger de informatie, hoe zwaarder de beveiliging van de informatie.

Minimale maatregelen zijn verplicht volgens het ‘pas toe of leg uit’ principe. Minimale maatregelen worden geïmplementeerd tenzij er expliciet wordt geformuleerd waarom niet én of er alternatieve maatregelen worden toegepast om een evenwaardig veiligheidsniveau te bereiken.

Voor meer informatie bezoek:
Informatieclassificatieraamwerk van de Vlaamse overheid

1.4 WETTELIJKE VERANKERING

De Vlaamse regering heeft in de ministerraad van 15 oktober 2021 de strategie voor Informatieveiligheid binnen (de dienstverlening van) de Vlaamse overheid goedgekeurd. Hiermee bekrachtigt de Vlaamse regering de toepassing van het Informatieclassificatieraamwerk (ICR) en maakt deze bindend. De scope van de nota is de Vlaamse administratie zoals bepaald in het bestuur decreet van 7 december 2018.

Voor meer informatie bezoek:
Bestuur decreet 7 december 2018
Ministerraad van 15 oktober 2021

Implementatiemijlpalen
Het Vo Informatieclassificatieraamwerk is bindend voor de Vlaamse administratie. Alle entiteiten moeten deze implementeren volgens de volgende tijdlijnen:

- Voor informatie van klasse 3, 4 en 5: 31 december 2024
- Voor informatie van klasse 1 en 2: 31 december 2026

1.5 AANSPRAKELIJKHEID BIJ DE LEIDEND AMBTENAAR

Om rollen, verantwoordelijkheden en aansprakelijkheid scherp te stellen, heeft de strategie Informatieveiligheid het begrip eigenaarschap genoemd als belangrijk verbeterpunt. Een aansprakelijke eigenaar is altijd een directielid met budgetbevoegdheid die een beslissing kan nemen over informatieveiligheidsrisico's en mogelijke implicaties op de werking van de entiteit specifiek en haar rol binnen de Vo in haar geheel.

In de regel is de leidend ambtenaar of administrateur-generaal van een entiteit de aansprakelijke eigenaar voor Informatieveiligheid. Net zoals deze functie ook aansprakelijk is voor bijvoorbeeld een gezonde financiële huishouding van de entiteit.

In de context van Informatieveiligheid is de eigenaar aansprakelijk voor de uitvoering van het informatieveiligheidsbeleid. Dit omvat onder andere de vertaling van de minimale maatregelen uit het Vo-brede Informatieclassificatieraamwerk naar specifiek informatieveiligheidsbeleid en implementatie binnen de eigen entiteit en het actieve beheer en acceptatie van (rest)risico's.

Een eigenaar kan ervoor kiezen om de verantwoordelijkheid te delegeren. Een gedelegeerd eigenaar moet rechtstreeks rapporteren aan een eigenaar en mag in diens naam sturen en beslissingen nemen over risico's

en budgetten. Deze verantwoordelijkheid mag een gedelegeerd eigenaar niet nogmaals delegeren naar een lager niveau. Een typisch profiel hiervoor is dikwijls een directielid, afdelings- of diensthoofd.

Deze rol mag niet toegewezen worden aan tijdelijke contracten (bijvoorbeeld consultant) en mag enkel toegewezen worden aan een extern profiel na goedkeuring door een leidend ambtenaar of administrateur-generaal. Een gedelegeerd eigenaar is verantwoordelijk, maar de eigenaar blijft aansprakelijk.

Voor meer informatie bezoek:

Vlaamse strategie Informatieveiligheid

Bestuurlijke principes voor Informatieveiligheid

Eigenaarschap, rollen en verantwoordelijkheden voor Informatieveiligheid

1.6 SAMENSPEL MET DE CISO OF INFORMATIEVEILIGHEIDSCONSULENT

De Chief/Corporate Information Security Officer (CISO) is een beroepsprofiel dat vandaag in veel organisaties te vinden is. Binnen de Vlaamse overheid komt de CISO niet veel voor, maar zijn er wel gelijksoortige rollen zoals informatieveiligheidsconsulenten. Soms vervult een DPO (Data Protection Officer) een dubbelrol en is dan ook verantwoordelijk voor Informatieveiligheid, naast het toezicht op de bescherming van persoonsgegevens.

De CISO-rol moet een organisatie-ondersteunende rol op strategisch/tactisch niveau vertegenwoordigen. De CISO is verantwoordelijk voor beleidsvorming, dreigingsanalyses, overzicht en aggregatie van risico's en toezicht op naleving. Daarnaast adviseert en ondersteunt de CISO de organisatie bij bijvoorbeeld informatieklassebepalingen, risicoanalyses en beheersmaatregelen.

De aanstelling van een CISO of gelijkwaardige rol binnen de entiteiten van de Vlaamse overheid is niet verplicht, maar ten sterkste aan te bevelen. Eventueel kan de rol gecombineerd worden met een andere organisatie-ondersteunende rol of als dienst ingekocht worden (CISO-as-a-Service).

Informatieveiligheid krijgt in de praktijk handen en voeten in een samenspel tussen het (top)management en de experten. Soms is dit samenspel lastig, omdat de interactie voor de topmanagers te veel gaat over technische details. Ze haken hierdoor af en het gevolg is dat de sturing op Informatieveiligheid het exclusieve terrein wordt van de CISO zonder de juiste en gewenste betrokkenheid van het management.

Handreiking

Deze handreiking biedt leidend ambtenaren, bestuurders en experten handvatten en een stappenplan om Informatieveiligheid in samenspel daadwerkelijk tot 'chefsache' te maken. Zodat bestuurders bewust en goed geïnformeerd keuzes kunnen maken over de informatieveiligheidsrisico's die de organisatie loopt en ze actief sturing kunnen geven in deze context.

Deze handreiking biedt ook een goed uitgangspunt om verantwoording af te leggen over risico's, keuzes, maatregelen en beleid.

Voor meer informatie bezoek:
De rol van de CISO – Blauwdruk en profiel

1.7 ORGANISATIEBEHEERSING

Informatieveiligheid gaat over veel meer dan computersystemen en hackers. Informatieveiligheid is een kwaliteitskenmerk en gaat over het beheren van de risico's rond informatie en informatieverwerking. Een groot deel van de beheersmaatregelen zijn van organisatorische aard en zijn niet-technisch. Daarnaast speelt het menselijke aspect, veelal gezien als de zwakste schakel, ook een grote rol in veiligheid.

Vaak gaat het bij cyberinbraken over de kwetsbaarheid en beperkte beveiliging van computersystemen. Als er iets verder wordt gekeken naar de hoofdoorzaken, dan wijzen die vaak in de richting van gebrek aan beheerprocessen, onduidelijke verantwoordelijkheden, geen goede afspraken met leveranciers, trage besluitvorming, ontoereikend budget, enz.

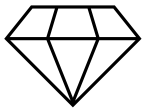
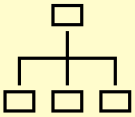
Deze oorzaken vallen bijna allemaal onder de categorie organisatiebeheersing. Organisatiebeheersing heeft als doel beheersmaatregelen in te bouwen in alle activiteiten en processen zodat de doelstellingen efficiënter en effectiever kunnen worden gerealiseerd.

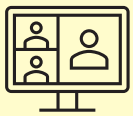
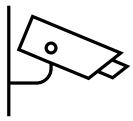
De Vlaamse overheid maakt elke dag weer werk van het realiseren van haar missie en de daaruit voortvloeiende doelstellingen. Om de realisatie van de doelstellingen te faciliteren, heeft de Vlaamse overheid beleid met betrekking tot organisatiebeheersing ontwikkeld. Een hulpmiddel hierbij is de leidraad interne controle en organisatiebeheersing.

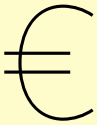
Voor meer informatie bezoek:
Organisatiebeheersing Vlaamse overheid
Leidraad interne controle en organisatiebeheersing Vlaamse overheid

2 HANDVATTEN

Dit hoofdstuk benoemt 10 verschillende onderwerpen die samen de basis vormen en helpen bij een goed gesprek tussen de leidend ambtenaar en de CISO of informatieveiligheidsconsulent. Deze onderwerpen hangen nauw samen met de eisen van het Vo Informatieclassificatieraamwerk. Deze handvatten zijn bedoeld om te bepalen wat de (jaarlijkse) prioriteiten zijn en welke beheersmaatregelen nodig zijn om risico's op een aanvaardbaar niveau te krijgen en om continu te monitoren en bij te sturen.

	Onderwerp	Aandachtspunten
1	**Identificeer en bescherm de kroonjuwelen** 	De kroonjuwelen zijn die gegevens, processen, producten en diensten die (de continuïteit van) de dienstverlening en bedrijfsvoering van de entiteit in gevaar brengen als er iets mee gebeurt. De informatieklassebepaling en een risicoanalyse helpen bij het inzichtelijk krijgen van welke informatievoorzieningen cruciaal zijn en welke gegevens zeker niet op straat mogen komen te liggen.
2	**Kijk verder dan de eigen organisatie** 	Maak goede contractuele afspraken met leveranciers en ketenpartners en zorg voor regelmatige afstemming over Informatieveiligheid om risico's op een acceptabel niveau te brengen en te houden. Eis van leveranciers en partners dat ze volgens industriestandaards voor Informatieveiligheid werken en er een onafhankelijke toetsing plaatsvindt.
3	**Zorg dat wat veilig is, ook veilig blijft** 	Installeer tijdig security-updates om nieuwe technische bedreigingen het hoofd te kunnen bieden. Vervang op de tijd oude software. Zorg ervoor dat producten en diensten veilig ontworpen en ontwikkeld worden vanaf de start en niet achteraf.
4	**Veilig werken, ook thuis**	Pas sterke authenticatie systematisch toe, bij voorkeur two-factor. Stel hoge(re) eisen aan bijzondere toegang. Beveilig naast de infrastructuur en centrale applicaties ook

		gebruikersapparatuur zoals laptops en andere draagbare apparatuur.
5	**Afscherming, detectie, monitoring en response** 	Bescherm de toprisico-applicaties door segmentatie tegen domino-effecten. Voorkom dat uitval van een applicatie leidt tot uitval van andere applicaties of zelfs de gehele infrastructuur. Zorg voor detectie, monitoring en response met centrale diensten zoals een Computer Emergency Response Team (CERT) of een Security Operations Centre (SOC).
6	**Effectief handelen bij incidenten en crisis** 	Zorg voor een waterdichte herstelaanpak voor toprisico-applicaties. Zorg voor voldoende afhandeling van incidenten en oefen regelmatig met cybercrisismanagement.
7	**Meet, leer en stuur bij** 	Laat de kwaliteit van informatieveiligheidsprocessen met self-assessments en reviews van toprisico-applicaties meten door een onafhankelijk team of externe partij.
8	**Verhoog het bewustzijn van medewerkers in een veilige cultuur** 	Zorg voor regelmatige bewustmakingcampagnes gericht op alle medewerkers om het bewustzijn van veiligheidsrisico's te verhogen. Organiseer specifieke trainingen voor belangrijke doelgroepen en houd medewerkers alert met bijvoorbeeld phishing campagnes of het simuleren van cyberaanvallen. Creëer en stimuleer een open en veilige cultuur waarin medewerkers zich veilig voelen om risico's en incidenten te melden, óók als hun eigen gedrag daarbij een rol heeft gespeeld.
9	**Definieer rollen en verantwoordelijkheden**	Definieer duidelijke rollen en verantwoordelijkheden op alle niveaus van directie en hoger management tot en met uitvoerende medewerkers. Leg hierbij de verantwoordelijkheid

		voor Informatieveiligheid en risicobeheer ook bij de eigenaren van processen, producten en diensten. Stel een CISO of een informatieveiligheidsconsulent aan met voldoende mandaat om een beleidsvormende, adviserende en ondersteunende rol te spelen met focus op overkoepelende risicoanalyses en –aggregatie, en toezicht op naleving en rapportering aan de directie. Zorg voor duidelijke scheiding van rollen ten voordele van de kwaliteit en veiligheid.
10	**Zorg voor voldoende middelen en capaciteit** 	Stel voldoende budget en middelen beschikbaar voor de uitvoering van het informatieveiligheidsbeleid.

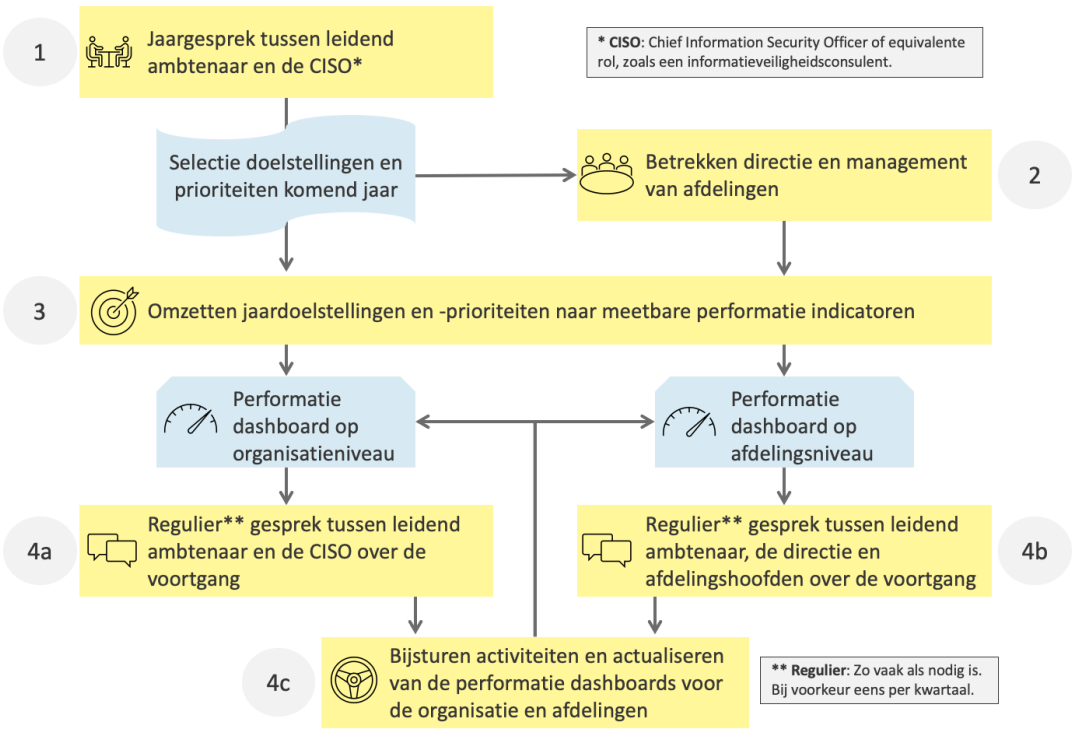
3 VAN GESPREK TOT STURING: EEN AANPAK

3.1 INLEIDING

Met de handvatten uit het vorige hoofdstuk kunnen de weerbaarheid, het herstelvermogen en een continu verbeter- en leerproces in samenhang besproken worden. Sturing begint met goede gesprekken tussen de leidend ambtenaar en de CISO of informatieveiligheidsconsulent. U leert elkaars werelden en opgaven beter te begrijpen. Incidenten met grote impact op Informatieveiligheid komen steeds meer voor. Met goede sturing en een grondige aanpak zijn de kansen op een onvoorspelbare en slechte afloop tot een aanvaardbaar niveau terug te brengen. Die aanpak begint met een gesprek over de zorgen en prioriteiten van de bestuurders gebruikmakend van bovenstaande handvatten.

Een volgende stap is om samen afspraken te maken over wat de organisatie wil bereiken op het gebied van Informatieveiligheid en de te nemen maatregelen daarvoor. In dit hoofdstuk vindt u de handvatten meer geduid samen met een aantal vragen die u kunt stellen. De gerichte vragen geven u tijdens het gesprek meer grip op de Informatieveiligheid van uw organisatie, maar ook daarna. Door regelmatig de voortgang en nieuwe ontwikkelingen te bespreken, komt u als bestuurder steeds meer aan het roer. Een gesprekscyclus op basis van afspraken en een periodieke rapportage op basis van meetbare performantie indicatoren, stellen u in staat steeds actiever te sturen en bij te sturen.

3.2 JAARCYCLUS



3.3 STAPPENPLAN

De leidend ambtenaar is als aansprakelijke eigenaar aan zet. De CISO of informatieveiligheidsconsulent kan of zal het initiatief moeten nemen in het organiseren van de voorbereiding van gesprekken en de vastlegging van hetgeen besproken is. Ook de verdere uitwerking van het verbeterplan, de ontwikkeling van performantie indicatoren en de opzet van een dashboard, maken deel uit van zijn rol.

Stap 1 Gesprek tussen de leidend ambtenaar en de CISO of informatieveiligheidsconsulent

1. Plan een (jaar)**gesprek** tussen de leidend ambtenaar en CISO. Het gesprek dient minstens de volgende twee onderwerpen te bevatten: 1) De doelstellingen van de organisatie en hoe Informatieveiligheid daaraan bijdraagt, 2) De grootste zorgen en prioriteiten van de bestuurder voor Informatieveiligheid. Gebruik als kapstok de 10 handvatten uit het vorige hoofdstuk.
2. Bespreek de belangrijkste onderwerpen. Gebruik hierbij de **vragenlijst** als kapstok (bijlage A) of stel uw eigen vragenlijst op en bespreek de belangrijkste aspecten. Noteer per onderwerp de vragen die de bestuurder heeft.
3. Verwerk de antwoorden in een **jaarprioriteitenoverzicht** op basis van de handvatten. Voor de CISO is het aan te bevelen om voorafgaand aan het gesprek al een concept met een prioriteitenoverzicht op te stellen en deze dan tijdens of na het gesprek bij te werken.
4. Schrijf een **gespreksverslag** en deel dit met de bestuurder.
5. **Beschrijf en documenteer de opdracht** en deel deze met de managementteams van de verschillende afdelingen om ze in de scope te betrekken. Je kan dit doen met een opdrachtbrief (zie voorbeeld in appendix B). In deze opdrachtomschrijving of opdrachtbrief benadrukt de leidend ambtenaar het belang van Informatieveiligheid en de betrokkenheid van de directie en het hogere management. Communiceer hierin ook duidelijk dat dat er verwacht wordt dat de dashboards, status en vooruitgang regelmatig besproken worden en dat de prioriteiten worden bijgewerkt.

Stap 2 Betrekken directie en management van afdelingen

Gebruik de opdrachtbrief voor het gesprek met (de leden van) de afdelingsmanagementteams en met de informatieveiligheidsmedewerkers en andere belanghebbenden.

Bijvoorbeeld met de volgende stappen:

1. Informeer de in de opdrachtbrief vermelde -direct betrokkenen- over de **goedkeuring** van de **prioriteiten** en de rapportage daarover door de leidend ambtenaar.
2. Deel het concept **jaarprioriteitenoverzicht** met de afspraken over rapportage en een concept dasboard.
3. Plan **vergaderingen** in de agenda's om deze stukken met iedereen individueel of in groepjes door te nemen en om **aanvullingen** en **verbetersuggesties** te verkrijgen.

Stap 3 **Omzetten jaardoelstellingen en -prioriteiten naar meetbare performantie indicatoren**

1. Verwerk alle verzamelde **input** en **feedback** in een aansprekend **dashboard** met duidelijk gedefinieerde **performantie indicatoren**. Overweeg hierbij om specifieke dashboards op te zetten op afdelingsniveau en op organisatieniveau voor de directie.
2. Bespreek het **proces** rond de **statusupdate** van de dashboards met de betrokkenen op directie- en afdelingsniveau, afhankelijk van de vastgestelde scope en prioriteiten. Streef naar het tijdig plannen van de statusupdates en zorg dat het **geagendeerd** is op de **vergaderingen** van directie en managementteams.
3. Afhankelijk van managementstijl en organisatiecultuur, en indien haalbaar, kan worden overwogen om een **competitie-element** in te brengen om op een ludieke manier de organisatie te stimuleren om proactief te werken aan de verbetering van Informatieveiligheid en zichtbare voortgang op de dashboards.

Stap 4 **Reguliere gesprekken tussen leidend ambtenaar, de directie, afdelingshoofden en de CISO over de voortgang, het bijsturen van activiteiten en het actualiseren van de dashboards**

1. **Bespreek** regelmatig (bij voorkeur ieder kwartaal) met de managementteams van de afdelingen hun **status**. Zorg er voor dat iedere afdeling in scope een aanspreekpunt of coördinator heeft. Het is niet de taak van de CISO om de leiding te nemen in alle afdelingsspecifieke verbeteractiviteiten.
2. **Bespreek** het **gecombineerde dasboard** met statussen van de gehele organisatie met de leidend ambtenaar en de directie.
3. **Bespreek** naast de status ook mogelijk gewenste **verbeteringen** en **uitbreidingen**.
4. **Evalueer** de uitkomsten van de reguliere gesprekken ter **verbetering** van het overkoepelende **informatieveiligheidsbeleid** en **praktische hulpmiddelen** en hoe de organisatie verder of beter geholpen kan worden door de CISO en experten. Op deze manier is er een continue verbeteraanpak met een regelmatige voortgangsrapportage.

Advies: Stap voor stap invoeren

Ieder begin is moeilijk, zo ook het verbeteren van Informatieveiligheid. U zult wellicht weerstand ondervinden in de organisatie die overwonnen moet worden. Informatieveiligheid wordt immers vaak (ten onrechte) gezien als een technisch ICT-probleem en geen business probleem.

Aanbeveling is om verbeteringen gefaseerd in te voeren, bijvoorbeeld als volgt:

- Kies jaarlijks 3 onderwerpen uit de set van handvatten
- Pak er elk jaar 3 nieuwe onderwerpen bij
- Continueer de rapportages in volgende jaren totdat uiteindelijk alle onderwerpen op het dashboard staan

Na het eerste jaar is het de uitdaging om de aandacht vast te houden. Dat gebeurt door het besef van urgentie levend te houden en jaarlijks de prioriteiten bij te stellen. Blijvende aandacht en sturing van de leidend ambtenaar en de directie is daarbij onontbeerlijk.

4 BIJLAGE A: VRAGENLIJST

Deze vragenlijst is bedoeld als voorbeeld en leidraad voor het gesprek over Informatieveiligheid tussen de leidend ambtenaar en/of zijn/haar gedelegeerde(n) en de CISO of informatieveiligheidsconsulent.

De kritische performantie indicatoren (KPI's) zijn suggesties om de vragen te vertalen in meetbare acties en resultaten. Een periodiek gesprek over deze vragen en de rapportage over de realisatie van de KPI's, kan de bestuurder helpen zijn rol te pakken.

Dit gesprek is overigens niet alleen nodig met de bestuurders, maar ook op afdelingsniveau, met de managementteams. Zij zouden zelf, in samenspraak met de directie, kunnen bepalen op basis van risicoafwegingen aan welke van de onderwerpen zij prioriteit willen geven.

Vragen	**Kritische performantie indicatoren (KPI)**
1. Identificeer en bescherm de kroonjuwelen	
Wat zijn de kroonjuwelen? Welke processen en systemen zijn kritisch voor de organisatie ervan? Wat zijn de toprisico's? Is per kroonjuweel vastgesteld wat de juiste maatregelen zijn om de risico's terug te brengen naar een aanvaardbaar niveau?	Kroonjuwelen en toprisico's zijn afgestemd Audit- of reviewplan wordt uitgevoerd volgens planning Lijst met kroonjuwelen en toprisico's is beschikbaar en besproken met de verantwoordelijke eigenaren: ☐ Per kroonjuweel is er een overzicht van de vastgestelde informatieklasse en geïmplementeerde beheersmaatregelen ☐ Een afgestemd audit- of reviewplan dat minimaal voorziet in een beoordeling door een onafhankelijke partij
2. Kijk verder dan de eigen organisatie	
Bevatten uitbestedingen en andere ketenafspraken alle eisen om Informatieveiligheid te borgen?	Aanbestedingen, inkopen en contracten met alle soorten ketenpartners met een ICT-component zijn voorzien van scherpe informatieveiligheidseisen ☐ In alle nieuwe aanbestedingen/inkopen en contracten met een ICT-component worden specifieke en toepasbare eisen gesteld ☐ Bestaande contracten zijn herijkt op deze toepasbare en specifieke eisen

	☐ Overzicht van contracten en aanbestedingen met herijking-status is beschikbaar en gerapporteerd aan de verantwoordelijke eigenaren

3. Zorg dat wat veilig is, ook veilig blijft

Nemen de risico's voor Informatieveiligheid door verouderde soft- en hardware af in de tijd?	Patchmanagement is op orde Verouderde informatiesystemen die de dienstverlening ondersteunen worden planmatig weggewerkt Websites en e-mail voldoen aan veilige internetstandaarden ☐ Veiligheidspatches worden aantoonbaar tijdig aangebracht. Tijdig is passend bij de ernst van de dreiging en kans van misbruik en overeenkomstig advies van de betrokken leverancier of cyberadviesorgaan ☐ Voor web en e-mail wordt voldaan aan de gangbare industriestandaards ☐ Er is een plan om verouderde hard/software risico-gebaseerd weg te werken ☐ Het vernieuwingsplan wordt volgens planning uitgevoerd

4. Veilig werken, ook thuis

Is de toegang voldoende afgeschermd? Worden incidenten adequaat afgehandeld? Neemt de meldingsbereidheid van gebruikers toe? Neemt de ernst van incidenten af?	Toegangsbeheer voldoet aan aangescherpte eisen. Incidenten worden afgehandeld volgens de vereisten uit het Vo Informatieclassificatieraamwerk (ICR). Meldingsbereidheid neemt aantoonbaar toe ☐ 2FA (2 factor authenticatie) wordt toegepast voor reguliere toegang ☐ Ook bijzondere toegang voor beheer/foutherstel en testen is ingericht volgens de eisen van het ICR ☐ Uit een periodiek overzicht van aantallen incidenten, gekwalificeerd naar ernst en periode, blijkt een afname van het aantal ernstige incidenten met x% per kwartaal, een toename van efficiëntie van de oplossing van incidenten met y% per kwartaal en bij een onverminderde meldingsbereidheid

5. Afscherming, detectie, monitoring en response

Zijn er voldoende maatregelen getroffen om te voorkomen dat uitval van een systeem niet leidt tot uitval van een ander systeem of zelfs van alle systemen? Worden dreigingen die mogelijk disruptief zijn voor de dienstverlening of bedrijfsvoering bijtijds gesignaleerd?	Segmentering van het ICT-landschap is zodanig ingericht dat de kans op (malware-)besmettingen van kroonjuwelen en toprisico segmenten sterk is gereduceerd ☐ De kroonjuwelen zijn aangesloten op een SOC/SIEM (securitycentrum en event monitoring) oplossing voor 24/7 monitoring en opvolging ☐ Er is aansluiting bij een CERT (computer emergency response) en CERT-adviezen rondom dreigingen en kwetsbaarheden worden binnen de gestelde termijnen uitgevoerd ☐ Er is een actueel overzicht van de doorgevoerde segmentering binnen het ICT-landschap en een audit op de robuustheid daarvan ☐ Er is een plan voor het oplossen van de tekortkomingen in de segmentering van het ICT-landschap en dit plan wordt uitgevoerd volgens planning

6. Effectief handelen bij incidenten en crisis

Is de crisisorganisatie voldoende geëquipeerd om in te grijpen bij crises door hacks en datadiefstal? Is recovery ten allen tijde mogelijk?	Back-up en recovery is voldoende geborgd. Crisisplan is compleet en actueel en wordt periodiek getest ☐ Er is een actueel back-up- en recoveryplan, geaccordeerd door het verantwoordelijk management ☐ Er is een actueel businesscontinuïteit managementplan, geaccordeerd door het topmanagement ☐ Beide plannen worden minimaal één keer per jaar geoefend, actualisaties en leerpunten worden direct verwerkt in de plannen

7. Meet, leer en stuur bij

Zijn de processen en maatregelen voor de bescherming tegen dreigingen op orde? Groeien deze processen en maatregelen mee met de toenemende kwetsbaarheden?	De maturiteit van Informatieveiligheid is op het minimaal vereiste niveau en neemt toe, in overeenstemming met gemaakte afspraken ☐ Maturiteit van Informatieveiligheid is minstens niveau 3 (ICR-maturiteitsmodel) en groei ervan is volgens afspraken ☐ Als het gewenste maturiteitsniveau nog niet is bereikt, dan is er een plan met mijlpalen die regelmatig wordt geëvalueerd

8. Verhoog het bewustzijn van medewerkers in een veilige cultuur

Zijn medewerkers voldoende op de hoogte van cyberdreigingen en het gewenste gedrag?	Feitelijk gedrag wordt regelmatig getest en uitkomsten daarvan zijn volgens afspraken ☐ Gedragstoetsingen als phishing en red-teaming vinden regelmatig plaats. Leerpunten worden gebruikt voor het dichten van gaten in de veiligheid van processen en systemen en de terugkoppeling van confronterende boodschappen en dit ter bevordering van bewustzijn en verantwoord gedrag ☐ Elke ondernomen gedragstoetsing wordt gepresenteerd aan het management met daarin de belangrijkste leerpunten ☐ Toereikend aanbod van leermiddelen voor alle werknemers

9. Definieer rollen en verantwoordelijkheden

Is er een cultuur van eigenaarschap in de organisatie? Zijn de belangrijkste rollen voor Informatieveiligheid gedefinieerd en toegekend?	Rollen, verantwoordelijkheden en bevoegdheden worden regelmatig beoordeeld en aangepast indien nodig ☐ Beschrijving van rollen is actueel en geborgd in processen en het HR-functiehuis ☐ Alle assets (processen, producten, diensten) hebben een verantwoordelijke eigenaar en deze zijn centraal geregistreerd ☐ De CISO heeft voldoende bevoegdheden om zijn/haar werk uit te voeren

10. Zorg voor voldoende middelen en capaciteit

Is er voldoende budget en menskracht voorzien voor het realiseren van informatieveiligheidsplannen?	Middelen en budget worden regelmatig beoordeeld. Bij tekorten worden prioriteiten en budget herzien en gerelateerde risico's (het niet realiseren van veiligheidsdoelstellingen) formeel geaccepteerd door de directie ☐ Er wordt voldoende budget gealloceerd voor Informatieveiligheid in de jaarlijkse budget-cyclus ☐ Er wordt voldoende menskracht met de juiste competenties en ervaring ingezet

5 BIJLAGE B: VOORBEELD OPDRACHTBRIEF

Dit is een voorbeeldbrief die dienst kan doen als opdrachtbevestiging tussen de leidend ambtenaar en de CISO of informatieveiligheidsconsulent. In dit document staat een beknopte omschrijving van de gemaakte afspraken en de bevoegdheid van de CISO om namens de leidend ambtenaar, een leidende rol te nemen in het overzicht en de status van de verbeterdoelstellingen en kritische performantie indicatoren.

Beste << naam CISO >>,

Op << datum-gesprek >> hebben we samen afgesproken om de sturing van Informatieveiligheid voor onze organisatie te verbeteren. In dat gesprek hebben we de KPI-vragen op basis van de 10 handvatten samen doorgenomen. Naderhand heeft u het besprokene omgezet naar een statusoverzicht. Deze vindt u als bijlage bij deze brief.

Ik geef u de opdracht om dit statusoverzicht om te zetten naar een dashboard dat organisatie-breed wordt bijgehouden. Dit dashboard wordt voortaan elk kwartaal met de deelnemende afdelingen en managementteams doorgenomen. Ikzelf doe dat in samenspraak met u elk kwartaal met het directieteam. In deze kwartaalgesprekken is feedback op de noodzakelijke betere sturing een vast agendapunt.

In onderstaande lijst heb ik de namen opgenomen van een aantal collega's. Ik geef hun opdracht om het komende jaar voldoende tijd vrij te maken voor het realiseren en bijhouden van dit KPI-dashboard voor de afdelingen << X, Y en Z >> inclusief een samengevoegd dashboard voor de hele organisatie als geheel.

Naam en functie:

…….

…….

…….

In de loop van de komende maanden kunnen extra namen aan deze lijst worden toegevoegd, zo nodig na afstemming met ondergetekende. Ik wens u succes en zal zorgen dat ik zelf ook beschikbaar ben mocht dat nodig zijn voor nadere tussentijdse afstemming.

Met vriendelijke groet,

<< Naam van de leidend ambtenaar >>

Bijlage: Concept statusoverzicht van de KPI's