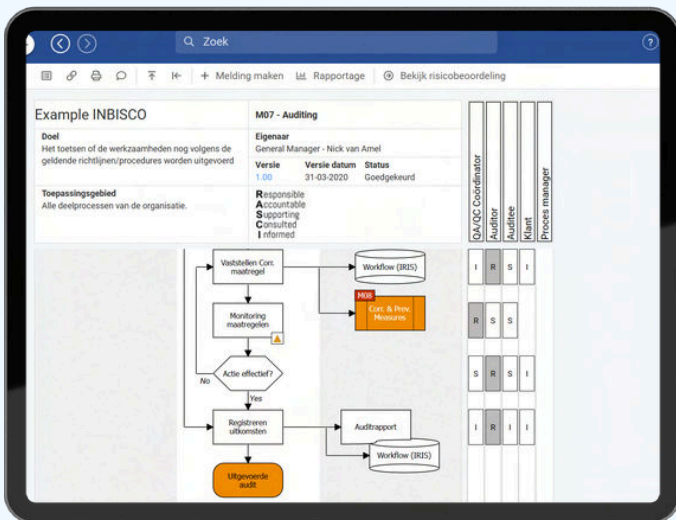


**Hoe groot is de kans op een datalek? Of een cyberattack? Wat zijn de consequenties als dit ons overkomt? Het informatiebeveiligingsbeleid dat we hebben opgesteld, wordt dit nageleefd? Kent iedereen in de organisatie het beleid? Deze vragen omtrent informatieveiligheid van de organisatie zijn voor velen te herkennen. Met INBISCO – Secure kan je op eenvoudige en overzichtelijke wijze de antwoorden verkrijgen.**



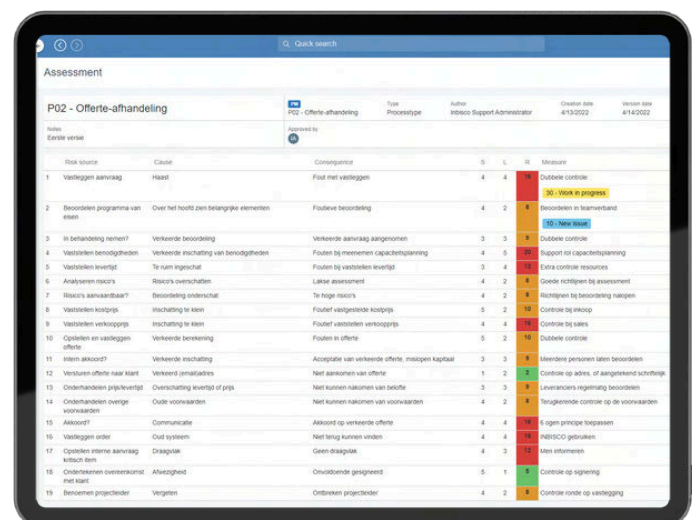
Proces incl. RASCI

### Werkwijze inzichtelijk

Het informatiebeveiligingsbeleid kan overzichtelijk opgeslagen worden in het systeem. De processen en instructies worden uitgewerkt en ondersteund door relevantie (beleids-)documenten. Binnen de processen wordt gebruik gemaakt van de RASCI methode, waardoor bij elke stap duidelijk is aangegeven welke personen betrokken zijn bij het proces en welke rol zij spelen. Iedere medewerker kan binnen enkele seconden bij de gewenste informatie. Nieuwe versies kunnen gemakkelijk aangemaakt worden, waardoor de informatie in het systeem eenvoudig up-to-date te houden is. Gebruikers kunnen aangesteld worden om een proces of document te beoordelen, zodat de kwaliteit van de informatie beveiligd blijft. Iedereen in de organisatie kan altijd bij de laatste versie van het beleid en de processen.

### Risico's in kaart

De uitgang van het informatiebeveiligingsbeleid zijn de risico's. Hoe groot is de kans op een cyberattack of een datalek? En als de organisatie wordt getroffen, wat zijn de consequenties? Wat kunnen we doen om de risico's te verminderen? Dit zijn vragen welke op overzichtelijke wijze te beantwoorden zijn in de risicobeoordeling. Door het aanmaken van eigen type risicobeoordelingen, risicovelden en het gebruik van een eigen risico matrix, is de beoordeling compleet in te richten naar wens van de organisatie. Om de kwaliteit en objectiviteit van de risicobeoordeling te beschermen kunnen er meerdere gebruikers aangesteld worden voor beoordeling.



Risk source	Class	Consequence	S	L	H	Measure
1. Verleggen aanpak	Maat	Fout met vastleggen	4	4	8	Dubbele controle 30: Work in progress
2. Beoordelen programma van eisen	Over het hoofd zien belangrijke elementen	Floute beoordeling	4	3	8	Beoordelen in teamverband 30: New issue
3. In behandeling nemen?	Verkeerde beoordeling	Verkeerde aanpak aangenomen	3	3	9	Dubbele controle
4. Vaststellen behoefte	Verkeerde inschatting van behoeftigheden	Fouten bij meenemen capaciteitsplanning	4	5	20	Support en capaciteitsplanning
5. Vaststellen eventjes	Te ruim ingeschat	Fouten bij vaststellen eventjes	3	4	12	Extra controle resources
6. Analiseren risico's	Risico's overschatten	Lake assessment	4	2	8	Goede richtlijnen bij assessment
7. Risico's aanvaardbaar?	Beoordeling onderschat	Te hoge risico's	4	2	8	Richtlijnen bij beoordeling nalegen
8. Vaststellen scope	Inschatting te klein	Fouten vastgestelde scope	5	2	10	Controler bij scope
9. Vaststellen verloop	Inschatting te klein	Fouten vaststellen verloop	4	4	16	Controler bij scope
10. Opstellen en vastleggen offerte	Verkeerde berekening	Fouten in offerte	5	3	15	Dubbele controle
11. Innen akkoord?	Verkeerde inschatting	Acceptatie van verkeerde offerte, missen kapitaal	3	3	9	Mede personeel laten beoordelen
12. Verkeuren offerte naar start	Verkeerd prioriteren	Niet aanpakken van offerte	1	2	2	Controler op datum of aangeleverde offerte
13. Onderhandelen prijs/levensijd	Overbieding eventjes of prijs	Niet kunnen nakomen van offerte	3	3	9	Leveranciers regelmatig beoordelen
14. Onderhandelen overige voorwaarden	Oude voorwaarden	Niet kunnen nakomen van voorwaarden	4	2	8	Regelmatige controle op de voorwaarden
15. Akkoord?	Communicatie	Akkoord op verkeerde offerte	4	4	16	Eigen principe toepassen
16. Vastleggen order	Oud systeem	Niet terug kunnen vinden	4	4	16	INBISCO gebruiken
17. Opstellen interne aanpak	Dringende	Geen draagvlak	4	3	12	Mees informeren
18. Onderscheiden overeenkomst met klant	Afwezigheid	Overstroomde gesigneerd	5	1	5	Controler op signering
19. Beoordelen projectleider	Vergeten	Ontbreken projectleider	4	2	8	Controler code op vastlegging

Risicobeoordeling

Gebruikers kunnen binnen het systeem communiceren over de beoordeling en samen de risico's beoordelen en maatregelen bespreken.

De mogelijkheid van deze eigen invulling stelt de organisatie in staat het systeem voor verschillende doeleinden te gebruiken, bijvoorbeeld om compliance te tonen aan de ISO 27001, NEN 7510 of de NIS2-richtlijn.

Op basis van de risico matrix kan de initiële inschatting van de ernst van het risico gemaakt worden. De risico reducerende maatregel wordt vervolgens weergegeven. De maatregel wordt uitgezet in de vorm van een melding. De melding doorloopt een statusflow, welke toont in hoeverre de maatregel is uitgevoerd. De status is vervolgens terug te zien in de risico-beoordeling bij de betreffende maatregel. In de beoordeling is dus duidelijk te zien in hoeverre de risico reducerende maatregel is geïmplementeerd.

Na implementatie van de maatregel kan de risicoscore naar een verlaagd restrisico veranderd worden. Als blijkt dat een bepaalde stap in een proces toch een verhoogd risico houdt, wordt dit aangegeven in het betreffende proces met een gevarendriehoek. Zo is voor iedereen binnen het proces gelijk duidelijk bij welke stappen de verhoogde risico's liggen.

R	Maatregel	E	K	R
8	Aanstellen Vertrouwenspersoon en opnemen in het personeelsbeleid	5	1	5
	20 - Toegewezen		∞	
8	Aanstellen Vertrouwenspersoon en opnemen in het personeelsbeleid	4	1	4
8	Aanstellen Vertrouwenspersoon en opnemen in het personeelsbeleid	4	1	4
4		4	1	4

Melding in de beoordeling

Impact	Kans				
	1 - Onrealistisch 1 x in de 10 jaar / >10% procent	2 - Onwaarschijnlijk 1x in de 5 jaar / >10% zekerheid	3 - Realistisch 1x per jaar / >30% zekerheid	4 - Waarschijnlijk 1x per half jaar / >60% zekerheid	5 - Bijna zeker 1x per maand / >80% zekerheid
5 - Catastrofaal Disastreuze impact op bedrijfsvoering, kan fallesement betekenen	5	10	15	20	25
4 - Hoge impact Flinke impact op bedrijfsvoering en zeer kostbaar	4	8	12	16	20
3 - Gemiddelde impact Gemiddelde impact op bedrijfsvoering en brengt kosten met zich mee	3	6	9	12	15
2 - Kleine impact Impact te overzien, minimale kosten	2	4	6	8	10
1 - Insignifcant Minimale impact en verwaarloosbare kosten	1	2	3	4	5

Risicomatrix

### Overzicht risico reducerende maatregelen

De risico reducerende maatregelen, maar ook bijvoorbeeld afwijkingen, incidenten, (interne) audits, etc., worden geregistreerd in een melding. Binnen de melding worden de taken aangemaakt en aan specifieke medewerkers toegewezen. Op deze manier is het duidelijk wie verantwoordelijk is voor de uitvoering van de taak.

De app geeft de mogelijkheid voor medewerkers om incidenten vanaf elke werkplek te melden. Medewerkers kunnen gemakkelijk binnen de melding communiceren en belangrijke bestanden en foto's uploaden. De informatie omtrent de melding is dus altijd op één plek te vinden.

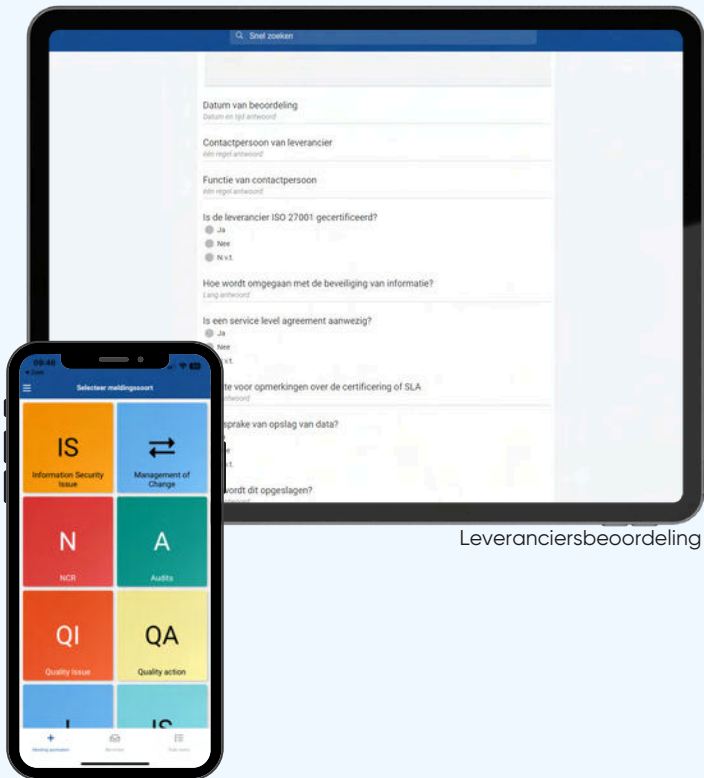
Status	Onderwerp	Afzender	Datum
In behandeling	Doorzak vaststellen	Esmee Blokland	02-02-2024 00:00 tot 05-02-2024 00:00
Gelopen	Vastleggen kwetsbaarheid in het systeem	Esmee Blokland	02-02-2024 00:00 tot 03-02-2024

Openstaande melding

## Eigen formulieren voor beoordelingen

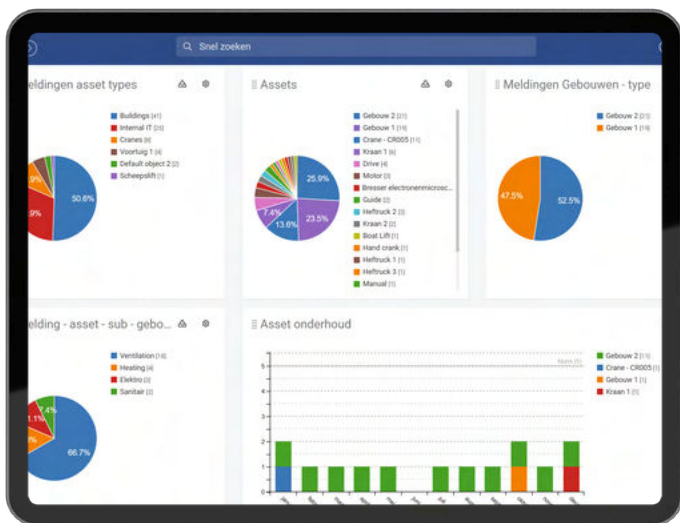
Risico's voor de informatieveiligheid kunnen intern, maar ook extern ontstaan. Grip op de risico's krijgen kan door het uitvoeren van interne audits en leveranciersbeoordelingen. Dit is tevens een belangrijk onderdeel van de normering voor de ISO 27001. In het systeem kan je eenvoudig eigen formulieren opstellen welke te gebruiken zijn als bijvoorbeeld een leveranciersbeoordeling of intern auditformulier. Eventuele bevindingen zijn tijdens het invullen van het formulier direct te koppelen. Alle uitkomsten worden gekoppeld aan de melding en kunnen worden omgezet in een rapportage. Alle uitkomsten zijn dus in één overzicht terug te vinden.

De formulieren zijn ook te benaderen via de app, bijvoorbeeld bij een audit op locatie of een IT-asset steekproef. De uitvoering, uitkomsten en mogelijke maatregelen of verbeteracties zijn zo allen te monitoren in het systeem.



Leveranciersbeoordeling

Melding in de app



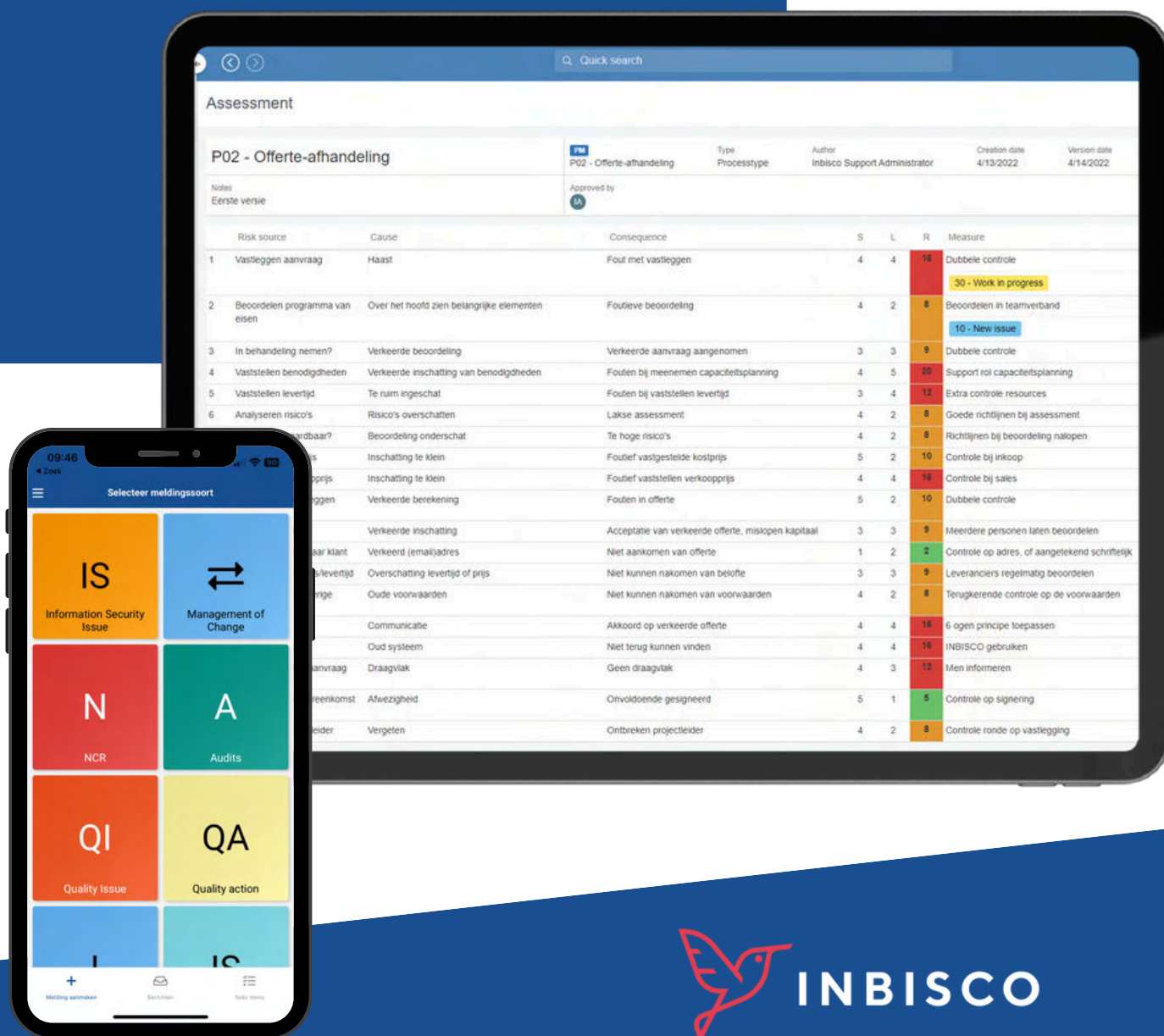
Rapportage

## Inzicht in één oogopslag

De meldingen kunnen omgezet worden in rapportages. De rapportages geven inzicht in bijvoorbeeld de openstaande meldingen, de status van risico reducerende maatregelen of de hoeveelheid incidenten. Naast een aantal standaard rapportagegrafieken zijn de grafieken zelf vorm te geven. Zo kan alle gewenste informatie uit het systeem overzichtelijk samen weergegeven worden. Het inzicht in de stand van zaken van de informatieveiligheid en het achterhalen van oorzaken van incidenten, stelt de organisatie in staat om hun informatieveiligheid continu te verbeteren.

Met INBISCO – Secure creëer je op eenvoudige wijze overzicht in de informatieveiligheid van de organisatie. Het informatiebeveiligingsbeleid en alle bijhorende processen, instructies en documenten zijn voor iedereen te vinden in één systeem. De processen tonen wie welke rol speelt bij elke stap. Door het maken van de risicobeoordeling kan er inzicht gecreëerd worden in de risico's en kunnen de risico reducerende maatregelen uitgezet worden. De maatregel, maar ook afwijkingen, incidenten en (interne) audits worden middels een melding vastgelegd en bijhorende taken zijn binnen één dossier vastgelegd. Het creëren van eigen formulieren biedt de mogelijkheid om verschillende controles, steekproeven, audits, leveranciersbeoordelingen, maar ook notulen of managementreviews vast te leggen. Deze kunnen vervolgens eenvoudig omgezet worden in handige rapportages.

Alles omtrent informatieveiligheid wordt opgeslagen, gemonitord en geanalyseerd in één systeem. Krijg grip op de status van informatieveiligheid met INBISCO – Secure.



INBISCO