INBISCO

Whitepaper Information Security

INBISCO B.V.
Baanhoek 144A
3361 GM Sliedrecht
085 - 00 43 847
INBISCO.NL

Inleiding

INBISCO streeft ernaar om de vertrouwelijkheid, integriteit en de beschikbaarheid van informatie middels een risicobeheerproces te beschermen, zodat belanghebbende het vertrouwen mogen hebben dat risico's adequaat worden beheerd. Om dit te verwezenlijken is veiligheid van informatie een belangrijk onderdeel binnen INBISCO.

Middels deze whitepaper willen wij meer inzicht geven in wat wij als organisatie doen voor het creëren van veiligheid van informatie.

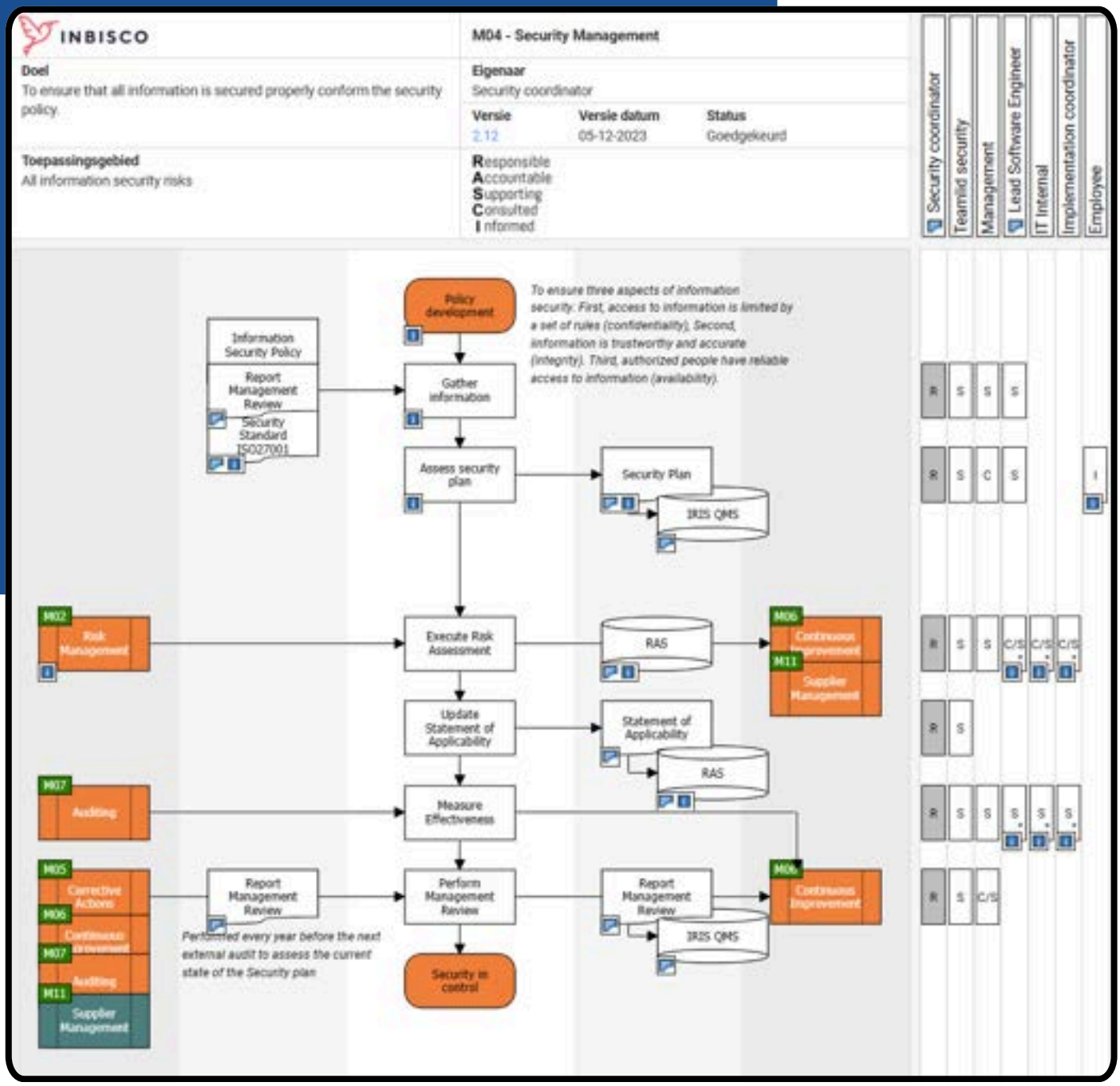
Index

Information Security

Information Security begint met het hebben van een security management proces en een information security beleid.

1.1 Security Management proces

Dit proces is opgesteld om ervoor te zorgen dat alle informatie correct is beveiligd, conform het beveiligingsbeleid.



1.2 Information Security Policy

Zoals eerder genoemd streeft INBISCO ernaar om de vertrouwelijkheid, integriteit en de beschikbaarheid van informatie middels een risicobeheerproces te beschermen.

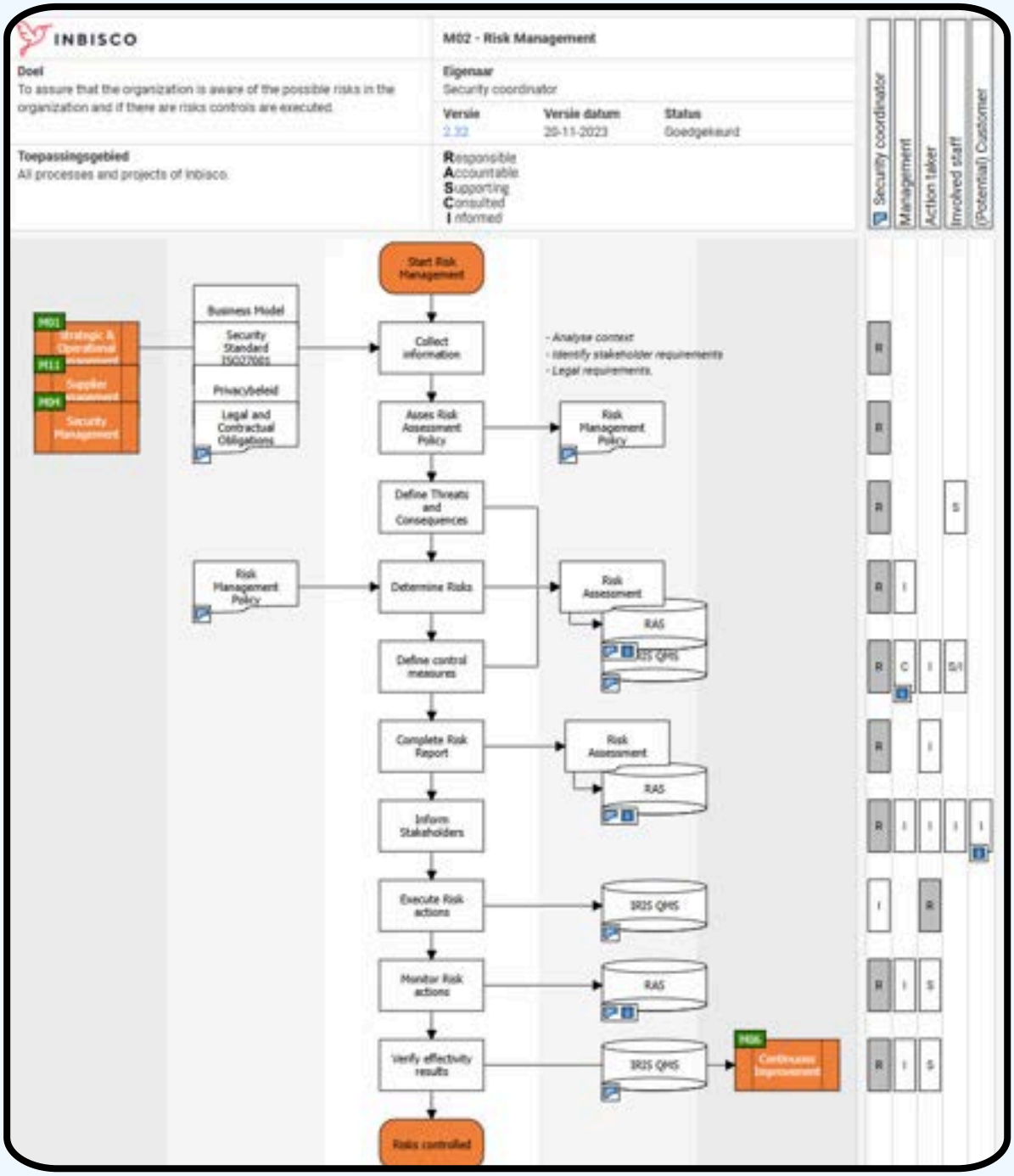
De organisatie wordt beïnvloed door interne en externe factoren. Middels de risicobeoordeling worden de risico's die deze factoren vormen, geïdentificeerd en geëvalueerd. Dit betreft de volgende factoren.

Intern		**Extern**	
Partijen			
Leveranciers en partners	INBISCO eist van leveranciers en partners die relevant zijn voor de omgang met gevoelige informatie dat zij en hun producten/diensten voldoen aan haar informatiebeveiligingseisen .	**Klanten**	Klanten verwachten dat de beschikbaarheid, vertrouwelijkheid en integriteit van hun bedrijfsgegevens worden gewaarborgd op basis van het overeengekomen beschermingsniveau.
		Overheid	Overheidsinstanties eisen dat de organisatie voldoet aan wet- en regelgeving.
		Speciale belangen groepen	Speciale belangengroepen verwachten dat INBISCO zich laat informeren over en handelen naar specifieke risico's die door hun inzichtelijk worden gemaakt.
Mensen			
Medewerkers	Medewerkers verwachten dat zij worden ondersteund met tijd, kennis en middelen om hun informatiebeveiliging te kunnen garanderen. Tevens verwachten zij dat INBISCO vertrouwelijk omgaat met gedeelde persoonsgegevens. INBISCO verwacht van medewerkers dat zij integer met vertrouwelijke informatie omgaan.	**Gebruikers**	Gebruikers willen dat de beschikbaarheid, vertrouwelijkheid en integriteit van hun (persoons)gegevens worden gewaarborgd.
Bezoekers	INBISCO draagt er zorg voor dat bezoekers geen toegang hebben tot vertrouwelijke informatie.		
Middelen			
Kantoor	INBISCO draagt er zorg voor dat het kantoorgebouw en de kantoorruimtes enkel toegankelijk zijn voor geautoriseerde en gewenste personen.		
Software	INBISCO draagt er zorg voor dat software wat gebruikt wordt voor het opslaan of verwerken van informatie beschermd zijn tegen informatiebeveiligingsincidenten.		
Hardware	INBISCO draagt er zorg voor dat de hardware wat gebruikt wordt voor het opslaan of verwerken van informatie beschermd is tegen informatiebeveiligingsincidenten.		
Organisatie			
Processen	INBISCO verwacht dat ze inzichtelijk heeft welke actoren verantwoordelijk zijn voor omgang met en overdracht van vertrouwelijke informatie per proces(stap).		

Beheersing en inzicht in risico's

Steeds vaker verschijnen berichten over bedrijven or organisaties die gehackt zijn of een datalek veroorzaken. Bedrijven worden gegijzeld en dienen losgeld te betalen voor vrijgave van de database. Wellicht denkt u dat het uw organisatie niet zal gebeuren. Hierdoor ontstaat een blinde vlek als het gaat om het beveiligen van informatie. Men realiseert zich niet wat de gevaren en consequenties zijn.

Het is daarom van belang om inzicht te hebben in de risico's die wij als organisatie lopen en de consequenties daarvan. Deze risico's brengen wij in kaart aan de hand van ons Risk Management proces.



Risico's die in kaart worden gebracht leggen we vast in onze RAS-module. Middels de risicobeoordeling worden vragen beantwoord zoals:

- Zijn er gevaren of bestaat er dreiging?
- Wat zijn de consequenties als deze er zijn?
- Wat voor impact hebben deze consequenties op onze organisatie?

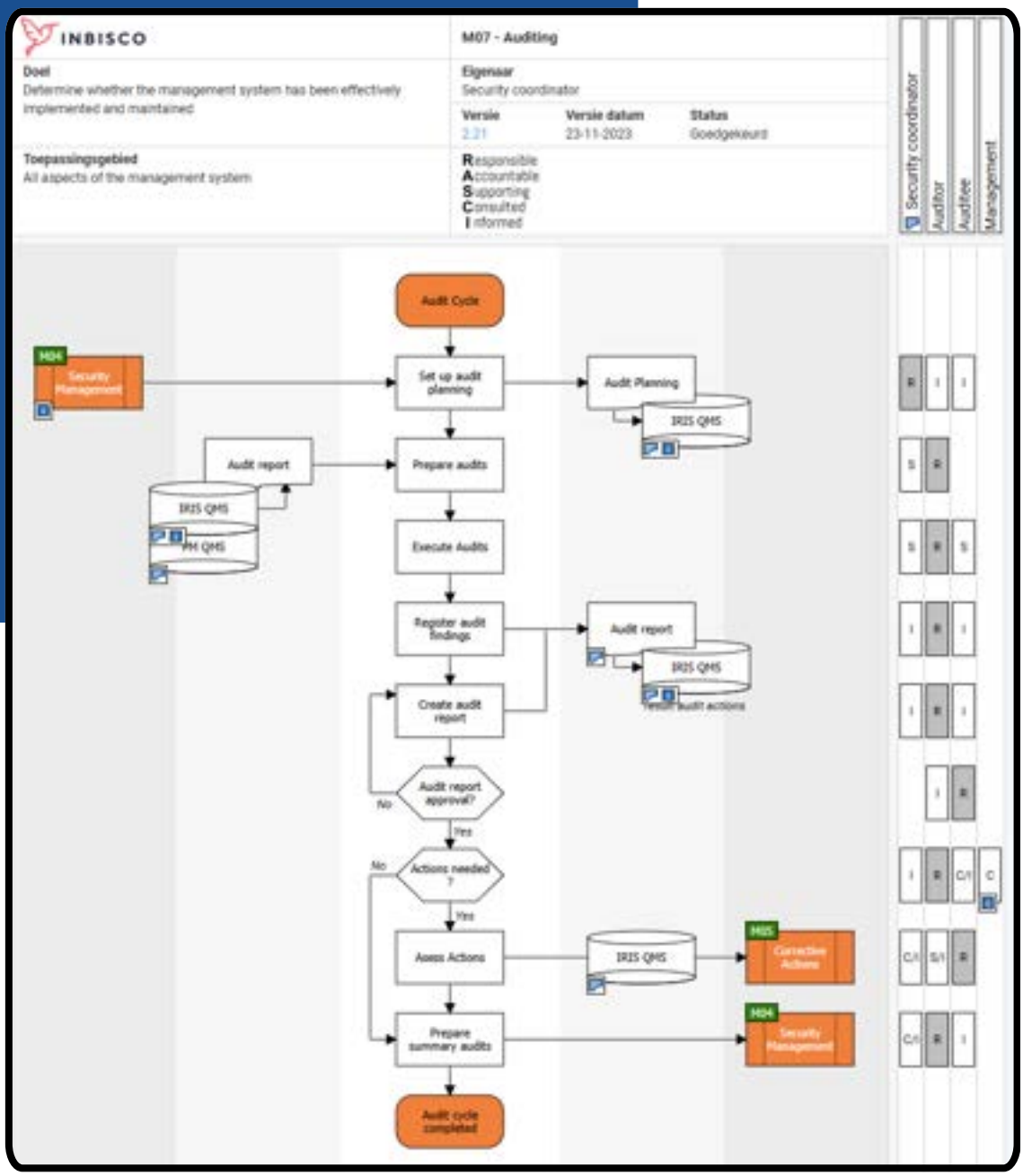
Om in te spelen op de risico's die je als organisatie loopt wordt gekeken naar eventuele beheersmaatregelen die kunnen worden getroffen. De opvolging van de diverse Information Security risico's, dossiers en de daarbij behorende acties leggen we vast en monitoren we in IRIS. Hierbij kunnen we zien welke dossiers open staan, welke status de acties hebben en of de afhandeling volgens afspraak gaat.

Monitoring en analyse

Naast informatie vanuit de risicobeoordeling wordt data verzameld via andere kanalen. Als organisatie voeren we interne processen audits uit, vragen we feedback van medewerkers en worden eventuele afwijkingen en incidenten geregistreerd.

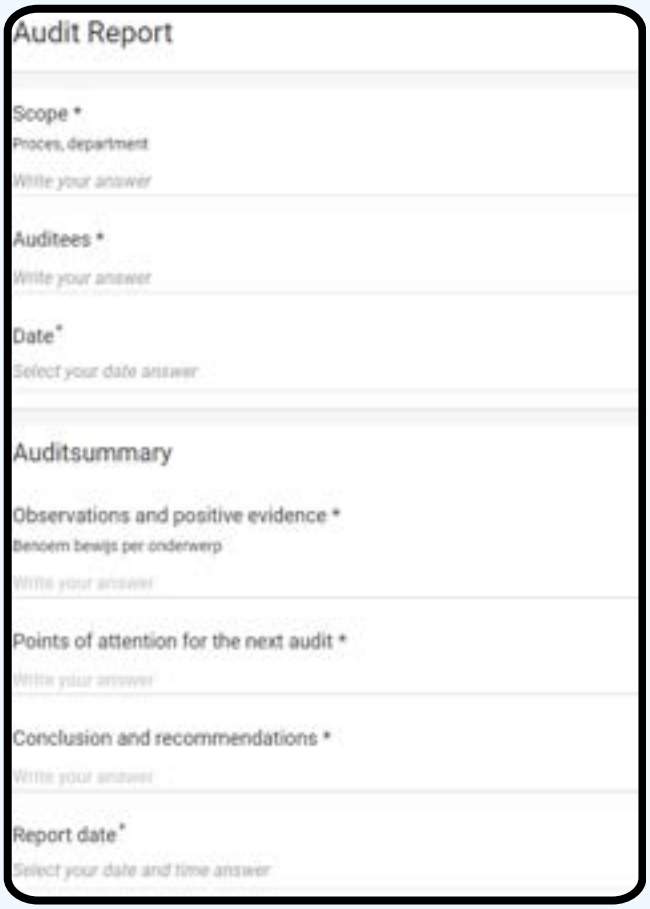
3.1 Interne audits

Jaarlijks worden interne proces audits uitgevoerd. Sterker nog, we hebben in ons security jaarplan opgenomen dat jaarlijks alle processen worden ge-audit. De audits worden uitgevoerd middels het proces Auditing.



INBISCO voert audits uit om vast te stellen of het managementsysteem effectief is geïmplementeerd en onderhouden. Om dit vast te stellen worden uitkomsten van audits vastgelegd in een auditformulier welke terug te vinden is in het IRIS-dossier.

Nodige maatregelen en acties die volgen uit audits, worden uitgezet en gekoppeld aan het IRIS-dossier. Zo monitoren we wederom welke dossiers open staan, welke status de acties hebben en of de afhandeling volgens afspraak gaat.


Audit Report

Scope *
Proces, department
Write your answer

Auditees *
Write your answer

Date*
Select your date answer

Auditsummary

Observations and positive evidence *
Benoem bewijs per onderwerp
Write your answer

Points of attention for the next audit *
Write your answer

Conclusion and recommendations *
Write your answer

Report date*
Select your date and time answer

3.2 Awareness

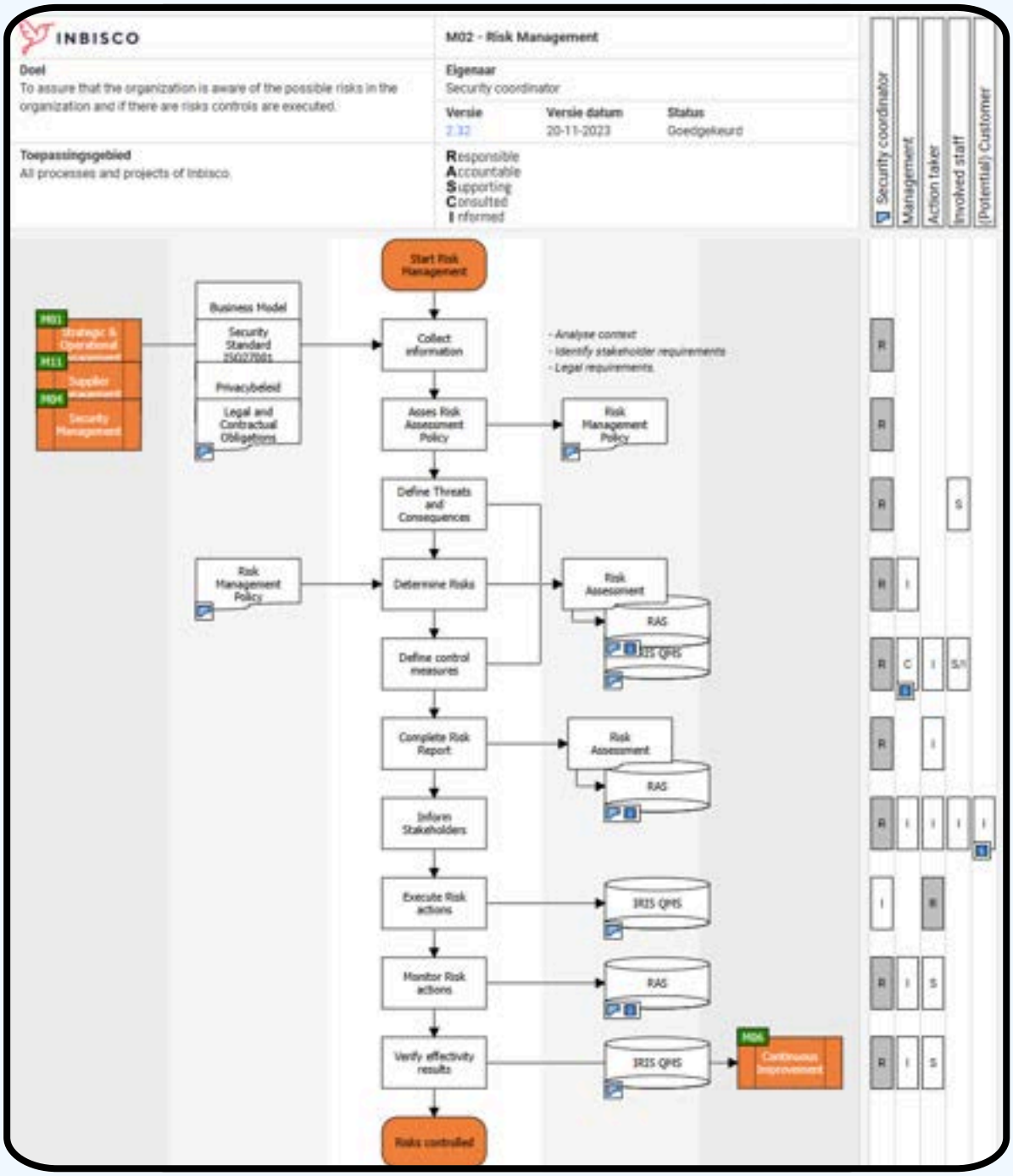
Om feedback vanuit medewerkers te krijgen en ervoor te zorgen dat iedereen binnen de organisatie de nodige data zoals incidenten en afwijkingen vastlegt, is het van belang dat zij inzien hoe belangrijk Information Security is.

Om dit te bereiken focust INBISCO zich op het bewustzijn van medewerkers door een awareness sessie. Onderdeel van het jaarplan is dan ook om minimaal vier awareness sessies per jaar uit te voeren.

3.3 Afwijkingen en incidenten

Naast audits en feedback van medewerkers, is het van belang dat wij als organisatie afwijkingen of incidenten die hebben plaatsgevonden vastleggen, opvolgen en nodige maatregelen treffen.

Uitvoering daarvan hebben we vastgelegd in het proces Corrective Actions waarbij we streven naar het structureel oplossen van afwijkingen.



De vastgelegde afwijkingen worden via rapportages en grafieken snel beoordeeld en geanalyseerd. Na de analyse hebben we inzicht in de verbetermogelijkheden van INBISCO en kunnen de maatregelen en/of verbeteracties in gang gezet worden. Dit is een terugkerend proces; de veiligheid van informatie wordt continu gemonitord en, indien mogelijk, verhoogd.

ISO 27001

ISO 27001 is een internationale standaard voor informatiebeveiliging. Binnen deze standaard staat beschreven hoe, wij als organisatie procesmatig om kunnen gaan met het beveiligen van informatie.

Om aan te kunnen tonen dat wij als organisatie veilig omgaan met informatie zijn wij ISO 27001:2022 gecertificeerd.

INBISCO

Bezoek- en postadres

Baanhoek 144A

3361 GM Sliedrecht

Telefoon en e-mail

085 - 00 43 847

info@inbisco.nl

Volg ons op: