Succesfactoren bij het implementeren van GRC

Whitepaper

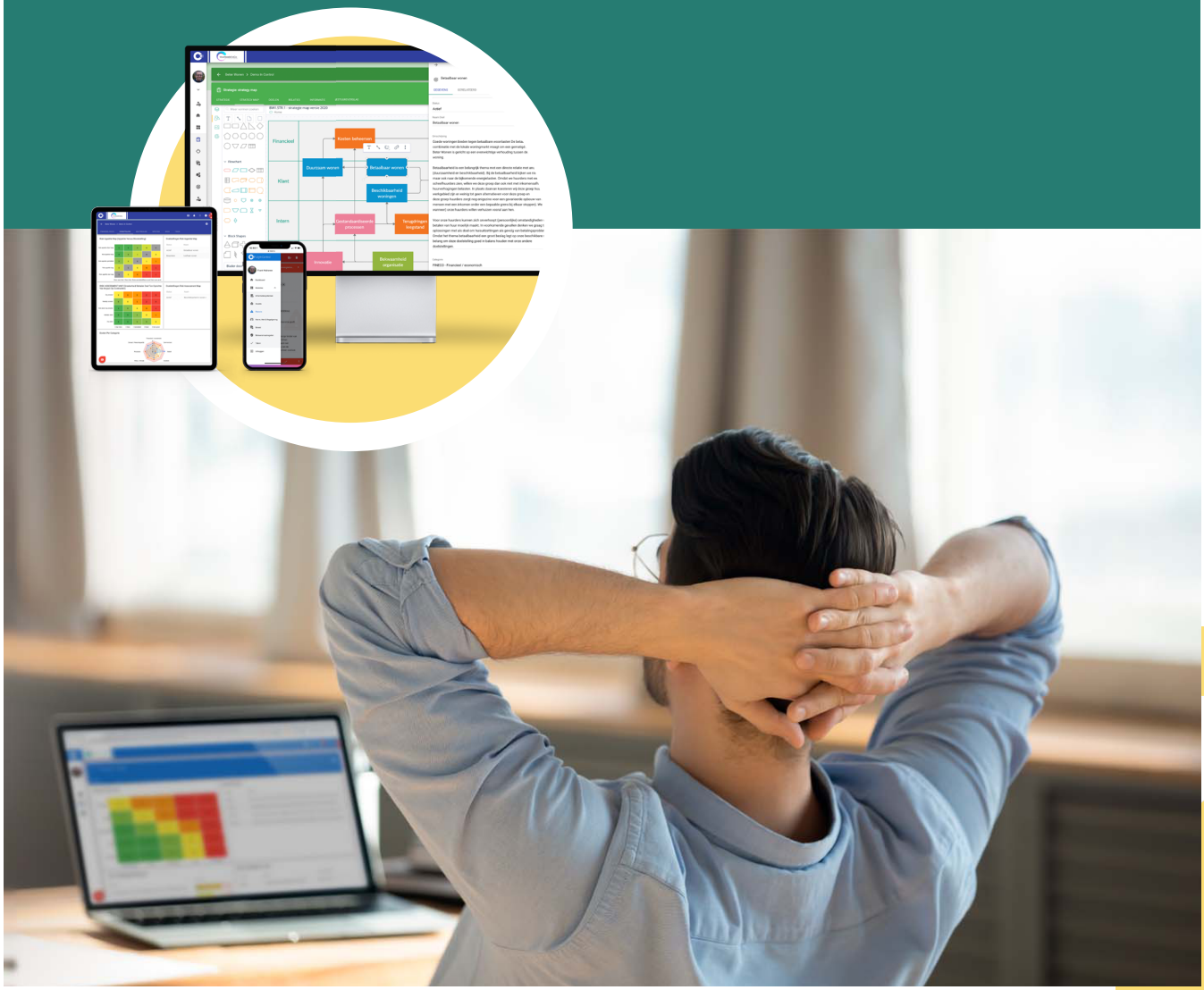
FullyInControl
Works your way

Inhoudsopgave

1. Inleiding

Professionele organisaties streven ernaar om hun Governance, Risk en Compliance Management (GRC) goed op orde te hebben. Dat is zelfs een voorwaarde om als organisatie op langere termijn succesvol te zijn en blijven. Er moet aardig wat opgepakt worden om GRC binnen je organisatie goed in te richten. Dit is geen eenmalige exercitie maar een continu proces, waarin je volgens de PDCA-cyclus (Plan-Do-Check-Act) continu leert en werkt aan het verbeteren en beheersen van de GRC-processen.

In dit whitepaper lees je hoe je in jouw organisatie GRC succesvol kunt implementeren of optimaliseren. Je leest ook alles over de toegevoegde waarde van geïntegreerde GRC-software en we loodsen je door de stappen die je kunt zetten om de beste GRC-software voor jouw organisatie te selecteren.



De 3 domeinen van GRC.

- Governance op orde
- Integraal Risicomanagement
- Altijd compliant

Governance op orde

Governance verwijst naar de manier hoe je organisatie is georganiseerd en wordt bestuurd. Voor governance breng je de aansturingsstructuur, het beleid, de processen en de regels van de organisatie in kaart en leg je ze gestructureerd vast. Dit geeft medewerkers kaders en richtlijnen bij het nemen van beslissingen en helpt ze om op de juiste manier bij te dragen aan het behalen van de organisatiedoelstellingen.

Iedere organisatie die professionaliteit nastreeft, hoort haar governance op orde te hebben. Met goede governance is de kans dat iedereen de juiste besluiten neemt aanzienlijk groter en wordt je organisatie uiteindelijk succesvoller. Voor goede governance gelden wel enkele voorwaarden.

Transparantie

Voor goede governance is transparantie en heldere communicatie over beleid, de processen en regels naar álle stakeholders essentieel. Deze dienen immers door de hele organisatie en overige stakeholders te worden gedragen en nageleefd, zodat iedereen op dezelfde lijn zit en organisatiedoelstellingen op gewenste wijze worden nagestreefd.

Verantwoordelijkheid

Natuurlijk moet er ook toezicht worden gehouden op het naleven van het organisatiebeleid, de processen en regels. Hierbij speelt een passende organisatie- en aansturingsstructuur een belangrijke rol. Zo zal een resultaatgerichte manier van besturen medewerkers stimuleren hun eigen verantwoordelijkheid te nemen.

Governance als continu proces:

- Bepalen en uitwerken van beleid, gebaseerd op de missie, visie en strategie.
- Uitwerken en implementeren van processen en maatregelen om het beleid uit te voeren.
- Toetsen van maatregelen op opzet, bestaan en werking.
- Periodiek reviewen - en zo nodig bijstellen - van het beleid en bijbehorende maatregelen en processen, aan de veranderende omgeving en inzichten.

(Her)schrijf beleid, processen en regels

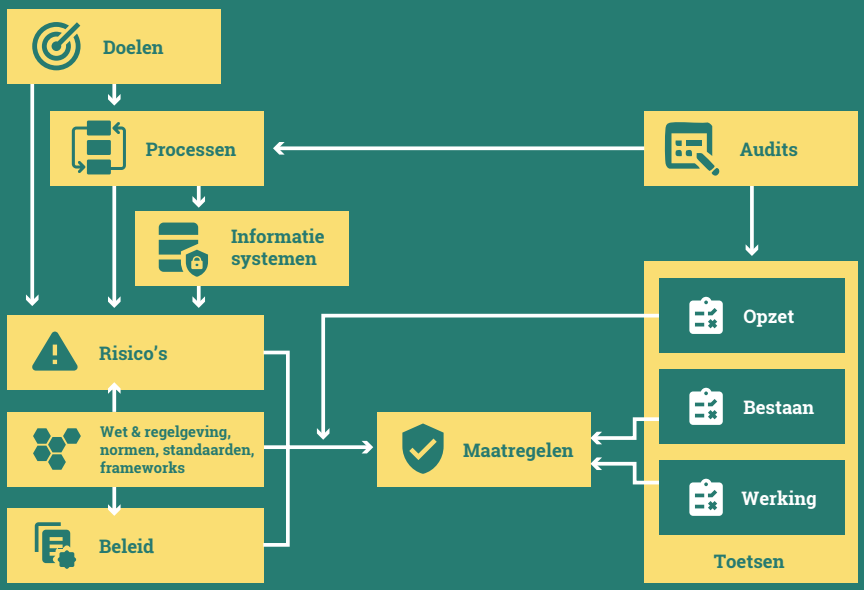
Aangezien de omgeving waarin een organisatie opereert continu verandert, zal ook de manier waarop de organisatie haar governance inricht, allesbehalve statisch zijn. Beleidsonderdelen, inclusief de processen, moeten daarom periodiek gereviewd worden.
Je beoordeelt daarbij of het beleid en de processen nog passend en uitvoerbaar zijn. Een GRC-oplossing kan jou ondersteunen bij dit review proces, bijvoorbeeld met:

- Het automatisch inplannen van review-acties.
- Het sturen van een herinnering aan verantwoordelijke managers om een beleidshoofdstuk te reviewen.
- Het ter beoordeling voorleggen van nieuwe, gewijzigde versies aan belanghebbenden.
- Het toesturen (en eventueel toelichten) van de definitieve versies aan stakeholders.

Implementeer je governance model

Het is niet alleen essentieel dat je beleid en processen helder beschreven zijn, je moet ook bedenken hoe je ze (zorgvuldig) implementeert. Daarnaast is het voor sommige, belangrijke regels essentieel dat je ze (periodiek) toetst op opzet, bestaan en werking. Hierover lees je meer in het hoofdstuk Risicomanagement.

De maatregelen die je neemt om het beleid te implementeren, zijn vaak maatregelen die je ook neemt om een risico te mitigeren (risicomanagement) of om aan wet- een regelgeving te voldoen (compliance management). In je beleid beschrijf je bijvoorbeeld dat je een integere organisatie wilt zijn. Met de maatregelen die je hiervoor treft, kun je ook je integriteitsrisico's aanpakken of voldoen aan bepaalde wet- en regelgeving met betrekking tot integriteit (zoals SIRA of Wwft). Met een goede GRC-oplossing hoef je maatregelen maar één keer te managen en te toetsen. Dezelfde maatregelen kunnen dus gekoppeld zijn aan beleidshoofdstukken, risico's en eisen uit normen en wet- en regelgeving. Met goede software kun je ook per risico, eis of beleidsthema, etc. aangeven in hoeverre een maatregel de onderdelen afdekt. Hierdoor heb je direct inzicht in de mate waarin je in control bent.



Samenhang GRC-componenten

Integraal Risicomanagement

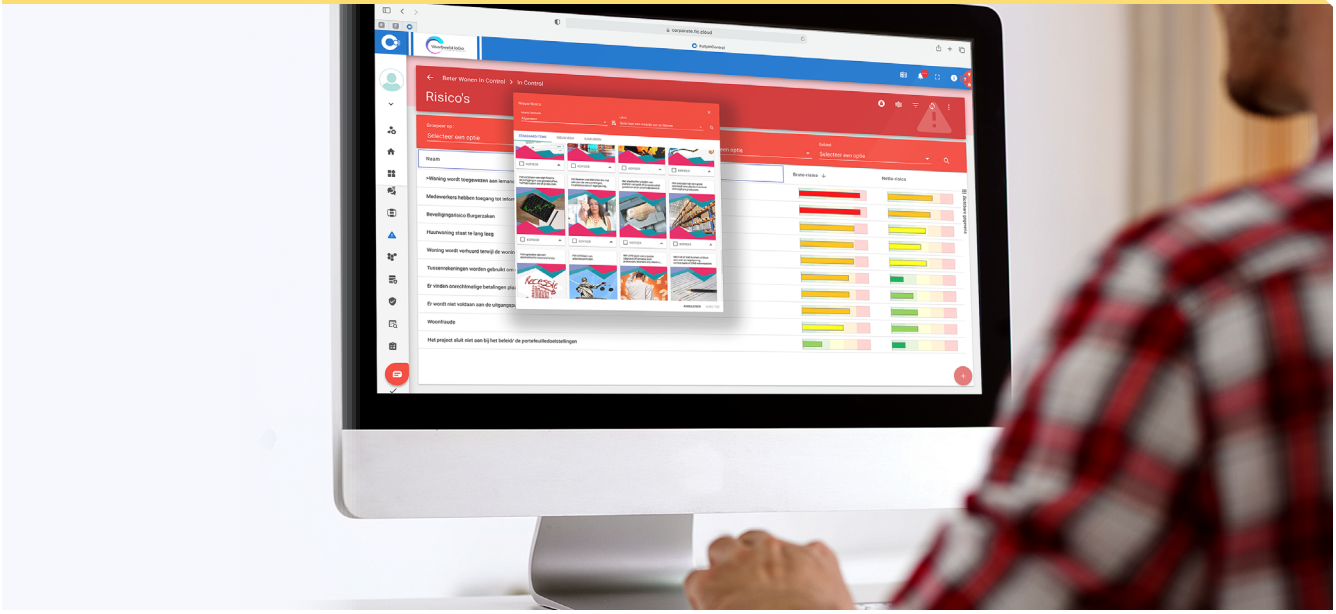
Met risicomanagement bereid je je voor op onzekere gebeurtenissen en bepaal je hoe je de kans op ongewenste gebeurtenissen kunt verkleinen en de schade kunt beperken mocht de ongewenste gebeurtenis toch optreden.

In iedere organisatie en bij elk programma, project of activiteit neem je risico's. Echter, organisaties hebben lang niet altijd (voldoende) inzicht in de risico's die ze lopen. Het nemen van risico's moet een bewuste afweging zijn. Daartoe doen organisaties er goed aan om bij iedere belangrijke doelstelling de bijbehorende risico's in kaart te brengen. Wil je een risico niet lopen, omdat het een doelstelling te veel in gevaar kan brengen, dan kun je maatregelen nemen om de kans op of de impact van het risico te verkleinen. Belangrijk is dat het altijd een bewuste keuze moet zijn om een (voorspelbaar) risico in een bepaalde mate te lopen.

Wel is het zo dat je niet altijd zélf de keuze hebt om een risico wel of niet te mitigeren. Er is ook veel wet- en regelgeving die organisaties dwingt om maatregelen te nemen tegen risico's die we als maatschappij niet acceptabel vinden. Ook normen en frameworks waar je als organisatie aan wilt of moet voldoen, kunnen je dwingen om bepaalde risico's aan te pakken. Hier zien we een belangrijke overlap met compliance binnen GRC.

Risicomanagement als continu proces:

- Identificeren van risico's en bepalen van de kans en impact van de risico's.
- Bepalen welke risico's je als organisatie accepteert en in welke mate je ze wilt mitigeren.
- Bepalen en implementeren van de maatregelen om risico's te mitigeren.
- Het (periodiek) toetsen van de maatregelen op opzet, bestaan en werking.



Risicomanagement is een continu proces dat onderdeel zou moeten zijn van de aansturing van iedere organisatie. Het zorgt voor:

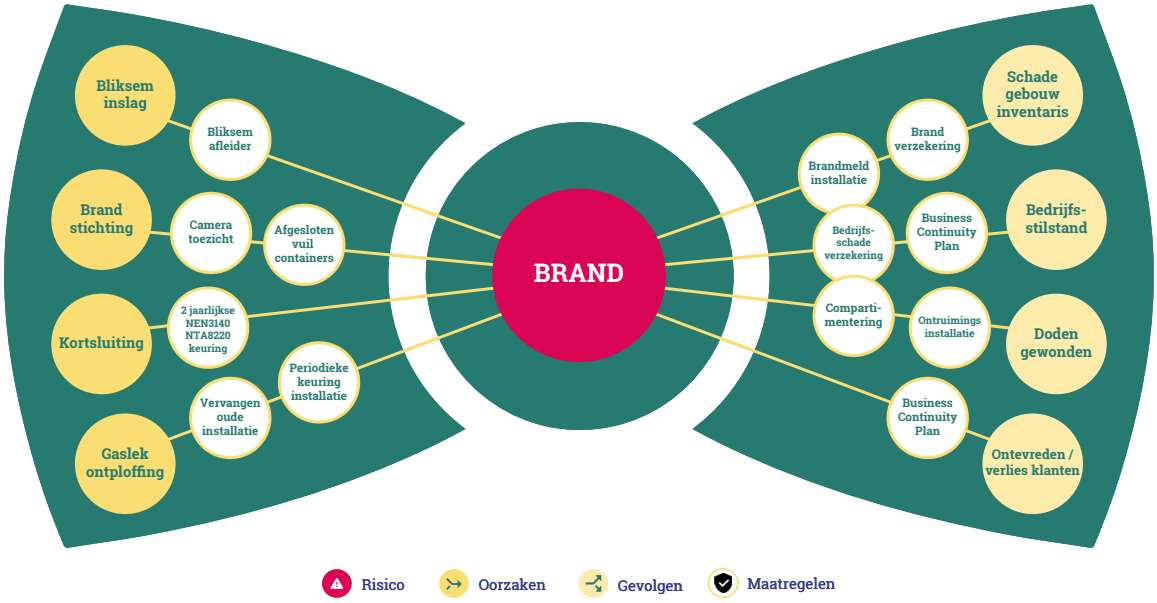
- **Minder faalkosten - goede kwaliteit van product en/of dienst**
  Voorkomt grote financiële tegenslagen.
- **Een veilige en gezonde werkomgeving**
  Leidt tot minder zieken en voorkomt ernstige ongelukken met doden en/of gewonden.
- **Behoud van een goede reputatie**
  Voorkomt negatieve publiciteit.
- **Een efficiënte en maatschappelijk verantwoorde bedrijfsvoering**
  Voorkomt aansprakelijkheidsclaims en boetes.
- **Een succesvolle operatie**
  Zorgt voor continuïteit, voorkomt verlies van marktaandeel, vergunningen en faillissement.

De 3 (zich herhalende) stappen van risicomanagement

1. **Risico-inventarisatie**
   Zorg ervoor dat risicomanagement onderdeel is van alle organisatiedoelen, -programma's, -projecten, -processen en belangrijke beslissingen. Hiermee bereik je dat iedereen risico gestuurd werkt. Inventariseer hiervoor al bij het opzetten van deze activiteiten de risico's. In een GRC-oplossing kun je bij programma's, projecten, doelen of processen eenvoudig al je risico's inventariseren via dialoogsessies. Een aantal mensen krijgt dan een uitnodiging om bij de verschillende onderdelen (via een digitaal inventarisatieformulier) risico's toe te voegen. Deze kunnen in een later stadium worden besproken als onderdeel van het doel waar ze onder komen te hangen. Vervolgens schat je (met meerdere mensen) de kans en impact van deze risico's in en ken je prioriteiten toe. Hierdoor wordt duidelijk welke risico's de grootste bedreiging vormen. Je hebt nu voldoende inzicht in de risico's om te kunnen bepalen welke risico's je wilt mitigeren en welke je als organisatie (gedeeltelijk) accepteert.

2. Bepaal je mitigatiestrategie en kies beheersmaatregelen

Wanneer alle risico's zijn geïnventariseerd en geprioriteerd, bepaal je welke beheersmaatregelen nodig zijn om de risico's te mitigeren. Deze beheersmaatregelen omvatten allerlei acties die ervoor zorgen dat de kans dat het risico optreedt, wordt verkleind of de schade wordt beperkt (mocht het risico niet geheel te mitigeren zijn). Om de juiste maatregelen te bepalen, is het bij belangrijke risico's aan te raden om eerst de oorzaken en gevolgen van het risico te inventariseren. Je bent dan beter in staat om de juiste maatregelen te kiezen. Dit wordt ook wel de bowtie methode genoemd. Het is belangrijk dat een GRC-oplossing goed met een bowtie kan omgaan.



3. Toets de maatregelen op opzet, bestaan en werking

Organisaties kunnen ervoor kiezen om de mitigerende maatregelen voor implementatie te laten toetsen door een onafhankelijke expert. Bij een positief oordeel ga je over tot implementatie. Na implementatie is het zaak dat je (periodiek) toetst of de maatregelen (nog) aanwezig en effectief zijn. Is dit niet het geval, dan wordt de maatregel automatisch op 'niet effectief' gezet en wordt een bevinding, issue en/of actie aangemaakt om de maatregel te corrigeren. Deze toetsen moeten automatisch herhaald kunnen worden waarbij de verantwoordelijke via een e-mail notificatie een herinnering ontvangt.

Altijd compliant

Het laatste - en zeker niet het minst belangrijke - onderdeel van GRC is Compliance. Met Compliance manage je het proces om (zoveel mogelijk) te voldoen aan wet- en regelgeving (extern en intern) en aan de eisen uit normen en frameworks die je organisatie zichzelf oplegt of die klanten of andere stakeholders aan je stellen.

Bij compliance moet je aantoonbaar (auditable) aan eisen voldoen. Sommige compliance onderdelen zijn risico gestuurd. Er wordt dan geëist dat je je risico's op het compliance thema in kaart brengt en maatregelen treft om deze te mitigeren (zie hoofdstuk over risicomanagement). Dit speelt bijvoorbeeld bij de wet- en regelgeving met betrekking tot integriteit (Wwft/SIRA) of veiligheid en gezondheid van medewerkers (Arbowetgeving).

Ook vanuit andere wet- en regelgeving, normen en frameworks kunnen duidelijke eisen worden gesteld waaraan je als organisatie moet voldoen. In veel gevallen mitigeer je daarmee ook risico's. Meestal wordt geëist dat je beleid hebt gedefinieerd, processen hebt uitgewerkt en geïmplementeerd en maatregelen hebt genomen. Voldoe je hier niet aan, dan riskeer je boetes of verlies je een (ISO) certificaat of zelfs vergunning.

Compliance als continu proces:

- Inventarisatie van de eisen waaraan je moet voldoen.
- Verklaar de eisen die niet van toepassing zijn voor je organisatie als 'niet van toepassing', inclusief de reden waarom.
- Inventariseer en implementeer het beleid, de maatregelen en processen waarmee je aan de eisen/controls uit de norm of regelgeving voldoet.
- Als een eis risico-gestuurd is: inventariseer de risico's die van toepassing zijn op het onderwerp en bepaal de benodigde maatregelen (zie risicomanagement).
- Toets maatregelen op opzet, bestaan en werking, review het beleid en voer zo nodig (als maatregelen niet effectief zijn) corrigerende acties uit.
- Inrichten en laten uitvoeren van interne en externe audits om aan te tonen dat je (op een onderdeel) compliant bent.

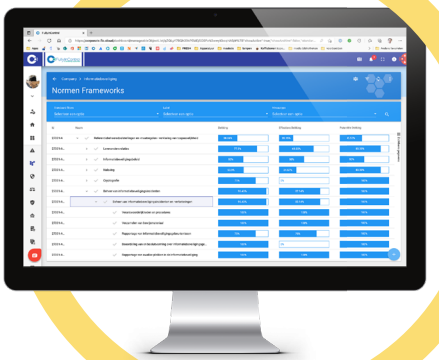
Aandachtspunten voor compliance management

Voor compliance management is een overzichtelijke omgeving vereist, die inzicht geeft in:

- De eisen waaraan je als organisatie moet voldoen;
- Wat je al gedaan hebt om te voldoen;
- De mate waarin je op een bepaald moment voldoet (mate van compliant zijn).

Het is dus belangrijk om inzicht te hebben in de eisen die gelden en de maatregelen die je moet treffen. Daarnaast is het noodzakelijk om acties die je uitzet om maatregelen te implementeren, goed te managen. Dit uiteraard in combinatie met Goverance en Risicomanagement. Het toetsen en uitvoeren van (interne) audits om de mate van compliance te bepalen, helpt bij het identificeren van hiaten. Het toont aan in welke mate normen, frameworks, wet- en regelgeving al dan niet afgedekt en/of nageleefd worden.

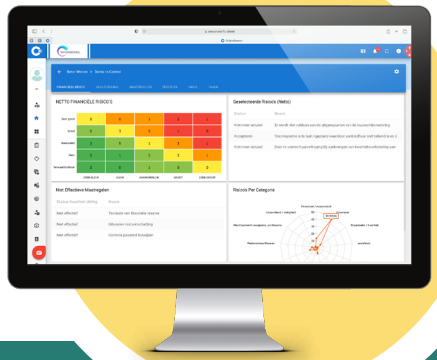
Omdat de omgeving waarin je opereert, net als de processen binnen je organisatie en de wet- en regelgeving continu veranderen, is het belangrijk om regelmatig de mate van compliance te toetsen en waar nodig tijdig bij te sturen. Dit proces kun je eenvoudig managen door het volledig te automatiseren met integrale GRC-software. Hierdoor creëer je een aantoonbare audit trail en ben je op ieder moment ‘audit ready’, zodat onder andere risico’s op incidenten, boetes en het verliezen van een certificaat of vergunning gemitigeerd worden en je altijd voorbereid bent op onvoorziene gebeurtenissen.



3. Toegevoegde waarde van geïntegreerde GRC-software

Het mag duidelijk zijn dat er aardig wat opgepakt moet worden om GRC succesvol te implementeren. Daarbij valt veel voordeel te halen uit een geïntegreerde GRC-software oplossing. Helaas zien we in de praktijk nogal eens dat organisaties voor ieder GRC-domein en de aanpalende domeinen een ander systeem en een brei aan spreadsheets gebruiken. Gegevens worden op verschillende plaatsen beheerd en de kans op fouten is groot. Het samenbrengen van data uit deze individuele systemen en het analyseren ervan, kost veel tijd, is zeer foutgevoelig of is zelfs onmogelijk. Hierdoor gaat GRC nooit werken en leidt het eerder tot onduidelijkheid, chaos en frustratie.

Een geïntegreerd GRC-platform ondersteunt organisaties bij het eenvoudig in control komen. Bij geïntegreerde software is sprake van een ‘single source of truth’. Gegevens voor de verschillende domeinen liggen maar een keer vast en hoef je slechts een keer te managen. Naast efficiency voordelen, biedt dat altijd écht inzicht, meer zekerheid en vertrouwen. Ook helpt het medewerkers om optimaal met elkaar samen te werken.



Andere voordelen van geïntegreerde GRC-software zijn:

- Je hebt de beschikking over geïntegreerde informatie, in plaats van (losse) gegevens. Hierdoor kun je betere beslissingen nemen en beter sturen om je organisatiedoelen te behalen.
- Eenmalig managen en toetsen van iedere maatregel, waarmee je tegelijkertijd risico’s mitigeert, beleid implementeert en voldoet aan normen, frameworks en wet- en regelgeving.
- Altijd inzicht in de mate van compliance met minimale Cost of Compliance.
- Automatisch periodiek uitzetten van audits, toetsen en assessments en altijd inzicht in het resultaat en de status. Ook in de tijd gezien.
- Altijd inzicht in de activiteiten die nog moeten plaatsvinden om o.a. risico’s te mitigeren en compliant te zijn, inclusief de mogelijkheid om deze activiteiten veel beter te prioriteren door risico gestuurd te werken.
- Aantoonbare audit trails waardoor je op ieder moment 'audit ready' bent.
- Altijd voorbereid op onvoorziene gebeurtenissen en toekomstige behoeften.
- Je bent succesvoller in het behalen van je doelen en je bent Fully In Control.

4. Selecteer de juiste (geïntegreerde) GRC-oplossing voor jouw organisatie

Het selecteren van een geschikte GRC-oplossing is niet eenvoudig. Hieronder beschrijven wij een aantal stappen die jouw organisatie kunnen helpen met het selecteren van de juiste oplossing.

Stap 1 Breng je huidige situatie in kaart

Het is verstandig om eerst je huidige situatie in kaart te brengen (IST situatie). Welke softwaresystemen, spreadsheets en andere hulpmiddelen gebruik je binnen het GRC-landschap? Welke GRC-activiteiten worden er door wie en hoe vaak uitgevoerd? Hoeveel tijd neemt dit in beslag? Welke informatie is waar opgeslagen? En wordt er mogelijk dubbel werk uitgevoerd? Om te begrijpen wat wel en wat niet van toegevoegde waarde is voor je organisatie is het belangrijk om antwoorden op deze vragen te krijgen.

Stap 2 Breng de knelpunten binnen je GRC-activiteiten in kaart

Nadat je inzicht hebt in de huidige situatie van je organisatie, is het van belang om de gewenste situatie in kaart te brengen (SOLL situatie). Als je daarna de IST en de SOLL situatie naast elkaar legt, heb je inzicht in de knelpunten binnen je GRC-activiteiten. Kijk ook wat breder dan alleen naar GRC. Staan Kwaliteitsmanagement, ISMS, Risk Based Performance Management of Privacy gerelateerde activiteiten al op de agenda van je organisatie? Kijk in hoeverre je dit nu of in de toekomst wilt integreren binnen de gewenste GRC-oplossing. Er is namelijk veel overlap tussen deze managementdomeinen. Probeer verder te achterhalen wat medewerkers lastig vinden aan hun werk en aan het gebruik van de huidige softwaresystemen en hulpmiddelen. Welke informatie missen ze? Hoe complex zijn hun werkzaamheden? En wat kost eigenlijk te veel tijd? Door antwoorden op deze vragen te krijgen, weet je snel op welke vlakken verbeteringen mogelijk zijn en krijg je inzicht in de gewenste situatie van je organisatie.

Stap 3 Kies de beste GRC-software voor jouw organisatie

Wanneer je weet wat je hebt en waar je naartoe wilt, is het tijd om een GRC-platform te kiezen dat optimaal aansluit bij deze behoeften. Bij deze keuze zou je in elk geval de onderstaande kritieke succesfactoren moeten laten meewegen.

Kritieke succesfactoren GRC-software:

- Integraliteit: managementdomeinen werken optimaal met elkaar samen.
- Een single source of truth: Gegevens liggen maar één keer vast en binnen de verschillende domeinen wordt overal gebruik gemaakt van dezelfde informatie.
- Intuïtief en laagdrempelig.
- Interactief: medewerkers kunnen optimaal samenwerken om hun doelen te bereiken.
- Innovatieve User Experience Design (UX): een betekenisvolle en aangename gebruikerservaring.
- Gericht op het succesvol behalen van je organisatie of projectdoelen: zorgt voor constante optimalisering en bijsturing van je organisatie.

5. Tot slot

In de traditionele uitvoering van GRC-activiteiten wordt nog vaak gebruik gemaakt van diverse softwaresystemen, spreadsheets en hulpmiddelen. Dit maakt het lastig om bepaalde informatie te delen en om data juist te analyseren, waardoor niet optimaal ingespeeld kan worden op de problemen, risico's en kansen van een organisatie. Dit zorgt (zonder uitzondering) voor veel handmatig werk. Hierdoor is de kans groot dat er fouten worden gemaakt en is de uitvoering van het GRC proces minder efficiënt dan het zou moeten zijn.

Geïntegreerde GRC-software, zoals Fully in Control, geeft daarentegen elke stakeholder in je organisatie precies de inzichten die hij of zij nodig heeft. Er is sprake van een single source of thruth dat overzicht, zekerheid en vertrouwen biedt en de cost of compliance aanzienlijk reduceert. Dankzij deze software zijn en blijven organisaties werkelijk in control als het gaat om GRC. Succesvolle organisaties kiezen niet voor niets voor geïntegreerde GRC-software.

FullyInControl
Works your way

Takenhofplein 1
6538 SZ Nijmegen
The Netherlands

+31 (0)85-3019073
info@fullyincontrol.nl
www.fullyincontrol.com