



16 tips voor de meest voorkomende valkuilen bij risicomanagement



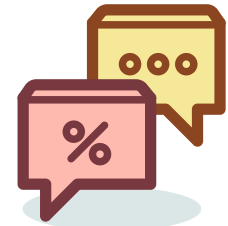


Herken je dit?

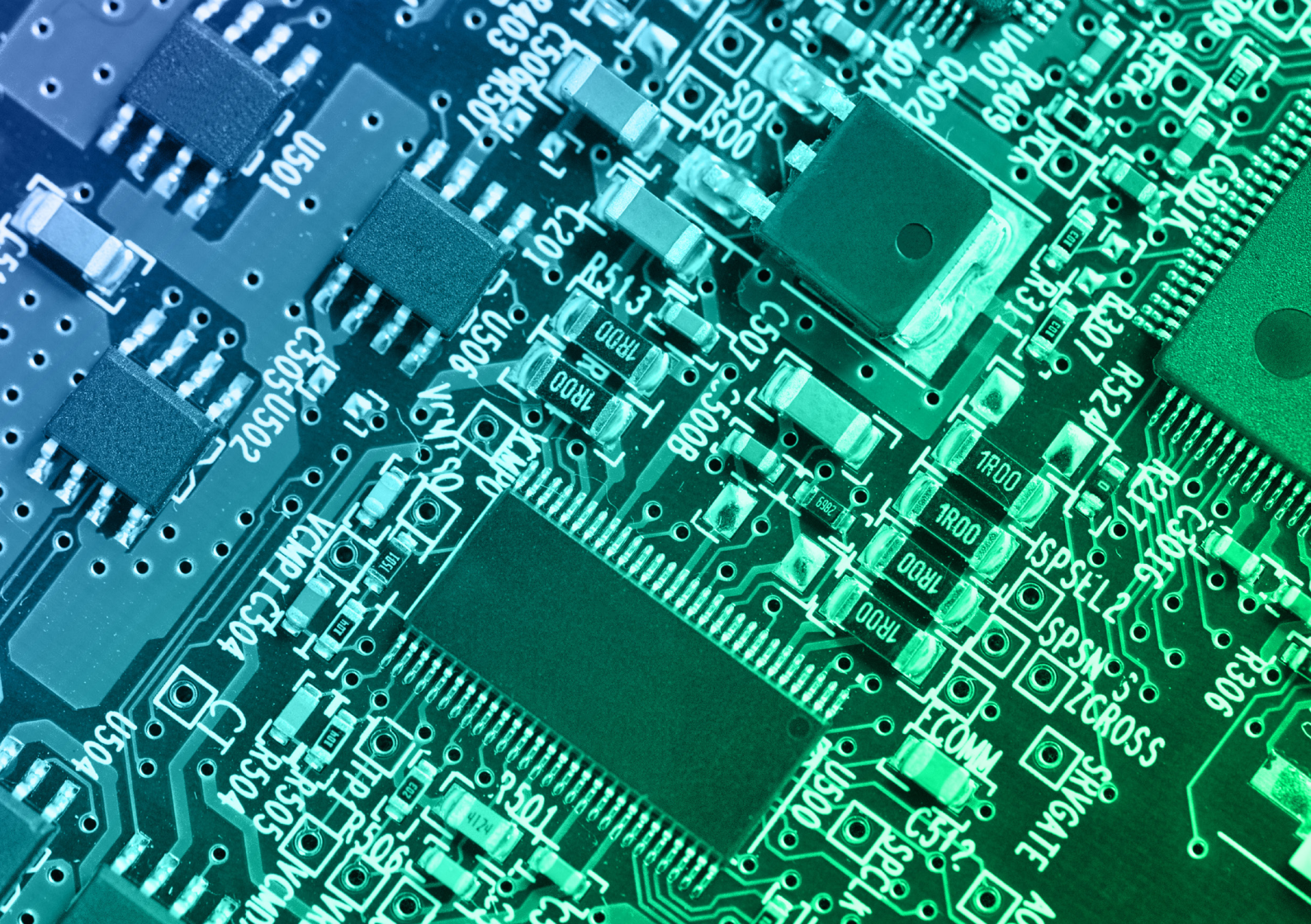
Voor veel organisaties is risicomanagement een verplichting (vanuit onder andere de NIS2) en tevens een administratieve last. In de huidige digitale wereld worstelen veel organisaties met de vraag: “Hoe zorg ik dat ik digitaal weerbaar ben?” Het voldoen aan wettelijke verplichtingen zoals AVG en NIS2, het voldoen aan de eisen van klanten en leveranciers en het vermijden van negatieve media-aandacht door een cyberaanval, zijn allemaal uitdagingen die organisaties onder ogen moeten zien.



...en je komt er niet uit?



Deze uitdagingen kunnen overweldigend zijn, vooral als je probeert te navigeren met dure en complexe GRC-oplossingen of als je worstelt met tijdrovende en inefficiënte tools zoals Excel. Het kan voelen alsof je constant het wiel opnieuw uitvindt, terwijl je eigenlijk je tijd en middelen zou moeten besteden aan het runnen van je bedrijf.



**“Ga niet op zoek naar 100% zekerheid.
Risicomanagement is geen exacte wetenschap.”**



Het is nu of nooit

De NIS2 dwingt af dat je organisatie aantoonbaar de digitale weerbaarheid op orde moet hebben! Je kunt als bestuurder persoonlijk aansprakelijk worden gesteld met boetes tot gevolg.



Klanten en leveranciers eisen meer. Niet voldoen is out of business.



Toezichthouders en inspecties eisen meer en meer. Vergunningen kunnen ingetrokken worden.



Cybercrime blijft toenemen.



Maar waar begin ik en hoe blijven de (administratieve) lasten zo laag mogelijk?

De afgelopen jaren hebben we met veel organisaties gesproken over risicomanagement en veel geleerd over hun ervaringen. Dit heeft geleid tot een lijst van 7 meest voorkomende fouten bij het implementeren en uitvoeren van risicomanagement. Vervolgens hebben we 16 tips gedefinieerd voor het robuust implementeren van risicomanagement om te voorkomen dat je in de valkuilen stapt. We hebben deze lessen gebundeld in een handzaam e-book waarmee je je voordeel kunt doen.





De 7 grootste valkuilen



1. Geen commitment van de top

Zolang de directie het belang van risicomanagement niet onderschrijft, zal de implementatie gedoemd zijn te mislukken.

2. Gebrek aan eigenaarschap

Zonder eigenaarschap van het risicomanagement proces, de risico's en de beheersmaatregelen worden activiteiten niet opgepakt en verbeteringen niet doorgevoerd.

3. Geen betrokkenheid van de lijn

Te vaak wordt risicomanagement belegd bij één functionaris, bijvoorbeeld de risicomanager'. Als de lijnmanagers geen commitment geven, sneeuwt risicomanagement onder in de waan van de dag.

4. We maken risicomanagement te ingewikkeld

Het is verleidelijk om risicomanagement complex te maken. Daardoor wordt de voortgang van implementatie ernstig vertraagd.

5. Risicomanagement sluit niet aan bij de strategie en doelstellingen van de organisatie

Organisaties die proportionaliteit (doen we de juiste dingen op de juiste manier) uit het oog verliezen ervaren risicomanagement als een te grote investering waarvan de benefits niet of nauwelijks ervaren worden.

6. De PDCA-cyclus ontbreekt

Risicomanagement werkt niet als er geen plan-do-check-act cyclus is geïmplementeerd. Het gevolg dat risicomanagement een eenmalige activiteit blijft is groot.

7. Geen schaalbare en laagdrempelige ondersteuning beschikbaar

Te vaak zien we dat organisaties hebben gekozen voor complexe tooling die onvoldoende aansluiten bij de ambities, strategie en doelstellingen van de organisatie. Dit demotiveert medewerkers omdat de administratieve lasten toenemen in plaats van afnemen. De tooling wordt slecht of niet gebruikt en de implementatie van risicomanagement is mislukt.

We geven 16 tips weg

Er is al veel bedacht in de wereld op het gebied van risicomanagement. Gebruik wat past bij jouw organisatie en beperk je (administratieve) lasten. Voldoe aan de wetgeving en wees aantoonbaar in control. Beheers je risico's, effectief en efficiënt. Veel succes met deze tips en neem vooral contact met ons op als je vragen hebt. 050 – 2111 729 - hallo@perium.nl



Tip 1 Ambitie



Ga niet op zoek naar 100% zekerheid. Risicomanagement is geen exacte wetenschap. Risicoanalyse gaat over het doen van aannames over wat er in de toekomst kan gebeuren en niemand heeft een glazen bol. Er bestaat dus geen 100% zekerheid. Er bestaan veel modellen, methoden en technieken om risico's te analyseren. Die hebben zeker waarde. Kies een manier die past bij je organisatie maar ga niet door tot achter de komma. Weet wanneer je moet stoppen. En besef; het gaat altijd om het antwoord op de vraag: Accepteer ik dit risico of niet? **Durf elkaar aan te spreken als je op zoek gaat naar te veel zekerheid!**



Tip 2

Proportionaliteit

Proportionaliteit impliceert dat de genomen maatregelen in verhouding moeten staan tot de ernst van het risico en de mogelijke impact ervan. Hierdoor werk je kosten efficiënt, terwijl tegelijkertijd adequate bescherming wordt geboden tegen reële bedreigingen. Een proportionele aanpak maximaliseert de effectiviteit van risicomanagement. Prioriteer beheersmaatregelen op basis van de risicoanalyse. Zorg dat je kunt groeien naarmate de organisatie verandert. Kies voor schaalbare oplossingen.

Vraag jezelf regelmatig af of dat wat je doet, proportioneel is!

Tip 3

Multidisciplinair

Betrek belanghebbenden van verschillende afdelingen bij het risicoanalyseproces, zodat je verschillende perspectieven krijgt en bredere input in overweging neemt. Dit draagt sterk bij aan de kwaliteit en draagvlak. Probeer de kans van een risico te scoren op basis van vastgestelde waarden. Probeer de impact van een risico te scoren op basis van vastgestelde mogelijke waarden van de impact op onder andere het gebied van financiën, imago/reputatie, operatie en HR. **Stel multidisciplinaire teams samen om periodiek de risico's te bespreken!**





Je bent alert op wat goed en niet goed gaat, je neemt initiatief tot verbetering en je volgt het effect ervan.”



Tip 4 Eigenaarschap

Eigenaarschap is een voorwaarde voor succesvol risicomanagement. Eigenaarschap betekent verantwoordelijkheid nemen en regelmatig verantwoording afleggen met betrekking tot de risico's en beheersmaatregelen. Het is belangrijk dat de eigenaar gevraagd wordt wat hij/zij nodig heeft om regelmatig feedback te geven op de status van het risico en de beheersmaatregelen. Eigenaarschap is verantwoordelijkheid voelen en nemen. Als professional wil je dat het werk goed verloopt en je weet dat jij daar een belangrijke bijdrage in hebt. Dat is je verantwoordelijk voelen. Je bent alert op wat goed en niet goed gaat, je neemt initiatief tot verbetering en je volgt het effect ervan. Dat is verantwoordelijkheid nemen. **Benoem een eigenaar voor elk risico en elke beheersmaatregel!**

Tip 5 Hergebruik

Er bestaan veel standaarden met risico's en beheersmaatregelen. Gebruik deze, je hoeft het wiel niet uit te vinden en zo ben je juist en volledig. Hergebruik voorgedefinieerde taken die je uit zult moeten voeren voor je managementsysteem. Ga op zoek naar bewezen best practices en tools voor specifieke maatregelen. Hergebruik beoordelingen van beheersmaatregelen van verschillende normen die gelijk zijn of grote overlap hebben.

Werk met standaarden en best practices!



Tip 6

Lijnverantwoordelijkheid

Lijnverantwoordelijkheid is essentieel voor risicomanagement omdat het de directe betrokkenheid van individuele teamleden en afdelingen bij het identificeren, beoordelen en beheersen van risico's waarborgt. Deze aanpak verspreidt de verantwoordelijkheid voor risico's over de organisatie en moedigt proactieve betrokkenheid aan. Door lijnverantwoordelijkheid worden risico's op operationeel niveau beter begrepen en kunnen gepaste maatregelen efficiënter worden geïmplementeerd, wat leidt tot een verhoogde veerkracht en betere prestaties van de organisatie. **Benoem medewerkers in de operatie als eigenaar van risico's en beheersmaatregelen!**

Tip 7

Commitment van de top



Zorg ervoor dat het belang van risicomanagement begrepen wordt op alle niveaus van de organisatie, van het management tot de werkvloer. De 'tone at the top' is van vitaal belang omdat het leiderschap de toon zet voor de organisatiecultuur en het gedrag van medewerkers. Als leiders risicobewust gedrag tonen en het belang van effectief risicomanagement onderstrepen, heeft dit een positieve invloed op de algehele veerkracht en prestaties van de organisatie. Het commitment is nodig voor het beschikbaar stellen van de middelen die nodig zijn om de risico's te beheersen. **Zet risicomanagement op de agenda van de directie en vraag commitment!**

Tip 8

Het 4-ogen principe

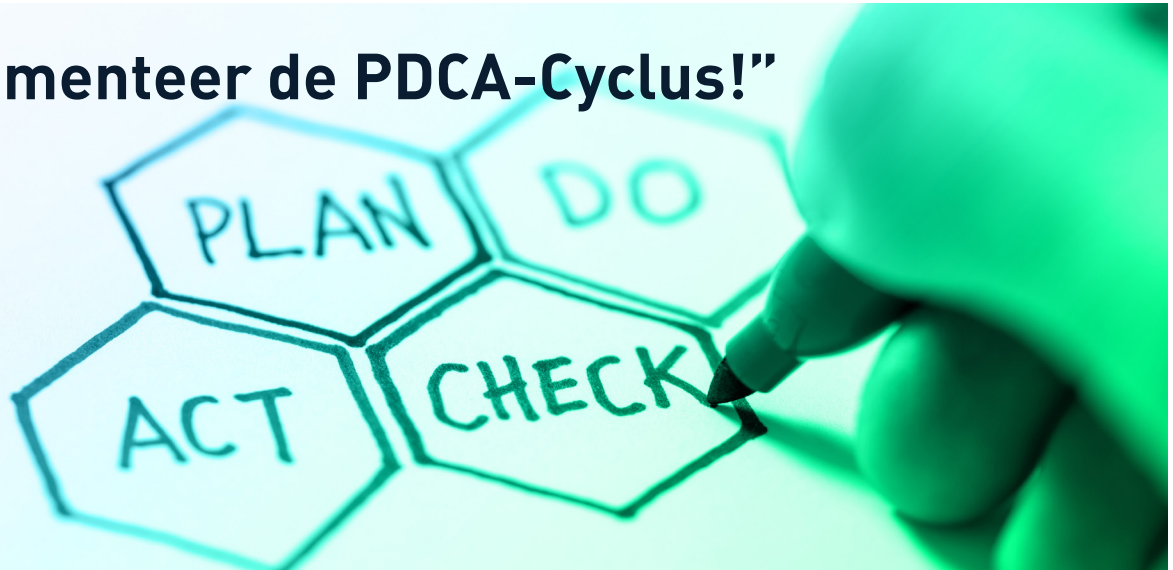
Het 4-ogenprincipe is een krachtig (en vaak onderschat) sturingsmiddel en draagt bij aan de kwaliteit op verschillende manieren: Foutdetectie, Verantwoordelijkheid, Fraudepreventie, Transparantie, Leermogelijkheden & Betrouwbaarheid. Het principe zorgt voor een extra laag van controle en verificatie die de algehele kwaliteit van het werk verbetert en helpt mogelijke problemen in een vroeg stadium te identificeren voordat ze grotere gevolgen hebben. **Implementeer het 4-ogen principe!**

Tip 9

De PDCA-Cyclus

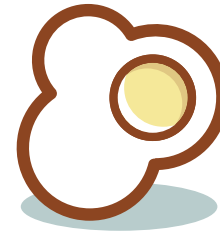
Risicomanagement is een continu proces. Dat betekent dat je periodiek beoordeelt hoe je risico's scoren op kans en impact en hoe effectief je beheersmaatregelen zijn. Daar waar nodig voer je verbeteringen door. De Plan-Do-Check-Act cyclus voor risicomanagement helpt bij het verminderen van het reactieve karakter en bevordert een proactieve benadering door voortdurend te plannen, uit te voeren, te evalueren en aan te passen. Dit resulteert in een continu verbeteringsproces. Elk goed managementsysteem (QMS, ISMS, PIMS) bevat de PDCA-cyclus. Mede daarom is een managementsysteem van groot belang.

“Implementeer de PDCA-Cyclus!”



Tip 10

Eenvoud



Je wilt snel aan de slag met laagdrempelige oplossingen. Kies voor een ondersteunende tool dat passend is: waarin de risico's en beheersmaatregelen al geïnventariseerd, gedefinieerd en gekoppeld zijn. Die het juiste managementsysteem aanbiedt inclusief de reguliere taken. Waarmee je zelf kunt kiezen wat je wel of niet registreert en hoe vaak je dat doet. Een regiefunctie heeft, die er voor zorgt dat de PDCA-cyclus automatisch voor je aan het werk gaat. Je niet voorschrijft welke methoden en technieken je moet gebruiken. Transparant is en overzicht en inzicht biedt. Meegroeit met jouw ambities. **Vraag je voortdurend af of zaken niet eenvoudiger kunnen!**



Tip 11

Definieer doelen

Je zult op verschillende niveaus doelen moeten definiëren. Je organisatiedoelstellingen zijn leidend. Vervolgens kun je je doelen vaststellen per domein, bijvoorbeeld op het gebied van informatiebeveiliging en privacy maar ook financieel, duurzaamheid, marketing, projecten en processen. Per risico kun je de gewenste netto score voor de kans en impact bepalen. Per beheersmaatregel kun je het ambitieniveau van de volwassenheid bepalen. De doelen op bovenstaande niveaus dienen een coherent geheel te zijn. **Stel doelen op alle niveaus vast!**

Tip 12

Train en communiceer

Risicomanagement is mensenwerk! Het trainen van mensen is van essentieel belang voor risicomanagement omdat goed opgeleide medewerkers de kennis en vaardigheden hebben om risico's te herkennen, te begrijpen en effectief te beheren. Training vergroot het bewustzijn over potentiële risico's. Communicatie is essentieel voor risicomanagement omdat het zorgt voor transparantie, begrip en samenwerking binnen de organisatie. Effectieve communicatie stelt belanghebbenden in staat om risico's te identificeren, te begrijpen en passende maatregelen te nemen. **Stel een opleiding-en communicatieplan op en voer dit uit!**



IN BIG LETTERS ...

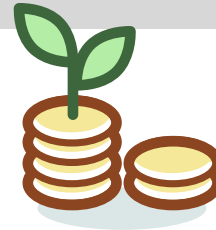
- Do start a draft
- Get your content right in the draft, draft and draft
- Clear advice will be given to you start in now:
- In week three of your theme / topic, you should have the average user knowledge. You should have a clear understanding of the user. What do they need to know? What do they not need to know?

Tip 13

Integreer in de bedrijfsvoering

Door risicomanagement te integreren in dagelijkse processen en besluitvorming, worden risico's systematisch proactief aangepakt in plaats van reactief. Dit bevordert veerkracht, verbetert de besluitvorming, minimaliseert verrassingen en ondersteunt de organisatie bij het bereiken van haar doelen op een duurzame en gecontroleerde manier. Denk aan het ontwikkelen van risicobewustzijn, integreer risicoanalyse in strategische planning, projectmanagement en operationele processen, rapporteer en evalueer. Maak risicomanagement onderdeel van de HR-cyclus. **Integreer risicomanagement in de bestaande processen!**

Tip 14 Focus en schaalbare maatregelen



Tijd en geld zijn schaars! Denk goed na welke investering je doet op basis van goed risicomanagement. Breng focus aan. Je kunt er ook voor kiezen om bepaalde beheersmaatregelen niet te implementeren of ineffectief te laten zijn als de gerelateerde risico's acceptabel zijn. Leg de onderbouwing goed vast. Bij het implementeren en verbeteren van beheersmaatregelen is het van belang dat maatregelen kunnen worden opgeschaald naarmate de omvang van een risico toeneemt. **Stel je zelf regelmatig de vraag of je aan de juiste maatregelen werkt en hoe schaalbaar deze zijn!**

Tip 15

Trendwatching

De wereld verandert in rap tempo! Door trends in industrie, technologie, regelgeving en economie te volgen, kunnen organisaties anticiperen op veranderingen en proactief maatregelen nemen om zich aan te passen aan nieuwe risicoscenario's. Hierdoor blijft het risicomanagement relevant en effectief in een steeds veranderende omgeving. Denk aan het volgen van relevante media, conferenties, online communities, forums en compliance updates. **Zorg dat je regelmatig de juiste bronnen raadpleegt!**



Tip 16

Beloon risicobewustzijn



Risicomanagement is mensenwerk! Erken en beloon individuen en teams die actief bijdragen aan het identificeren en beheren van risico's, om de betrokkenheid te stimuleren. Je kunt dit bereiken door bijvoorbeeld risicomanagement periodiek op de agenda te zetten van afdeling overleggen en onderdeel te laten zijn van de HR-cyclus. Besteedt aandacht aan risicomanagement in nieuwsbrieven, personeelsbijeenkomsten, beloon medewerkers die effectieve oplossingen aandragen, biedt training en cursussen aan en communiceer successen. **Zorg voor incentives voor risicobewustzijn!**



“Je kunt er ook voor kiezen bepaalde beheersmaatregelen niet te implementeren als de gerelateerde risico’s acceptabel zijn.”



Er is een oplossing...

Hier komt Perium in beeld. Perium is een platform dat speciaal is ontworpen om organisaties te helpen hun (digitale) weerbaarheid efficiënt en effectief te vergroten. Met Perium kun je voldoen aan wettelijke vereisten, de verwachtingen van klanten en leveranciers overtreffen en de kans op negatieve media-aandacht drastisch verminderen. Perium maakt gebruik van de filosofie 'create once, use many', waardoor je niet steeds opnieuw het wiel hoeft uit te vinden. In plaats daarvan kun je profiteren van wat al is bedacht en getest door andere organisaties.

...en die oplossing past.

Of je nu een grote organisatie bent met een team van specialisten, of een klein bedrijf zonder de middelen om dure specialisten in te huren, Perium biedt een betrouwbaar en kosteneffectief alternatief. Met Perium krijg je een praktische oplossing voor risicomanagement, waarmee je alle relevante informatie bij de hand hebt en kunt leunen op een sterke regiefunctie. Doe net als vele andere organisaties en kies voor Perium om je weerbaarheid te vergroten.



Resultaten tot nu toe...

“Wij hebben met Perium grip op onze digitale risico's, nemen betere besluiten en besparen geld.”

“Onze PDCA-cyclus is vele malen sterker geworden waardoor we ECHT groeien.”

“Onze administratieve lasten zijn sterk verminderd waardoor we meer tijd hebben om te werken aan belangrijke zaken.”

“We konden binnen een half uur aan de slag met Perium. Geen dure implementatie trajecten. Een verademing! “





De voordelen!

- ✓ Overzicht en inzicht
- ✓ Efficiënt en effectief ISMS
- ✓ Aantoonbaar in control
- ✓ Verlaging administratieve lasten en auditlasten
- ✓ Hogere digitale weerbaarheid

**“Perium biedt een betrouwbaar en
kosteneffectief alternatief.”**

De volgende stap!

Wil je als organisatie aan de slag met risicomanagement? Ben je op zoek naar een partner die je daarin optimaal faciliteert tegen lage kosten?

Plan dan nu een gratis gesprek in om kennis te maken en waarin we je de mogelijkheden van Perium laten zien.

050 – 2111 729
hallo@perium.nl

Perium BV
Atoomweg 6b
9743 AK Groningen

