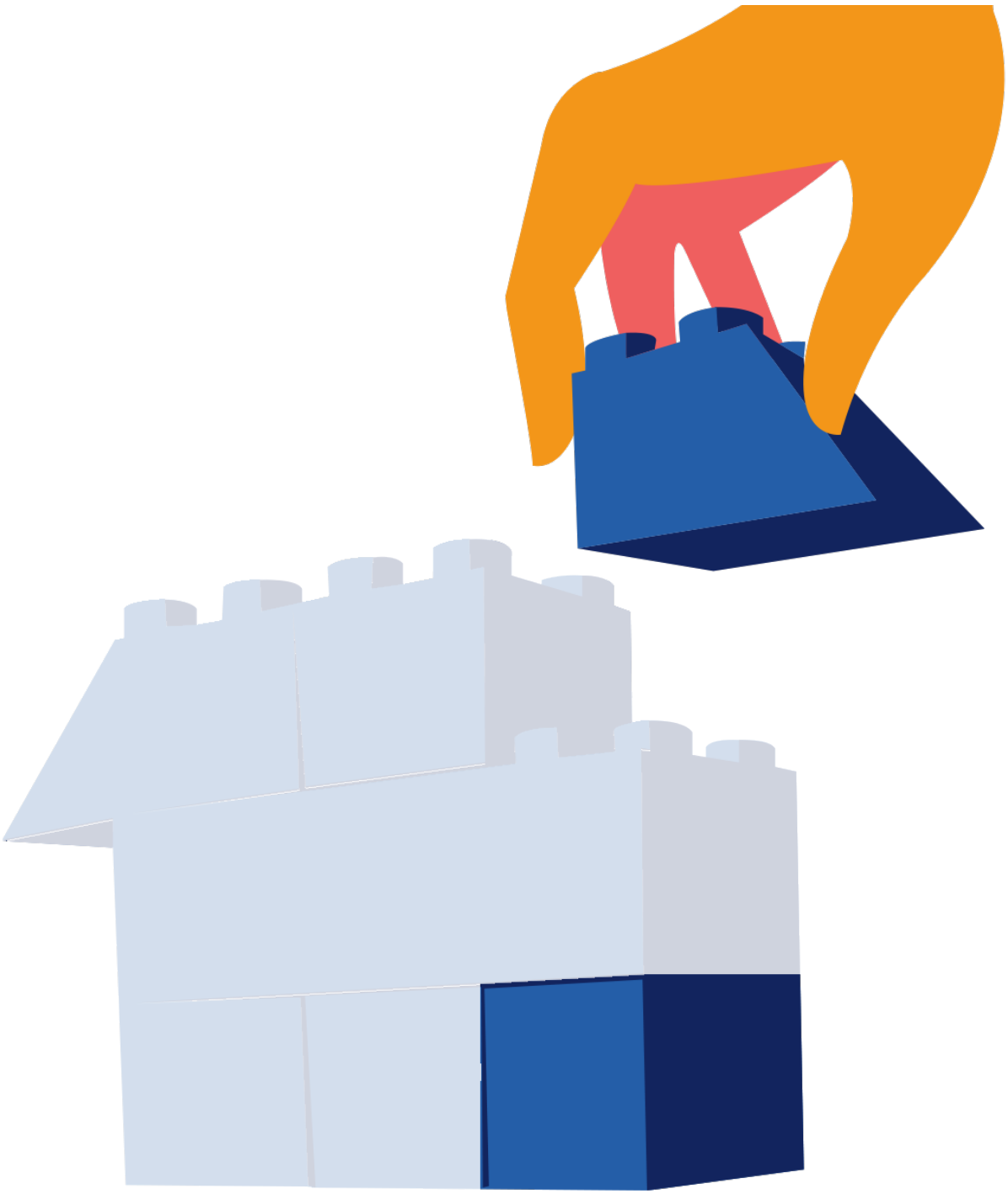
Audittrail
information security | privacy | quality | grc

BIC Building Blocks
Risico's & Impact



RISICOMANAGEMENT

"Risicomanagement is het systematisch opzetten, uitvoeren en bewaken van acties om risico's te identificeren, te prioriteren, te analyseren en voor deze risico's oplossingen te bedenken, te selecteren en uit te voeren."

Veel corporaties starten informatiebeveiliging met een normenkader zoals de BIC. Door de maatregelen van dit kader toe te passen bereikt u een algemene basisbeveiliging voor uw gehele organisatie. Maar is al uw informatie hiermee voldoende beschermd? Met pássende informatiebeveiliging implementeert u precies die maatregelen die nodig zijn om uw informatie te beschermen. Elke organisatie is anders en daarom is beveiliging voor elke organisatie uniek.

Om te komen tot passende beveiliging is een het uitvoeren van een classificatie van informatie en goede risicoanalyses essentieel. De mate waarop u beveiligingsmaatregelen toepast binnen uw organisatie is afhankelijk van het type gegevens dat u in huis heeft, de risico's die u bereid bent te nemen en de manier waarop u risico's wenst te mitigeren. Maar hoe bepaalt u waar de grens ligt van uw risicobereidheid? En hoe komt u tot een goede afweging tussen dreiging, kans en impact? Dit whitepaper behandelt het onderwerp risicomanagement.

CLASSIFICATIE VAN INFORMATIE

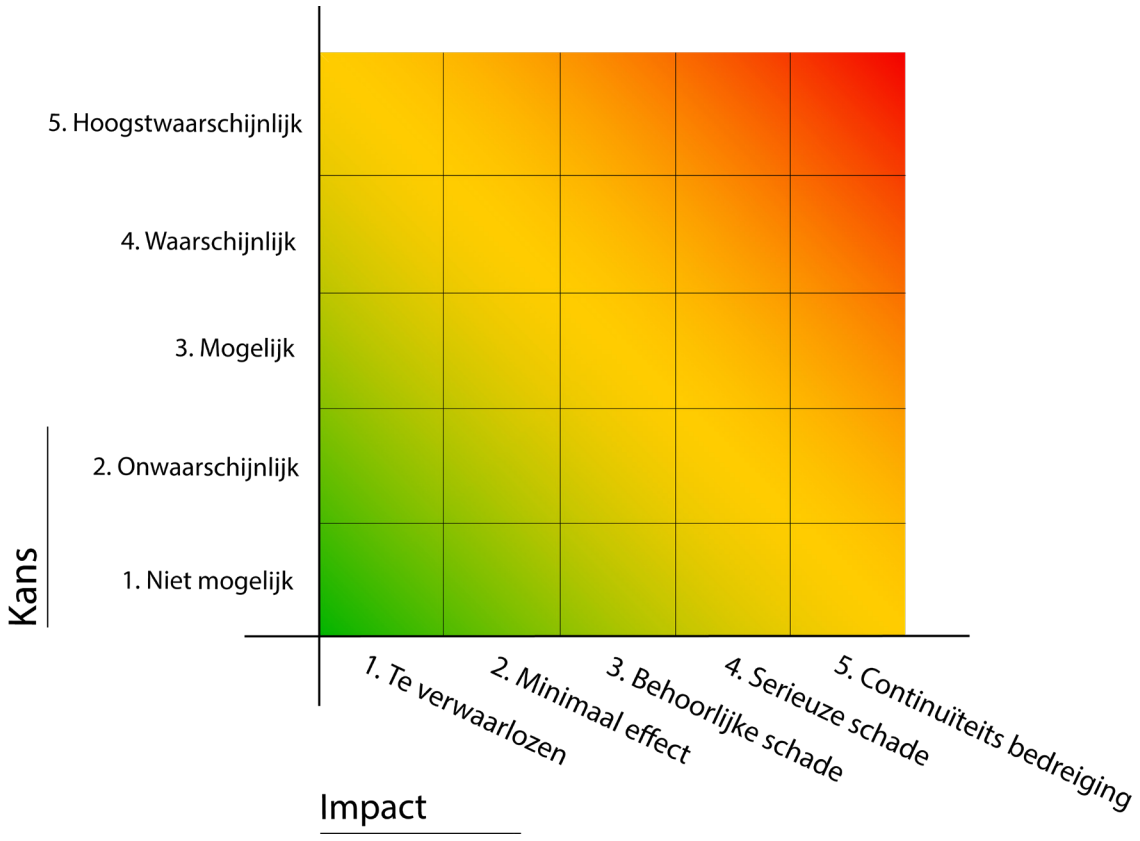
Om te komen tot passende beveiliging is een classificatie van alle informatie die een organisatie rijk is essentieel. Het classificeren van informatie gebeurt aan de hand van drie betrouwbaarheidseisen: de beschikbaarheid (B), integriteit (I) en vertrouwelijkheid (V) van de informatie. Met het scoren van informatie op deze drie punten kunt u veel gerichter maatregelen kiezen die passen bij de behoefte van de organisatie, bijvoorbeeld door de (bijzondere) persoonsgegevens binnen uw organisatie af te schermen met een extra wachtwoord.

Classificeren start met inventariseren. Vaak heeft u hier al een start mee gemaakt met het verwerkingsregister: een inventarisatie van alle persoonsgegevens binnen uw organisatie en een verplichting vanuit privacywetgeving. Naast persoonsgegevens is het belangrijk ook andere type gegevens te verzamelen. Onderstaand model geeft aan op welke wijze u de gegevens kunt scoren. In de Bic Building Blockssjablonen kunt u ook een voorbeeld vinden die u helpt bij het scoren.

Bev. klasse: Categorie:	Zeer laag - 1	Laag - 2	Gemiddeld - 3	Hoog - 4	Zeer hoog - 5
Beschikbaarheid	Onnodig	Onnodig	Belangrijk binnen beperkte tijd	onmisbaar binnen beperkte tijd	Onmisbaar 24u/dg
Vertrouwelijkheid	Openbaar	Openbaar	Intern openbaar	Vertrouwelijk	Cruciaal vertrouwelijk
Integriteit	Onnodig	Wenselijk	Noodzakelijk	Onontbeerlijk	Cruciaal
Maatregelen	Geen eisen	Voldoen aan basis eisen	Voldoen aan minimale vereisten	Voldoen aan hoge vereisten	Voldoen aan bijzondere vereisten

BEDREIGINGEN, KANS EN IMPACT

Een risico is de rekensom van de kans x impact van een bedreiging. Met andere woorden: wanneer u een bedreiging voor uw gegevens identificeert, zult u daarnaast ook moeten inschatten wat de kans is dat deze bedreiging zich voordoet en daarnaast wat de impact zou zijn wanneer de bedreiging ook daadwerkelijk tot uiting komt. De inschatting kunt u doen op basis van een vijfpuntsschaal. Al uw risico's zijn vervolgens te plotten in onderstaand model, ook wel een heatmap genoemd.



Audittrail
information security | privacy | quality | grc

STANDAARD RISICOPROFIEL CORPONET

Corponet heeft voor woningcorporaties een standaard risicoprofiel opgesteld met bedreigingen voor de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens, alsmede een set aan algemene bedreigingen. Dit onderstaande profiel is ook terug te vinden in de BIC.

Het algemene dreigingsprofiel voor woningcorporaties, categorie Vertrouwelijk, is voor de Baseline vastgesteld op onder andere de volgende bedreigende factoren:

- de onbetrouwbare medewerker
- de wraakzuchtige medewerker
- de wraakzuchtige huurder
- de verontruste huurder
- de actiegroep
- de criminele opportunist
- de ingehuurde medewerker
- de vreemde overheden
- georganiseerde misdaad

BIV
als basis voor
BIA

Hierbij zijn onder andere de volgende bedreigingen gedefinieerd voor woningcorporaties, categorie Vertrouwelijk:

- infiltratie light
- social engineering
- publiek benaderbare sociale netwerken
- verhoor (fysiek geweld tegen personen)
- hacking op afstand
- malware (met en zonder remote control)
- crypto kraken
- ransomware
- (draadloze)netwerken interceptie
- (draadloze)netwerken actief benaderen
- inpluggen op fysiek netwerk
- verlies/diefstal van media
- publieke ruimtes
- achterblijven van patches
- beproeving van fysieke, technische en elek tronische weerstand

Naast de specifieke bedreigingen gaat de Baseline ook uit van een set algemene dreigingen waarvan de hoofdgroepen zijn:

- onopzettelijk menselijk handelen
- opzettelijk menselijk handelen
- niet-beïnvloedbare externe factoren
- technisch falen

Uitgesloten zijn de volgende bedreigers:

- terreurgroep

Audittrail
information security | privacy | quality | grc

RISICOANALYSE EN RISICO'S MANAGEN

RISICOANALYSE

Het uitvoeren van een risicoanalyse kan op elk type asset binnen uw organisatie: zowel op systemen, applicaties, gegevensverzamelingen of processen. Wat past het beste bij uw organisatie? Wanneer u een volledig proceshuis heeft ingericht met proceseigenaren is het aan te bevelen om risicoanalyses op procesniveau uit te voeren. Mocht u echter veel meer systeemgericht werken, dan kunt u er ook voor kiezen te starten met risicoanalyses op applicatieniveau: zolang u maar ergens een start maakt en alle risicoanalyses volgens eenzelfde methodiek uitvoert. Op deze manier voorkomt u het vergelijken van appels met peren. Daarnaast is het van belang om aan te sluiten bij het risicomanagementbeleid van de organisatie. Zo krijgt informatiebeveiliging een verbinding met het strategische risicolandschap en daarmee een plaats op de agenda.

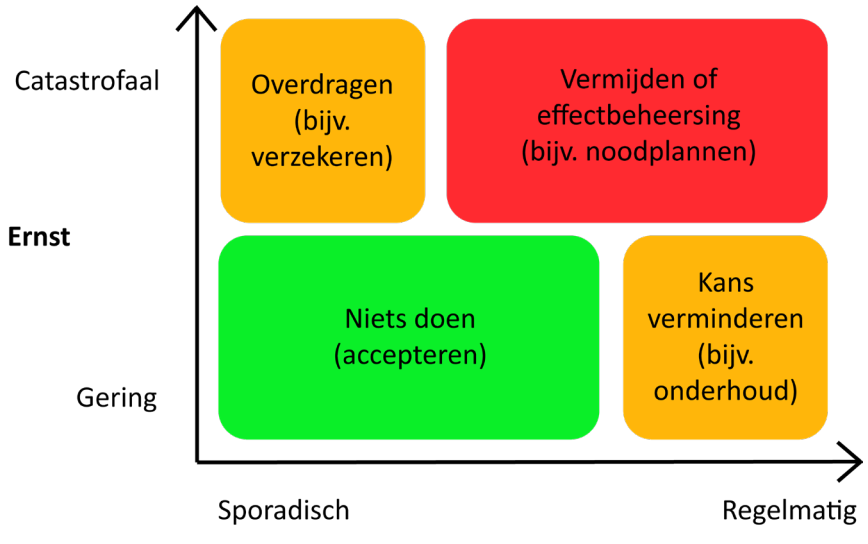
Bij de Bic Building Blockssjablonen is een voorbeeld te vinden die u ondersteunt bij het uitvoeren van een risicoanalyse.

RISICO'S MANAGEN

Nu alle data is geclassificeerd en alle risico's in kaart zijn gebracht is het tijd om maatregelen te treffen om risico's te verkleinen ofwel mitigeren. Voor elk risico zijn een aantal opties die u kunt overwegen:

1. Accepteren. Vooral de risico's waarbij de kans en/of impact verwaarloosbaar zijn kunnen worden geaccepteerd. Hoeveel risico's u wenst te accepteren, is volledig afhankelijk van de risicobereidheid (ook wel risk appetite) van uw organisatie en kan ook afhankelijk zijn van het risico zelf. Ga hierover vooral in gesprek met elkaar!
2. Voorkomen. Soms heeft u de mogelijkheid om een risico te voorkomen of vermijden. Bijvoorbeeld door de applicatie niet aan te schaffen, een andere leverancier te zoeken of een proces anders in te richten. Maar ook werken aan awareness is een vorm van preventie!
3. Overdragen. Sommige risico's zijn over te dragen. Denk hierbij aan verzekeringen.
4. Mitigeren. Hier komen de BIC maatregelen bij kijken. Door het implementeren van deze maatregelen kunt u risico's verkleinen.

Hoe u het beste kunt starten met het implementeren van maatregelen en een pakket van maatregelen kunt onderhouden komt aan bod in onze volgende whitepaper.



Audittrail
information security | privacy | quality | grc

Contactgegevens
Audittrail
Sisalbaan 5a
2352 AE Leiderdorp

KantNoord
Winschoterdiep 50
9723 AB Groningen

071 - 747 71 71
BBB@audittrail.nl

Audittrail
information security | privacy | quality | grc