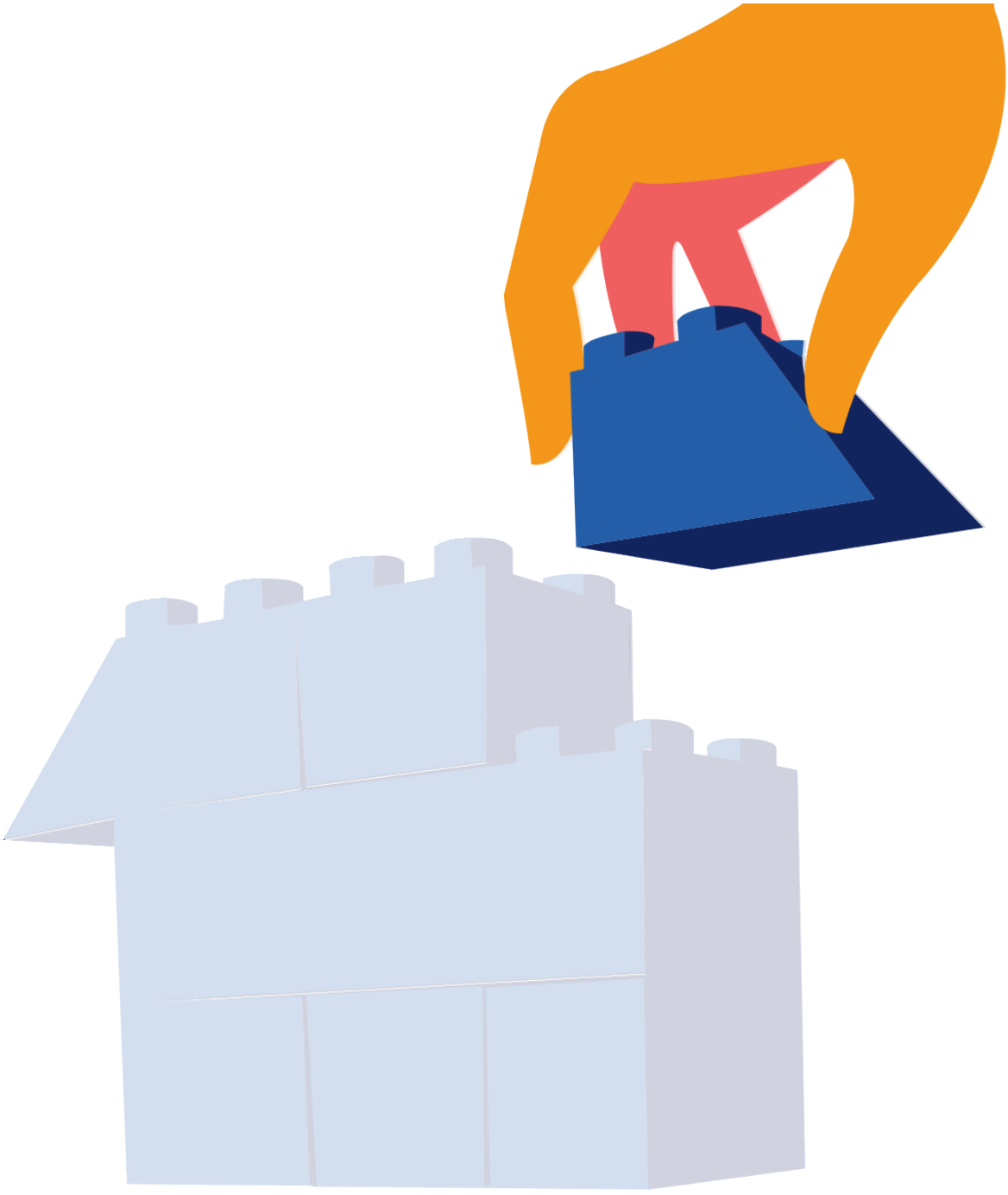
Audittrail
information security | privacy | quality | grc

BIC Building Blocks
Beleid & Strategie



INFORMATIEBEVEILIGING

BIC

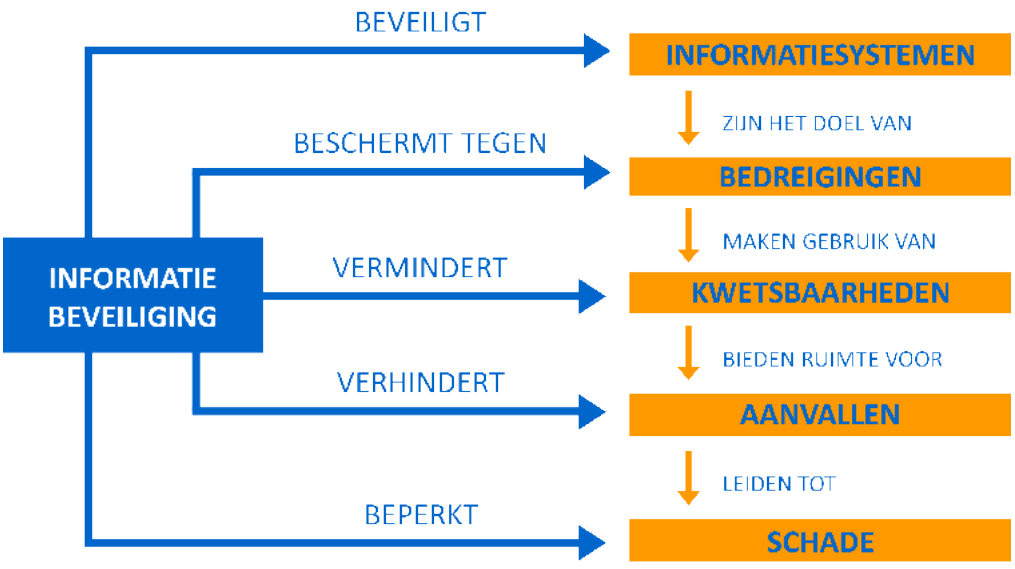
De informatievoorziening van een organisatie is het geheel van mensen, middelen en maatregelen, gericht op de informatiebehoefte van die organisatie.

Informatiebeveiliging garandeert de beschikbaarheid, integriteit en vertrouwelijkheid van alle vormen van informatie en de informatievoorziening binnen de grenzen van een organisatie.

Informatiebeveiliging gaat niet alleen over fysieke en technische maatregelen, maar ook over organisatie, processen en bovenal menselijk gedrag.

Informatiebeveiliging is een breed begrip en kent vele facetten. De implementatie van een goed informatiebeveiligingsbeleid is een complex project. Als kapstok voor woningcorporaties is een Baseline voor informatiebeveiliging uitgewerkt (BIC).

De belangrijkste trend op het gebied van informatiebeveiliging is het almaar toenemende belang ervan. In het algemeen kan worden gesteld dat dit belang toeneemt naarmate het aantal mensen met toegang tot de diverse informatiebronnen groter wordt.



DOELSTELLING

Het beschermen van de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie(systemen).

Beschikbaarheid

Zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers.

Integriteit

Beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.

Vertrouwelijkheid

Waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking.

BESCHERMEN VAN KROONJUWELEN

Informatiebeveiliging dient een dynamisch proces te zijn. Het raakt de gehele organisatie, ketenpartners en klanten.

Data, informatie en systemen raken de kernprocessen van corporaties. Corporaties verwerken hoofdzakelijk persoonsgegevens, financiële gegevens, vertrouwelijke plannen en maken gebruik van kritieke systemen. Risico's liggen op het vlak van privacy van huurders en medewerkers, maar ook op het vlak van dienstverlening. Uitval van ICT leidt bijvoorbeeld tot problemen bij dienstverlening.

Veilig werken betekent vooral een veilige en goed georganiseerde inrichting van werkprocessen. Een belangrijk onderdeel hiervan is dat medewerkers bewust zijn en blijven. Techniek kan namelijk niet alles oplossen, het blijft mensenwerk. Risico's accepteren kan, zolang je dit bewust doet.

BELANGRIJKSTE RISICO'S

- Menselijke fouten (verkeerd geadresseerde e-mails, links aangeklikt, device verloren).
- Onvoldoende waarborging voor veiligheid in samenwerking met ketenpartners en leveranciers.
- "Gedeelde" verantwoordelijkheden in samenwerkingsverbanden.

RISICOBEREIDHEID (WAT IS ACCEPTABEL?)

Risicomanagement behoort ingebed te zijn in alle afdelingen en is een continu proces. 100% veilig bestaat niet en 100% risico's afdekken bestaat ook niet. Er zijn gradaties (volwassenheidsniveaus). Deze behoeven elk andere maatregelen. Er is geen One-Size-Fits-All oplossing.

- Risicoanalyse is het middel
- Beheersbaarheid is de sleutel
- Een gestructureerde aanpak loont!

Audittrail
information security | privacy | quality | grc

OVERIGE RISICO'S INFORMATIEBEVEILIGING

UITDAGINGEN

- Extern: hackers en datalekken.
- Extern: wetten, (Europese) regelgeving en boetes.
- Intern: toenemende interesse vanuit RvC en accountants.
- Techniek: verdergaande complexiteit, cloud, outsourcing, klantportalen en uitwisseling van gegevens.
- Proces: dat processen steeds meer afhankelijk worden van informatie die beschikbaar is en steeds meer informatie die opgeslagen wordt.
- Mens: nog altijd de zwakste schakel (niet alleen fraude, ook onwetendheid van goedwillenden).

INFORMATIEBEVEILIGING STUREN

- U staat aan het roer, de directie bepaalt de richting.
- Ga met bestuur in gesprek over risico's en beheersing.
- Het (lijn)management draagt zorg voor uitvoering.
- Security officer is eerste aanspreekpunt bij vragen over informatiebeveiliging.
- Richt een werkgroep in die adviseert en een samenhangend pakket aan maatregelen opstelt voor de gehele organisatie aan de hand van de BIC.
- Uitdaging om de agenda niet te laten bepalen door de waan van de dag.

DE WERKGROEP INFORMATIEBEVEILIGING

- Is een organisatiebrede werkgroep.
- Is verantwoordelijk voor de implementatie en borging van informatiebeveiliging in de organisatie.
- Heeft een adviserende rol richting directie/MT op het gebied van informatiebeveiliging.
- Stelt het jaarplan informatiebeveiliging vast en draagt zorg voor de uitvoering hiervan.
- Zet activiteiten met betrekking tot informatiebeveiliging uit in de organisatie en bewaakt de uitvoering hiervan.
- Rapporteert aan de directie.

Informatiebeveiliging betreft niet alleen de beveiliging van ICT systemen. Het betreft ook veilig personeel, fysieke (toegangs) beveiliging, privacy en het beheer van bedrijfsmiddelen.

Audittrail
information security | privacy | quality | grc

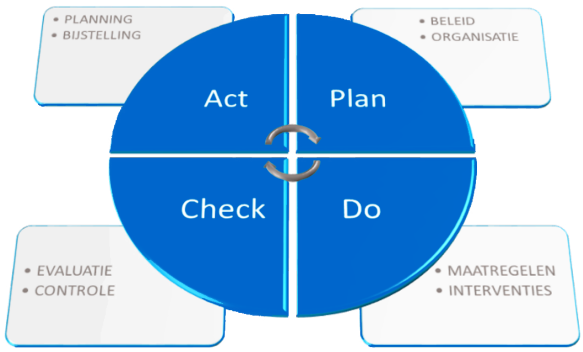
INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

Het hoofddoel van een ISMS is het verbeteren van de effectiviteit van informatiebeveiliging door een procesmatige aanpak, die wordt ondersteund door het management.

Het doel van het ISMS is onder andere het continu beoordelen van welke beveiligingsmaatregelen passend zijn en deze indien nodig bij te stellen.

Het ISMS is een proces dat de basis legt voor passende beveiligingsmaatregelen over de langere termijn.

Het ISMS wordt uitgevoerd door de informatiebeveiligingsorganisatie met verschillende activiteiten in de PDCA-cyclus van het ISMS.



ISMS is een procesbenadering voor de beheersing van informatiebeveiliging van bedrijfsvoeringprocessen, de onderliggende informatiesystemen en het informatiegebruik in de meest brede zin van het woord. Het ISMS heeft ook betrekking op de informatie die daarbinnen verwerkt wordt.

Een ISMS helpt corporaties om de beveiligingsdoelstellingen te ondersteunen, bijvoorbeeld door:

- De bedrijfscontinuïteit te faciliteren
- Een bijdrage te leveren aan de juiste beveiliging van middelen
- Instructies, werkwijze, evaluatie van informatiebeveiligingsincidenten.
- Implementeren van beveiligingsmaatregelen en het zoveel mogelijk reduceren van de bijbehorende kosten.
- Het rapporteren en leren omgaan met verantwoording. Een bijdrage te leveren aan verbeterde interne controle van beveiligingsmaatregelen.

ISMS
=
een proces

Audittrail
information security | privacy | quality | grc

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

Het hoofddoel van een ISMS is het verbeteren van de effectiviteit van informatiebeveiliging door een procesmatige aanpak, die wordt ondersteund door het management

ACT

Rapportage status en effectiviteit van de maatregelen:

- Evaluatie
- Managementrapportage en stuurinformatie
- Verbetervoorstellen

Evalueren en bijsturen

PLAN

Wet en regelgeving

BIC

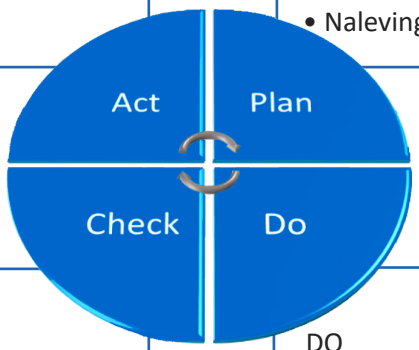
Corporatie beleid en doelstellingen

Beleidskaders Informatiebeveiliging:

- Organisatie en governance
- Informatiegebruik en personele aspecten

Beheer informatiebeveiliging:

- Business continuïteit management
- Naleving en controle



CHECK

Inzicht status en effectiviteit van de maatregelen van:

- Selfassessments
- Onafhankelijke audits
- Interne controles
- (Management) Rapportages

Uitvoeren van:

- Kwetsbaarheidsscans
- Pentesten
- Social enginering
- Evaluatie en Rapportage

DO

Beleidskaders vertaald in concrete maatregelen en acties:

- Informatiebeveiligingsplan
- 0-meting en GAP Analyse BIC
- Richtlijnen en maatregelen
- Architectuur van beveiliging
- Richtlijnen, procedures en werkinstructies
- Bewustwordingsprogramma
- Sturen op naleving

Op basis van risicomanagement word vastgesteld wat de (rest)risico's zijn.

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