



Concern Informatiebeveiligingsbeleid 2018

College van B&W

Datum

1 februari 2018

Voorwoord

Gemeente Rotterdam zet zich in om een betrouwbare en cyberveilige stad te zijn voor bewoners, bezoekers, studenten en ondernemers. We werken dus aan een aantrekkelijke stad die een veilige haven is voor mensen en bedrijven. De maatschappij wordt steeds meer digitaal. Digitalisering versnelt binnen nu en 2030 de wereld met twintig keer, doordat wereldburgers 24 uur per dag digitaal met elkaar verbonden zijn en zij continu gezamenlijk werken aan doelstellingen en initiatieven. Ons leven is zelfs afhankelijk van digitale voorzieningen. Dit maakt ons kwetsbaar. Deze kwetsbaarheid is een bedreiging voor zaken zoals ons grondwettelijke¹ recht op privacy, de democratie, de economie, gezondheid, etc.. Informatiebeveiliging maakt het mogelijk met passende maatregelen die kwetsbaarheid te verminderen. Deze maatregelen zitten zeker niet alleen in techniek, maar vooral ook in veilig menselijk gedrag.

De geschiedenis laat zien dat de stad Rotterdam flexibel en veerkrachtig is. De prachtige skyline is een bewijs van deze cultuur en mentaliteit. Deze zelfde instelling passen we toe in het beschermen van gemeentelijke en burger informatie. Waar Rotterdam ontwikkelt, innoveert en ondersteunt, neemt de gemeente haar verantwoordelijkheid voor de gerelateerde risico's en ziet toe op een vooruitgang die we vol kunnen houden.

Het gecontroleerd omgaan met risico's is een grote verantwoordelijkheid voor directie, lijnmanagement en alle medewerkers van de gemeente. De beveiligingsorganisatie binnen de gemeente zet zich in om directie en lijnmanagement te faciliteren in het beveiligen van informatie van medewerkers en de gemeentelijke taken/processen waar zij verantwoordelijk voor zijn. De primaire processen hebben elk hun eigen dynamiek die bescherming vraagt. Denk bij de verschillende clusters aan:

- Maatschappelijke Ontwikkeling met gevoelige informatie over de gezondheid van vaak kwetsbare burgers.
- Werk en Inkomen dat de integriteit van de uitkeringsverstrekking bewaakt en burgers ondersteunt om ondanks privéomstandigheden te kunnen werken en leven.
- Dienstverlening dat eigenaar is van de basisadministratie van Rotterdamse burgers met al haar gevoelige facetten.
- Stadsontwikkeling dat verantwoordelijk is voor vastgoedontwikkelingen, verkeer en de economie van de stad.
- Stadsbeheer dat bruggen, sluizen, riolering en de basisadministratie van gebouwen onderhoudt en beschermt.
- Bestuurs en Concernondersteuning met privacy gevoelige gegevens van alle medewerkers in beheer en de verwerking van de financiële gegevens van de gemeente.

Dit strategische informatiebeveiligingsbeleid van de gemeente Rotterdam heeft als doel het beschermen van gemeentelijke informatie en informatie van burgers, bedrijven en ketenpartners. Het uitgangspunt is dat de bescherming van de informatie aansluit bij de risico's, bedrijfsvoering en relevante wet- en regelgeving. Dit beleid vormt een kapstok voor nadere uitwerkingen en een leidraad voor het handelen van iedere ambtenaar, inhuur en contractant. Het college van B&W hecht grote waarde aan dit onderwerp en verwacht hetzelfde van iedere betrokken ambtenaar. Ieder individu is verantwoordelijk voor het veilig omgaan met gevoelige informatie.

¹Hoofdstuk 1, artikel 10, lid 1 en 2 van de grondwet "Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer."; "De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens."



Inhoudsopgave

Voorwoord	2
1. Inleiding	4
2. Uitgangspunten voor Informatieveiligheid	8
3. Continu leren, verbeteren en verantwoorden.....	11
4. Organisatie van de informatiebeveiliging	13
5. Naleving en compliance	17
Bijlage 1: Onderhavig strategisch kader en andere relevante beleidsdocumenten	19
Bijlage 2: Relevante documenten en bronnen	19
Bijlage 3: Weerbaarheid	21
Bijlage 4: Verklarende woordenlijst	22

1. Inleiding

Aanleiding

Door de technologische ontwikkelingen en de stijging van de waarde van informatie in onze maatschappij is regelmatige actualisatie van het beleid en maatregelen noodzakelijk. Denk bijvoorbeeld aan de ontwikkelingen waarbij steeds meer informatie en functionaliteit wordt geboden vanuit de cloud. Het recente onderzoek van de Rekenkamer² heeft uitgewezen dat dankzij investeringen in het verleden de belangrijkste bedreigingen, namelijk de bedreigingen van buitenaf, zeer beperkt zijn, maar dat bedreigingen op locatie (lees: in de gebouwen van de gemeente) aandacht behoeven. Bovendien moet het bewustzijn van alle medewerkers op een hoger plan gebracht worden. Door continu te werken met oog voor risico's en bedreigingen borgen we cyberveilige werkprocessen en creëren we tevens een belangrijke succesvoorwaarde voor innovatieve ontwikkelingen binnen de gemeente. Immers, innovatieve trajecten zullen alleen tot werkelijkheid kunnen komen wanneer ze voldoen aan wet en regelgeving en de risico's op beveiligingsincidenten geminimaliseerd zijn. Door de kans daarop sterk te verkleinen voorkomen we dat innovatieve trajecten onnodige kosten met zich meebrengen of schade toebrengen aan burgers of bedrijven.

Vanwege de ontwikkelingen in het dreigingslandschap gaat de gemeente door met investeringen voor de bescherming tegen aanvallen van buitenaf. Dit blijft een continue opgave. De investeringen in dat kader zijn naast preventief ook gericht op detectie en het snel verhelpen van kwetsbaarheden en incidenten. Dit moet leiden tot een gemeentelijke beveiligingsorganisatie die in staat is snel en adequaat te reageren op het snel wisselende karakter van de risico's die de gemeente loopt.

Dreigingslandschap voor de gemeente Rotterdam

De grootste dreiging gaat uit van statelijke actoren (digitale spionage) en van beroepscriminelen (cybercriminaliteit). Voor Rotterdam is met name deze laatste een reële dreiging gezien de incidenten in de afgelopen periode: diefstal van login-gegevens, hacken van websites, malware, etc. Digitale spionage vormt net als voorgaande jaren eveneens een grote dreiging, maar voor de gemeente Rotterdam zijn er vooralsnog geen concrete bewijzen dat wij hierdoor zijn geraakt. De kans is echter wel degelijk aanwezig en reëel, zoals ook aangetoond is tijdens de afgelopen Franse en Amerikaanse verkiezingen. Mede door de aanwezigheid van een wereldhaven ligt het wel voor de hand dat Rotterdam doelwit is. De gemeente wordt door de AIVD gewaarschuwd hiervoor.

In het algemeen winnen aanvallen aan complexiteit, omvang en impact. In de loop van 2017 zien wij in Rotterdam een toename van het aantal meldingen vanuit het Nationaal Cyber Security Centrum (NCSC) met het label: hoge kans, hoge impact. Verder zal de trend van steeds meer verzamelen en aftappen van informatie en gebruiken in allerlei activiteiten zal zich de komende jaren voortzetten. Het verlies van grip op informatie blijft een reële dreiging.

De Rekenkamer geeft als één van de conclusies in haar rapport aan dat medewerkers een risico vormen. Medewerkers van de gemeente Rotterdam werken voor de stad, bedrijven en burgers en gebruiken daarvoor aanzienlijke hoeveelheden (privacygevoelige) informatie. Ondanks het feit dat medewerkers geacht worden zorgvuldig om te gaan met informatie is het onvermijdelijk dat er fouten gemaakt worden. Vanuit de beveiligingsorganisatie wordt daarom veel nadruk gelegd op het versterken van de bewustwording van medewerkers, hierdoor zijn zij in plaats van een dreiging een onmisbare schakel in onze verdediging. Medewerkers³ zullen door een verbeterde bewustwording dreigingen onderscheiden en melden. Deze meldingen stellen de gemeente in staat bedreigingen in de kiem te smoren. In het tactisch beleid zal meer uitgewerkt worden rond informatieveiligheid en medewerkers.

² "In onveilige handen" Rekenkamer Rotterdam, 2017

³ Gezien de importantie van de medewerker zal hier nog specifiek aandacht aan worden gegeven in tactisch beleid.



Weerbaarheid

De huidige weerbaarheid van de gemeente geeft een wisselend beeld. De weerbaarheid is afhankelijk van het vaardigheidsniveau van actoren. In het algemeen kan Rotterdam zich goed verdedigen tegen actoren met een lage tot gemiddelde vaardigheid. Voor actoren met een hoog vaardigheidsniveau (bijvoorbeeld vijandige staten) maakt de gemeente gebruik van professionele dienstverleners die beschikking hebben over vergaande kennis over en ervaring met zeer vaardige actoren, aangevuld met geavanceerde technieken en middelen. Denk daarbij aan kennis over de mogelijkheden van inlichtingendiensten om versleuteld dataverkeer te ontcijferen, de financiële middelen van cybercriminelen of de ongekeerde capaciteit van statelijke actoren om gevoelige informatie te verzamelen. Het volledige overzicht van actoren die de gemeente bedreigen staat in bijlage 3. Ook wordt samengewerkt met andere overheden (grote gemeenten, BZK) op het gebied van kennis- en informatiedeling.

Visie

Rotterdam a cybersafe and resilient municipality
Rotterdam een cyberveilige en veerkrachtige gemeente

Met het beveiligen van gevoelige informatie beschermen we de gemeentelijke functies die daarmee worden ondersteund, zoals: privacy van burgers, belangen van bedrijven, vitale maatschappelijke functies (denk aan verkeerssystemen). Het droombeeld is een veilige en veerkrachtige stad. Onze gemeentelijke organisatie maakt onderdeel uit van de stad en heeft een voorbeeldfunctie voor de stad. Het gaat over verantwoord en bewust gedrag van medewerkers, bedrijven en burgers ten aanzien van het werken met informatie.⁴

Missie

Wij bieden een open en betrouwbare omgeving, zodat Rotterdam kan wonen en werken

Risicobewustzijn, kennisuitwisseling en leerprocessen staan centraal in de Rotterdamse initiatieven om de stad digitaal veilig te maken. Binnen de gemeentelijke organisatie werken we samen en nemen onze verantwoordelijkheid in het realiseren van de gemeentelijke missie. We communiceren waar het kan open over veiligheid met elkaar en andere betrokkenen.

De beveiligingsorganisatie hanteert bij het faciliteren van de gemeentelijke organisatie een transparante en betrouwbare werkwijze waarin wordt gekeken en gehandeld vanuit wat mogelijk is, zodat primaire processen optimaal en cyberveilig functioneren vanuit een open en betrouwbare omgeving (open waar het kan en veilig waar noodzakelijk).

⁴ Medewerker = (1) ambtenaar in de zin van het Ambtenarenreglement of (2) degene die op arbeidsovereenkomst of anderszins betaalde of niet-betaalde werkzaamheden voor de gemeente Rotterdam verricht.

Doelstelling Concern informatiebeveiligingsbeleid

Informatie is dé grondstof van onze organisatie, processen, producten en diensten. Verlies, diefstal, of manipulatie van informatie alsook schending van privacy kan ernstige gevolgen hebben voor burgers, bedrijven, ketenpartners en onze eigen organisatie. Informatieveiligheid is essentieel, informatiebeveiliging is het proces dat dit beoogt. Dit strategische concern informatiebeveiligingsbeleid biedt het kader voor passende technische, facilitaire, organisatorische, procesmatige, communicatieve maatregelen (tactisch en operationeel beleid). Communicatieve maatregelen richten we op de bewustwording van medewerkers om gemeentelijke informatie te beschermen. Maatregelen zijn ook gericht op het voldoen aan relevante wet- en regelgeving en uiteraard het op betrouwbare wijze realiseren van de gemeentelijke doelstellingen. Rotterdam stuurt actief op informatiebeveiliging en legt daar op professionele wijze verantwoording over af. Het doel dat de gemeente met dit beleid en het toepassen daarvan wil bereiken, is een verbetering van de informatieveiligheid. Concreet betekent dit:

1. Rotterdam is risicobewust en legt daar rekenschap over af:
Informatieveiligheid is ook: risicobewustzijn en controleerbaarheid.
2. Rotterdam beheerst risico's:
 - We beschermen de stad met haar burgers en bedrijven (een betrouwbare overheid):
 - We beschermen gevoelige informatie en verhogen onze weerbaarheid.
 - Oplossingen hebben altijd een duidelijk organisatie- of stadsbelang.
3. Rotterdam is veerkrachtig en weerbaar:
 - We innoveren en verbeteren op verantwoorde en veilige wijze.
 - We leren van ontwikkelingen in ons dreigingslandschap en van incidenten opdat het volwassenheidsniveau wordt verhoogd.

Gemeente Rotterdam streeft naar het bereiken van volwassenheidsniveau 3 voor haar beveiligingsproces conform de volwassenheidsindeling in 5 niveaus van COBIT. Volwassenheidsniveau 3 staat voor gedocumenteerde beheersing, geformaliseerde en gestructureerde uitvoering waarbij de beheersing aantoonbaar is. Dit geeft invulling aan het op professionele wijze afleggen van verantwoording. Dit draagt er toe bij dat gemeentelijke processen beter beschermd zijn. Dit zal regelmatig worden getoetst door middel van audits (zoals bijvoorbeeld die in het kader van de jaarrekening). Praktische invulling aan de doelstellingen zijn weergegeven in het meerjarenuitvoeringsplan Informatiebeveiliging en de Digitaliseringsagenda. Het Rotterdamse informatiebeveiligingsbeleid is in lijn met het algemene beleid van de gemeente en relevante landelijke en Europese wet- en regelgeving. Het beleid is gebaseerd op de "Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging" (ISO/IEC 27001 en 27002:2013) en de Baseline Informatiebeveiliging Gemeenten (KING, VNG).



Scope

- De scope van dit beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen, informatie en gegevens van de gemeente en externe partijen (bijv. politie), het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.
- Dit concern informatiebeveiligingsbeleid is een algemene basis. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving specifieke (aanvullende) beveiligingseisen.⁵
- Er zijn meerdere domeinen waar informatiebeveiliging overlap mee heeft. Informatiebeveiliging houdt zich bezig met het beveiligen van alle gevoelige gegevens die binnen de gemeente worden gebruikt. Dit maakt dat het domein privacy, waarbij privacygevoelige gegevens worden beschermd overlap heeft met het domein van informatiebeveiliging. Domeinen waar ook overlap mee is, zijn: business continuity, informatiebeheer, compliancy, facilitair en integriteit (gedrag). De beleidsmatige aspecten (wat mag wel en wat mag niet) van privacy, business continuity, informatiebeheer, compliancy, facilitair en integriteit vallen buiten de scope van dit beleid, waar privacy, business continuity, facilitair en integriteit betrekking heeft op de informatiebeveiligingscomponent (hoe beschermen we informatie) valt dit binnen de scope van informatiebeveiligingsbeleid.

Doelgroepen

Het concern informatiebeveiligingsbeleid is bedoeld voor iedereen in en rond de gemeentelijke organisatie:

Doelgroep	Relevantie
College van B&W	Integrale verantwoordelijkheid
Concerndirectie	Kaderstelling
Lijnmanagement (proces eigenaren)	Sturing op informatieveiligheid en controle op naleving
Medewerkers	Gedrag en naleving
Gegevenseigenaren	Classificatie: bepalen van beschermingseisen van informatie
Beleidsmakers	Planvorming binnen informatiebeveiliging kaders
Informatiebeveiliging functionarissen	Dagelijkse coördinatie van informatiebeveiliging
Personeelszaken	Arbeidsvoorwaardelijke zaken
Facilitaire zaken	Fysieke toegangsbeveiliging
ICT diensten (en ontwikkelaars)	Technische beveiliging
Auditors	Onafhankelijke toetsing
Leveranciers en ketenpartners	Compliance

Besluitvorming en vervolg

- Het Rotterdamse concern informatiebeveiligingsbeleid is vastgesteld door het college van B&W.
- Dit informatiebeveiligingsbeleid treedt in werking na vaststelling door college van B&W. Hiermee komt het oude informatiebeveiligingsbeleid (van 2014) te vervallen.
- Het informatiebeveiligingsbeleid wordt jaarlijks herijkt. Dit beantwoordt het snel veranderende omgevingsbeeld en het kat en muis spel van aanval en beveiligen.

⁵ Bijvoorbeeld SUWI (structuur uitvoeringsorganisatie werk en inkomen) en gemeentelijke basisregistraties.

2 Uitgangspunten voor Informatieveiligheid

Inleiding.

In dit beleidskader Informatiebeveiliging sluiten we aan bij strategische principes die de gemeente Rotterdam toepast. Principes zijn algemene uitgangspunten die ten grondslag liggen aan de inrichting van de gemeentelijke organisatie. Ze zijn universeel van toepassing en ze vormen zo de uitgangspunten voor het bestuur, management, het beleid, de inrichting en de werkwijze van de gemeente Rotterdam.

De samenwerking tussen de informatiebeveiligingsorganisatie en bedrijfs- en ICT-architectuur is cruciaal voor het borgen van een betrouwbare en open omgeving binnen de gemeente. Daarnaast stelt wetgeving voor privacy verplicht om "Privacy by design" toe te passen. Dit "Privacy en Security by design" betekent dat vanaf de eerste ontwikkelingen rond het gebruik van (privacy)gevoelige informatie rekening moet worden gehouden met o.a. risico's.

Bij het toepassen van deze strategische principes moet altijd worden gezocht naar een goede balans tussen informatieveiligheid en bijvoorbeeld gebruiksvriendelijkheid. Aangezien niet alle risicovolle situaties te vatten zijn in beveiligingsmaatregelen volgen hier een aantal principes die de grondslag is voor maatregelen die worden getroffen in het kader van het concern informatiebeveiligingsbeleid.

2.1 Strategische principes Informatieveiligheid

1. Gemeente Rotterdam werkt zowel norm als risico gebaseerd.

- a. 100%-veilig bestaat niet. Risico's worden doelbewust en proactief geaccepteerd en beheerst.

Keuzes zijn noodzakelijk (mitigeren, vermijden, overdragen, accepteren), daarom werken we risico gebaseerd. Hierbij wegen we constant voor en nadelen af voor de stad, burger en de organisatie.

- b. We beveiligen niet meer dan noodzakelijk.
We beveiligen zo efficiënt en effectief mogelijk.

- c. Indien de kosten niet opwegen tegen de baten of voordelen wordt een risico geaccepteerd. Echter een onnodig risico wordt niet geaccepteerd.

Informatiebeveiliging kost geld, energie en menskracht. Deze bronnen zijn niet onuitputtelijk en beperkt beschikbaar. Als de kosten voor beveiligingsmaatregelen zo hoog worden dat het niet meer in verhouding staat tot het risico neemt de eigenaar doelbewust een gecalculeerd risico. Als meer investeringen niet leiden tot vermindering van de risico's, is die investering niet effectief. We accepteren dat risico en leggen het ondubbelzinnig vast. Sommige risico's kunnen we door eenvoudige maatregelen zonder veel kosten vermijden. Deze risico's accepteren we niet.

- d. We accepteren risico's als maatregelen te complex zijn.

Door implementatie van vergaande maatregelen om risico's te vermijden, kan er een complexe situatie ontstaan waarmee niet te werken is. Te complexe situaties worden vermeden, omdat anders medewerkers er niet mee kunnen werken en op zoek gaan naar onveilige alternatieven en omdat complexe situaties leiden tot fouten.



- e. We benoemen in de informatiebeveiliging niet alle mogelijke risico's.

Het is ondoenlijk alle mogelijke risico's te inventariseren, te benoemen en maatregelen te treffen. We hebben altijd een onvolledig beeld van het bedreigingslandschap. In eerste instantie hebben we een normen kader op basis van classificatie. Vervolgens wordt via een risicoanalyse gekeken naar eventuele aanvullende risico's of wettelijke eisen. Als we een onbekend risico detecteren, schatten we in of het zich zal herhalen. Alleen indien nodig nemen we maatregelen en voegen het risico toe aan het risico-overzicht.

- f. We zijn geoutilleerd onbekende risico's snel te detecteren en passende maatregelen tijdig te treffen. Aangezien 100% veiligheid niet bestaat is het geen kwestie of de gemeente aangevallen wordt maar wanneer. De veerkracht en flexibiliteit om snel op dit soort aanvallen te reageren is cruciaal in het zijn van een betrouwbare gemeente.

- g. Beslissingen over risico's worden expliciet en op het juiste niveau genomen.

Naarmate de kans op en de impact van een risico groter is, stelt een hoger bestuur of managementlaag deze vast en neemt het passende maatregelen. De beslissing over welke risico's we al dan niet willen lopen, is geen bagatel. Bestuur, directie en lijnmanagement dragen verantwoordelijkheid voor het al dan niet accepteren van risico's en informeren zich actief over aard, omvang en impact van een risico.

2. Gemeente Rotterdam minimaliseert toegang en autorisatie op gevoelige informatie

Het uitgangspunt van gemeente Rotterdam is dat informatie open is tenzij. Zodra de tenzij van kracht is geldt dit principe van het minimaliseren van toegang en autorisatie.

- a. Medewerkers en ICT-componenten krijgen alleen die toegang en bevoegdheden tot informatie, die noodzakelijk is voor het effectief uitvoeren van de rol en de uitvoering van hun werkzaamheden (rolgebaseerde dienstverlening) op de juiste momenten.

Dit principe maakt duidelijk dat informatie waarde heeft en dat we er zorgvuldig mee moeten omgaan. Dit houdt ook in dat we regelmatig en stelselmatig nagaan wie welke informatie vanuit welke rol wanneer mag en kan gebruiken.

- b. Elke rol of functie is altijd tijdelijk.

Door rolwisselingen kan de noodzaak voor toegang tot informatie veranderen. Dit geldt bij primair lijnmanagement voor: vertrek en komst van medewerkers, voor de inhuur van externen en het beëindigen ervan en voor het wijzigen van het takenpakket van een medewerker. Het geldt voor het starten, aantrekken en afstoten van organisatieonderdelen en werken met ketenpartners en systemen waarvan ook andere organisaties dan de gemeente Rotterdam onderdeel uitmaken.

3. Gemeente Rotterdam stuurt proactief op Informatiebeveiliging

- a. Informatiebeveiliging ontwikkelt zich continu en leert van incidenten.

De wereld waartegen we gemeentelijke informatie beschermen is complex en onvoorspelbaar. Het is een wapenwedloop, waarvan het einde niet in zicht is. Informatiebeveiliging is dus nooit af of klaar. We gaan vastberaden door en bezien beveiliging als een continu ontwikkelingsproces van medewerkers, techniek en communicatie zonder vaststaand eindpunt of eindresultaat.



- b. Beveiligingsmaatregelen zijn werkbaar.

Beveiligingsmaatregelen die het dagelijks werk ernstig hinderen, leiden tot een onwerkbaar situatie. Maatregelen werken dan averechts en leiden juist tot meer risico's, omdat medewerkers op zoek gaan naar alternatieven om de uitvoering van het werk makkelijker te maken.

- c. Informatiebeveiliging vereist altijd een bewuste houding van iedereen

Over informatieveiligheid moeten we constant blijven nadenken. We besteden voldoende tijd en aandacht aan informatiebeveiliging, opdat elke medewerker zich bewust is van de risico's, gedragsalternatieven heeft en in voldoende mate ondersteund wordt om aan de richtlijnen te kunnen voldoen.

- d. We maken gebruik van meerdere lagen en strategieën van beveiligingsmaatregelen.

Door de complexe omgeving en de onvoorspelbaar ontwikkelingen hanteren we meerdere lagen en strategieën van beveiligingsmaatregelen. Eén allesomvattende bescherming (de zogenoemde muren van Jericho) waarbinnen alle capaciteit en middelen zijn ondergebracht, is niet meer de oplossing. We moeten er altijd rekening mee houden, dat kwaadwillende zich toegang weten te verschaffen. Gebeurt dit, dan kan door meerdere verdedigingslagen de schade beperkt blijven tot een deel van de informatiehuishouding.

- e. Het meest kostbare bezit wordt het zwaarst bewaakt.

Periodiek stellen we vast wat ons meest kostbare bezit is en passen onze beveiligingsstrategie daarop aan.

2.2 Domeinen

Bovenstaande strategische principes zijn een invulling van de drie domeinen binnen informatiebeveiliging:

BESCHIKBAARHEID: De beschikbaarheid van informatie en IT voldoet aan de gemaakte continuïteitsafspraken. Informatie is toegankelijk en kan gebruikt worden.

INTEGRITEIT: De informatie-eigenaar waarborgt de integriteit van gegevens. Het in overeenstemming laten zijn van informatie met de werkelijkheid en garanderen dat niets ten onrechte is achtergehouden of verdwenen (juistheid, volledigheid en tijdigheid).

VERTROUWELIJKHEID: De informatie-eigenaar verschaft alleen geautoriseerde gebruikers toegang tot gevoelige gegevens. Het beperken van de bevoegdheden en de mogelijkheden tot muteren, kopiëren, toevoegen, vernietigen of kennisnemen van informatie tot een gedefinieerde groep van gerechtigden.

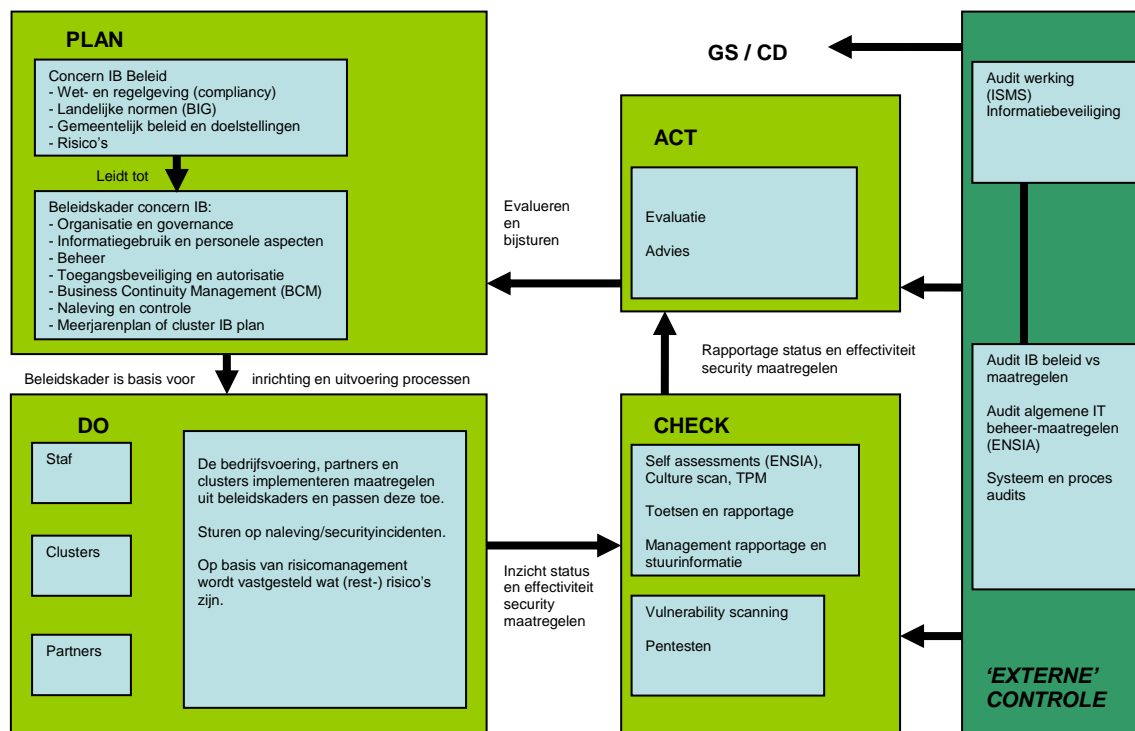
Aansluitende domeinen die impact hebben op informatieveiligheid zijn:

FYSIEKE VEILIGHEID: De verantwoordelijke van het pand of de ruimte verschaft alleen geautoriseerde gebruikerstoegang toegang tot panden of ruimtes waar gevoelige informatie fysiek of digitaal aanwezig is. De verantwoordelijke van het pand of de ruimte neemt maatregelen op basis van risicoafweging tot het beschermen van de aanwezige informatie conform de eisen uit het informatiebeveiligingsbeleid.

BUSINESS CONTINUITY MANAGEMENT: De verantwoordelijke van het primaire proces draagt zorg voor het tijdige herstel van de werking van zijn proces in geval van een onderbreking als gevolg van een incident of calamiteit. Waar het gaat over de continuïteit van informatie worden de maatregelen genomen conform het informatiebeveiligingsbeleid.

3 Continu leren, verbeteren en verantwoorden

Informatiebeveiliging is ingericht als continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging.⁶ Deze kwaliteitscyclus is in onderstaande figuur weergegeven. Deze cyclus is aangesloten op de bestuurlijke P&C cyclus. We werken binnen de gemeente voor informatiebeveiliging met het "three lines of defence" model. Dit wordt verder uitgewerkt binnen het tactische informatiebeveiligingsbeleid.



Toelichting Continu leren, verbeteren en verantwoorden in Rotterdam

- **Plan:** De cyclus start met informatiebeveiligingsbeleid, gebaseerd op wet en regelgeving, landelijke normen en 'good practices', uitgewerkt in regels voor onder meer informatiegebruik, bedrijfscontinuïteit en naleving. Planning geschiedt op jaarlijkse basis en wordt indien nodig tussentijds bijgesteld. Cluster specifieke activiteiten worden gepland in het clusterinformatiebeveiligingsplan of het clusterinformatieplan. Deze planning wordt door de CISO getoetst.
- **Do:** Het beleidskader uit de planfase is de basis voor risicomanagement (tactisch beleidskader), uitvoering van (technische) maatregelen en bevordering van beveiligingsbewustzijn. Uitvoering geschiedt op dagelijkse basis en maakt integraal onderdeel uit van het werkproces.

⁶ ISO/IEC 27001:2013

- Check: Control is onderdeel van het werkproces met als doel: waarborgen van de kwaliteit van informatie en ICT en compliancy aan wet en regelgeving. Dit is een zgn. 2^e lijns control functie (onafhankelijke (rapportage)lijn naar verantwoordelijk management) uitgevoerd door beveiligingsfunctionarissen en/of Interne Controle.
 - Externe controle: betreft controle van buiten het primaire proces door een auditor of extern toezichthouder op zowel het primaire proces zelf, de ICT als het ISMS. Deze controle heeft het karakter van een steekproef en wordt jaarlijks uitgevoerd.
- Act: De cyclus is rond met het opstellen en uitvoeren van verbeteracties o.b.v. check en externe controle. De cyclus is een continu proces; de bevindingen van controles zijn weer input voor de jaarplanning. De bevindingen worden in beginsel gerapporteerd aan de concerndirectie. Na een calamiteit of groot incident wordt geëvalueerd om tot verbeteracties te komen. Voor ingrijpende verbeteracties wordt een gevraagde beslissing voorgelegd.

4 Organisatie van de informatiebeveiliging

Beheer van informatieveiligheid binnen de organisatie.

Rotterdam stuurt actief op informatiebeveiliging en legt op professionele wijze verantwoording af. Gezien het grote overlap met Privacy is samenwerking tussen beider organisaties cruciaal evenals nauw contact tussen de Functionaris gegevensbescherming en de CISO.

4.1 Taken en rollen

Er zijn vier verschillende soorten taken. De kaderstellende taak, de lijnsturingstaak, de ondersteunende taak en de control taak.

De kaderstellende taak:

Het College van B&W stelt het informatiebeveiligingsbeleid formeel vast. De conerndirectie (CD) adviseert B&W formeel over vast te stellen beleid. Directeur IIFO bereidt de kaderstelling voor en de CISO stelt de kaderstelling op

De lijnsturingstaak:

Clusters zijn verantwoordelijk voor risicomanagement, compliancy, continuïteit en sturing op naleving.

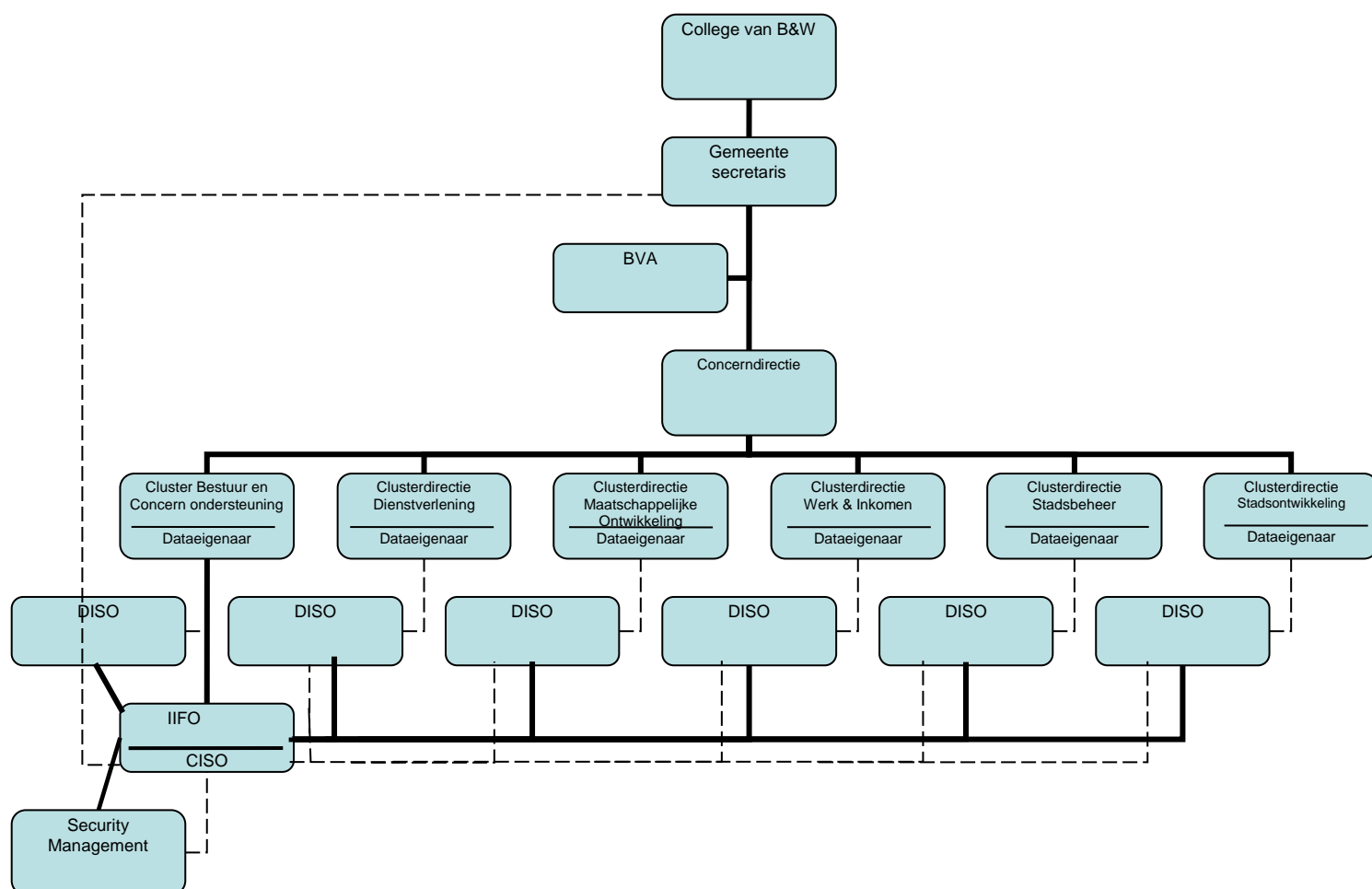
De ondersteunende taak:

BCO/IIFO geeft op dagelijkse basis invulling aan concern ondersteunende taken. De (decentrale) information security officers ondersteunen de clusterdirecties.

De control taak:

Zowel het College als de Raad kan uitvoering van beleid (laten) controleren. Het college legt verantwoording af over informatiebeveiliging aan de Raad. Over het functioneren, wordt jaarlijks gerapporteerd door het cluster conform de P&C cyclus. Naleving van kaders wordt door de CISO getoetst binnen het concern en de DISO's toetsen de naleving van de kaders binnen hun cluster.

Verantwoordelijkheden⁷



De verantwoordelijkheden zijn gekoppeld aan de taken door te categoriseren of de persoon of het orgaan hiërarchisch bij Besturing, Demand of Supply hoort. Deze verantwoordelijkheden hebben een interne werking.

Demand: Iedere medewerker (ambtenaar, inhuur, etc.) van de gemeente heeft de verantwoordelijkheid zich veilig te gedragen waar het gaat om gevoelige informatie binnen de kaders van het informatiebeveiligingsbeleid.

- zet zich actief in om de regels van veilig gedrag zich eigen te maken;
- is zich bewust van zijn of haar invloed op informatieveiligheid in de gemeente;
- meldt (vermoedelijke) beveiligingsincidenten op correcte wijze.

Demand: De informatie/proceseigenaar is verantwoordelijk voor het veilig gebruik van informatie binnen het/zijn proces. Wanneer onderdelen van het proces naar een externe partij of ander cluster(onderdeel) worden overgedragen blijft de eindverantwoordelijkheid voor de bescherming van de informatie altijd van de eigenaar.

- toezien op de kwaliteit van de informatie;
- voorlichting van gebruikers over procedures en afspraken voor veilig gebruik;
- stuurt op uitvoering van maatregelen;
- vaststellen van: te loggen en/of monitoren gebeurtenissen, dataclassificatie, bewaartermijnen, rapportage over naleving, wie toegang krijgt en met welke rechten, functiescheiding, etc.;

⁷ Zie ook: Baseline Informatiebeveiliging Gemeenten, Strategisch normenkader, KING (VNG)



- e. inventarisatie en vastlegging (in overeenkomsten) van beveiligingseisen voortkomend uit wet- en regelgeving;
- f. toezien op registratie;
- g. evaluatie van de informatieclassificatie en effectiviteit van beveiligingsmaatregelen;
- h. afleggen van verantwoording over eigenaarschap aan de clusterdirectie.

Supply: De DISO (decentrale information security officer vanuit BCO gedeconcentreerd bij een cluster) is verantwoordelijk voor het informatiebeveiligingsproces binnen het cluster.

- a. stelt eventuele cluster specifieke kaders op als aanvulling op concernkaders;
- b. rapporteert en legt verantwoording af aan de CISO en de clusterdirectie over de kwaliteit van de werkzaamheden;
- c. zal bij een ernstige inbreuk op de beveiliging van clusterinformatie, of een risico daarop, aanwijzingen geven aan de desbetreffende ambtenaar van zijn cluster teneinde eventuele gevolgen te beperken dan wel een onderzoek laten uitvoeren. Stemt dit af met de CISO.

Supply: De Securitymanager (gepositioneerd bij IIFO) is verantwoordelijk voor het informatiebeveiligingsproces binnen de ICT

- a. stelt ICT specifieke kaders op als invulling van concernkaders;
- b. rapporteert en legt verantwoording af aan de CISO en ICT lijnmanagement over de kwaliteit van de werkzaamheden.
- c. zal bij een ernstige inbreuk op de beveiliging van de infrastructuur, of een risico daarop, aanwijzingen geven aan de desbetreffende ambtenaar van ICT teneinde eventuele gevolgen te beperken dan wel een onderzoek laten uitvoeren.

Demand: De clusterdirecties zijn verantwoordelijk voor de integrale beveiliging van hun organisatieonderdelen.

- a. formuleren op basis van risicoafweging eventueel aanvullende beveiligingseisen;
- b. sturen op beveiligingsbewustwording, gedrag en bedrijfscontinuïteit;
- c. stellen eigenaren aan die toe zien op informatieveiligheid binnen clusterprocessen;
- d. rapporteren over compliancy aan wet en regelgeving en beleid;
- e. hebben een voorbeeldfunctie ten aanzien van het veilig omgaan met informatie.

Supply: De directie van BCO is verantwoordelijk voor ondersteuning.⁸

- a. is verantwoordelijk voor uitvoering van maatregelen op het gebied van HR, juridisch en ICT;
- b. is verantwoordelijk voor ondersteuning van het concern en de concerndirectie;
- c. legt intern verantwoording af;
- d. heeft een voorbeeldfunctie ten aanzien van het veilig omgaan met informatie.

Supply: De CISO (concern information security officer, geplaatst bij IIFO) is verantwoordelijk voor het informatiebeveiligingsproces binnen het concern.

- a. stelt kaders op voor informatiebeveiliging;
- b. vertegenwoordigt de gemeente in externe gremia;
- c. legt verantwoording af aan directeur IIFO, BVA en gemeentesecretaris;
- d. adviseert bestuur op strategisch niveau over informatiebeveiliging;
- e. stuurt de DISO's en Security Managers inhoudelijk aan en coördineert clusteroverstijgende zaken;
- f. zal bij een ernstige inbreuk op de beveiliging van concerninformatie, of een risico daarop, aanwijzingen geven aan de desbetreffende ambtenaar ten einde eventuele gevolgen te beperken dan wel een onderzoek laten uitvoeren.

⁸ Let op, BCO is tegelijk ook clusterdirectie, het gaat hier echter om de uitvoerende rol.



Supply: Directeur IIFO is verantwoordelijk voor voorbereiding van kaderstelling.

- a. bereidt kaderstelling voor;
- b. toetst de naleving van kaders;
- c. geeft gevraagd en ongevraagd advies aan conerndirectie.

Control: Directie Middelen en Control is verantwoordelijk voor concerncontrol wat binnen dit beleid geen aanpassing vraagt.

Besturing: De concerndirectie is verantwoordelijk voor kaderstelling en sturing.

- a. stuurt op concernrisico's en naleving van wet- en regelgeving;
- b. bepaald de totale risicobereidheid van de gemeente;
- c. controleert periodiek de effectiviteit van beleid en maatregelen;
- d. evalueert en stelt waar nodig bij;
- e. heeft een voorbeeldfunctie ten aanzien van het veilig omgaan met informatie.

Besturing: De BVA (beveiligingsambtenaar) is verantwoordelijk voor de integraliteit van beveiliging.

- a. stuurt en heeft toezicht op integraliteit van beveiligingsdomeinen;
- b. bevordert een gezamenlijke aanpak van beveiligingsbelangen.

Besturing: De gemeentesecretaris is portefeuillehouder van informatiebeveiliging⁹ als lid van de conerndirectie.

Besturing: Het college van Burgemeester en Wethouders is integraal verantwoordelijk voor informatiebeveiliging en privacybescherming binnen de werkprocessen van de gemeente.

Besturing: De burgemeester is verantwoordelijk voor sturing bij een zodanig informatiebeveiligingsincident dat er sprake is van verstoring van de openbare orde, ontwrichting van het openbare leven, slachtoffers en/of significante materiele schade.

⁹ Zie Baseline informatiebeveiliging gemeenten, Tactisch normenkader blz. 20.

5 Naleving en compliance

Voorkomen van schending van enige wetgeving, wettelijke en regelgevende of contractuele verplichtingen, en van beveiligingseisen.

5.1 Organisatorische aspecten

- 5.1.1 Het verbeteren van de kwaliteit van informatieveiligheid is een continu proces en onderdeel van alle gemeentelijke processen waarin wordt gewerkt met gevoelige informatie. De kwaliteit wordt gemeten aan:
- a. de mate waarin een volledige set aan maatregelen is geïmplementeerd, gebaseerd op vastgesteld beleid;
 - b. effectiviteit van de geïmplementeerde maatregelen;
 - c. de mate waarin de informatiebeveiliging het bereiken van de strategische doelstellingen ondersteunt.
- 5.1.2 Een belangrijk fundament van naleving is de classificatie van informatie, processen en applicaties. Classificatie maakt het vereiste beschermingsniveau zichtbaar en maakt direct duidelijk welke maatregelen nodig zijn. Er wordt geclassificeerd op drie betrouwbaarheidsaspecten van informatie: beschikbaarheid, integriteit (juistheid, volledigheid) en vertrouwelijkheid. Bij elkaar ook wel afgekort als BIV.
- 5.1.3 IIFO en externe hosting providers leggen verantwoording af aan hun opdrachtgevers over de naleving van het informatiebeveiligingsbeleid. Bij uitbestede (beheer) processen kan een verklaring bij leveranciers worden opgevraagd (TPM of ISAE3402-verklaring).
- 5.1.4 In opdracht van de gemeentesecretaris (gedelegeerd aan de CISO) wordt periodiek de kwaliteit van informatieveiligheid onderzocht door interne IT auditors en door onafhankelijke externen (bijvoorbeeld d.m.v. technische onderzoeken). Jaarlijks wordt een integrale audit uitgevoerd. De bevindingen worden gebruikt voor de verdere verbetering van de informatieveiligheid.
- 5.1.5 In de P&C cyclus wordt gerapporteerd over informatieveiligheid aan de hand van het 'in control' statement. Resultaten uit voorgeschreven ENSIA¹⁰ (audit) wordt als input gebruik voor verantwoording in de P&C cyclus.

¹⁰ ENSIA: Eenduidige Normatiek Single Information Audit - verantwoordingsproces over informatieveiligheid bij gemeenten

5.2 (Wettelijke) kaders

De juridische grondslag van het informatiebeveiligingsbeleid is terug te vinden in wet en regelgeving. Wetten en regelingen die van toepassing zijn (niet limitatief): Wet Openbaarheid van Bestuur (WOB), Algemene Verordening Gegevensbescherming (AVG), Wet Computercriminaliteit II, Comptabiliteitswet, Archiefwet, Wet, Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007), Wet SUWI, Wet meldplicht datalekken, Wet GBA en wet BRP, Richtlijnen van het Nationaal Cyber Security Centrum (NCSC).

- 5.2.1 Naleving van regels vergt steeds meer externe verantwoording, bijvoorbeeld voor gebruik van DigiD¹¹, SUWI¹² en BRP¹³. Aanvullend op dit informatiebeveiligingsbeleid kunnen daarom specifieke regels gelden, bijvoorbeeld op grond van de Archiefwet, de wet BRP of SUWI. Rotterdam sluit aan bij de landelijk ingevoerde ENSIA.
- 5.2.2 Voor elk alle categorieën informatie is de bewaartermijn bepaald in overeenstemming met wet, regelgeving, contractuele verplichtingen en bedrijfsmatige eisen.
- 5.2.3 Bij het (laten) vervaardigen en installeren van programmatuur wordt er voor gezorgd dat de intellectuele eigendomsrechten die daar op rusten niet worden geschonden.

¹¹ DigiD: Naam van het systeem waarmee Nederlandse overheden op internet iemands identiteit verifiëren

¹² SUWI: Wet Structuur Uitvoeringsorganisatie Werk en Inkomen

¹³ BRP: Basisregistratie Personen

Bijlage 1: Onderhavig strategisch kader en andere relevante beleidsdocumenten

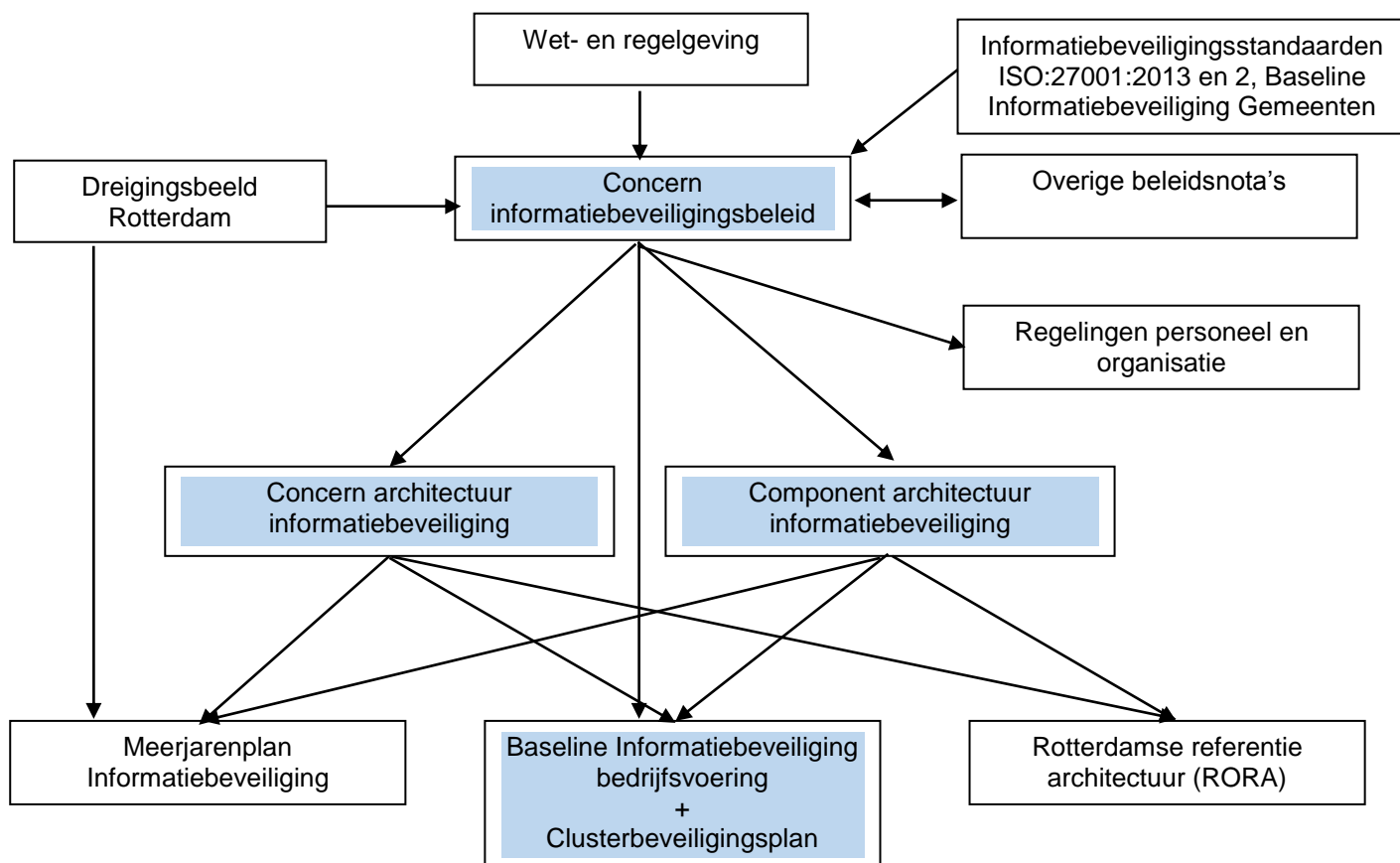
Informatiebeveiliging kaders:

Concern architectuur informatiebeveiliging (concernbrede beveiligingsmaatregelen)
 Component architectuur informatiebeveiliging (beveiligingsmaatregelen per informatieclassificatieniveau)
 Toekomstige specifieke architectuur stukken (Beveiligingsmaatregelen gericht op specifieke domeinen (zoals mobiele apparaten, verantwoordelijkheden van eigenaren, etc.)
 Cluster beveiligingsplan
 Baseline informatiebeveiliging
 Regeling ICT- en informatiegebruik

Overlappende domeinen/beleidsnota's:

Informatiebeheerbeleid
 Gegevensmanagementbeleid
 Facilitairbeleid
 Privacybeleid
 Informatiebeleid
 Gedragcode
 BIP's en CIP
 Toekomstige kaders voor industriesystemen, personele veiligheid, fraude en continuïteit

Hieronder volgt een schematisch overzicht van de verhouding tussen verschillende nota's met de informatiebeveiligingsnota's in het blauw.



Bijlage 2: Relevante documenten en bronnen

Intern

- Informatiebeleid 2014-2018 gemeente Rotterdam, B&W, 2014
- Component Architectuur Concern Informatiebeveiliging, Concerndirectie, 2014
- Regeling ICT en Informatiegebruik, B&W, 2012
- Baseline Informatiebeveiliging, RSO, 2012
- Richtlijn Certificaten, CIO, 2012
- Checklist Cloudcomputing, juridische diensten, 2011
- Procedure aanvragen externe toegang tot Intranet Rotterdam
- Template risicoanalyse

Bovenstaande documenten, inclusief factsheets en rapportages zijn gepubliceerd op:
<https://rio.rotterdam.nl/Project/ConcernInformatiebeveiliging>

Extern

- ISO/IEC 27001 en 27002 (Code voor Informatiebeveiliging), 2013
- Baseline Informatiebeveiliging Gemeenten (BIG), KING, 2015
 - Strategisch normenkader (SNK)
 - Tactisch normenkader (TNK)<https://www.ibdgemeenten.nl/producten/strategische-en-tactische-big/>
- ICT-Beveiligingsrichtlijnen voor Webapplicaties, NCSC, 2015:
<https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html>
- Meldplicht Datalekken:
<https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken>

Bijlage 3: Weerbaarheid

Actor	Relevantie	Weerbaarheid nu	Weerbaarheid ambitie
Staten	Digitale Spionage	Laag	Midden
	Offensieve cybercapaciteiten	Laag	Laag
Terroristen	Verstoring/overname ICT	Laag	Laag
Beroeps-criminelen	Diefstal en publicatie of verkoop van informatie	Laag	Midden
	Manipulatie van informatie	Laag	Laag
	Verstoring ICT *)	Laag	Midden
	Overname ICT	Midden	Midden
Cybervandalen en scriptkiddies	Diefstal informatie	Hoog	Hoog
	Verstoring ICT	Midden	Hoog
	Verkrijging en publicatie van informatie	Midden	Hoog
Cyberonderzoekers	Diefstal en publicatie verkregen informatie	Midden	Midden
Hacktivisten	Defacement	Midden	Midden
	Verstoring ICT	Midden	Hoog
	Overname ICT	Midden	Midden
	Diefstal en publicatie of verkoop verkregen informatie	Laag	Hoog
Interne actoren (bewust)	Verstoring ICT	Laag	Midden
	Verstoring ICT (malware/spam)	Hoog	Hoog
Interne actoren (niet bewust)	Verstoring ICT online diensten	Midden	Hoog
	Onbewust gegevens lekken	Laag	Hoog
Private organisaties	Verkrijging van informatie	Laag	Midden
Geen actor	Uitval ICT	Midden	Midden

Hoog	Maatregelen zijn effectief tegen dit type dreiging/actor
Midden	Maatregelen zijn ten dele effectief tegen dit type dreiging/actor
Laag	Maatregelen zijn niet effectief tegen dit type dreiging/actor

Toelichting

De weerbaarheid ambitie wordt bepaald door (1) het dreigingsniveau en (2) het vaardigheidsniveau van de actor. Maatregelen zullen in beginsel altijd gericht zijn tegen de grootste dreigingen (midden en hoog). Het vaardigheidsniveau van de actor weegt echter mee: kunnen we onszelf wel beschermen? Bijvoorbeeld, China heeft naar schatting 2 miljoen medewerkers in dienst die zich bezig houden met datamining. De middelen zijn welhaast onbeperkt en de gebruikte technieken zeer geavanceerd. Volledige bescherming is met de huidige middelen en technieken simpelweg niet realistisch. Desondanks vereist de wet 'passende technische en organisatorische maatregelen', dat wil zeggen: passend bij de risico's, de kosten om deze te beheersen en de haalbaarheid van technische oplossingen.

Gelet op het dreigingsbeeld zal Rotterdam zich beter moeten weren tegen externe actoren als Cybercriminelen, maar met name ook interne actoren.



Bijlage 4: Verklarende woordenlijst

Autorisatie	Het recht dat een persoon heeft om op informatie een bewerking uit te voeren (bv. aanmaken, opzoeken, wijzigen, doorsturen, weggooien, afdrukken, etc.) met behulp van een informatiesysteem.
Baseline Informatiebeveiliging Gemeenten	Een onder auspiciën van VNG/KING uitgebracht normenkader, waarin op hoofdlijnen beschreven staat op welke manier gemeenten hun informatiebeveiliging inrichten.
Bedrijfscontinuïteit	Een set van maatregelen om na een verstoringen zo spoedig mogelijk de reguliere activiteiten van de organisatie te kunnen hervatten.
Best Practices	Een manier van werken die zich eerder, veelal in andere organisaties, bewezen heeft als succesvol, effectief en efficiënt.
Beveiligingsincident	Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de beschikbaarheid, integriteit of vertrouwelijkheid van informatie of informatiesystemen in gevaar kan komen. Enkele voorbeelden zijn besmettingen met computervirussen, pogingen om toegang te krijgen tot informatiesystemen ('hacken'), verlies van usb-stick waarop gevoelige informatie staat en diefstal van een laptop.
Beveiligingsmaatregelen	Technische, organisatorische of procedurele maatregelen om te voorkomen dat kwetsbaarheden misbruikt worden. Deze kunnen zowel preventief (voorkomen), detectief (ontdekken), repressief (beteugelen) als correctief (herstellen) zijn.
(Beveiligings/Risico) bewustwording	Het proces waarbij men tot besef komt van de beveiligings- c.q. risico-aspecten in de eigen omgeving.
Business continuity	zie Bedrijfscontinuïteit
CISO	Concern Information Security Officer
Classificatie	Het indelen van informatie en informatiesystemen in een beperkt aantal groepen op grond van overeenkomstige eigenschappen. Aan een groep kan vervolgens een set standaard-maatregelen gekoppeld worden.
Cloud	Het via een netwerk (veelal internet) beschikken over schaalbare computercapaciteit (zoals rekenkracht of opslag) of informatiesystemen.
Compliance	Het aantoonbaar voldoen aan relevante wet- en regelgeving.
Cyber	De virtuele wereld van computercommunicatie (in tegenstelling tot de fysieke wereld).
Digitalisering	Digitalisering is de overgang van informatie naar een digitale vorm, zodat die verwerkt kan worden door computers. De term kan betrekking hebben op de gegevens zelf, op de bijbehorende procedures of op de samenleving in het algemeen.
DISO	Decentrale (i.e. per cluster) Information Security Officer
Dreigingslandschap	Het overzicht van mogelijke beveiligingsincidenten en de actoren die hiervoor verantwoordelijk kunnen zijn.
Gevoelige informatie	Informatie die bij onoordeelkundig gebruik schade kan toebrengen aan burgers, bedrijven of de gemeente zelf.
Governance	Het toezicht houden op de naleving en correcte uitvoering van wet- en regelgeving in een organisatie.
Hacken	Oorspronkelijk het gebruiken van technologie op een wijze die niet door de producent bedoeld is (bv. het gebruik van bruisende frisdranken als roestoplosser). Tegenwoordig gebruikt als synoniem voor computercriminaliteit.
Informatiebeheer	Het (langdurig) opslaan, ontsluiten en - indien noodzakelijk - vernietigen van informatie.
Informatiebeveiliging	Informatiebeveiliging is de verzameling processen en technische



	voorzieningen die zorg dragen voor de beschikbaarheid, integriteit en vertrouwelijkheid van informatie binnen de organisatie, met als doel de continuïteit van de informatievoorziening te waarborgen en de gevolgen van beveiligingsincidenten te beperken.
Informatiebeveiligingsbeleid (IB-beleid)	Het beleidsdocument met daarin de verzameling beleidsuitgangspunten over informatiebeveiliging waarmee de organisatie een aantal algemene beleidskeuzes maakt.
Informatieveiligheid	Het beschikbaar hebben van beschikbare, correcte en betrouwbare informatie die in de dienstverlening van de gemeente gebruikt kan worden.
ISO27001	Voluit: "NEN-EN-ISO/IEC 27001:2017 Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging – Eisen". Een internationale, breed geaccepteerde norm, die onder andere voor de "Baseline Informatiebeveiliging Gemeenten" gebruikt is.
ISO27002	Voluit: "NEN-EN-ISO/IEC 27002:2017 Informatietechnologie - Beveiligingstechnieken - Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging". Een internationale, breed geaccepteerde norm, die onder andere voor de "Baseline Informatiebeveiliging Gemeenten" gebruikt is.
Kwetsbaarheid	Een zwakke plek in soft- of hardware, veelal veroorzaakt door een fout in de programmatuur. Een kwetsbaarheid kan misbruikt worden voor een aanval op de informatievoorziening.
Malware	Een overkoepelende term die gebruikt wordt voor software die ongewenste bewerkingen uitvoert, zoals het verzamelen van gevoelige informatie of het blokkeren van toegang tot het betreffende informatiesysteem.
Nationaal Cyber Security Centrum (NCSC)	Het Nationaal Cyber Security Centrum is het centrale informatieknooppunt en expertisecentrum voor cybersecurity in Nederland. De missie van het NCSC is het bijdragen aan het vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein, en daarmee aan een veilige, open en stabiele informatiesamenleving. Het NCSC is het aanspreekpunt op het gebied van ICT-dreigingen en cybersecurity-incidenten binnen de Rijksoverheid.
Privacy by design	Het expliciet aandacht schenken aan het aspect 'Privacy' bij de ontwikkeling van een nieuw product of dienst en de daarbij behorende informatiesystemen.
Risico	De mogelijkheid dat zich een ongewenste situatie voordoet die schade tot gevolg kan hebben.
Rolgebaseerd	Het toekennen van autorisaties gebaseerd op de rol die een persoon binnen de organisatie heeft.
Security by design	Het expliciet aandacht schenken aan het aspect 'Informatiebeveiliging' bij de ontwikkeling van een nieuw product of dienst en de daarbij behorende informatiesystemen.
Weerbaarheid	Het vermogen van een organisatie om zich succesvol te verdedigen tegen een (cyber)aanval.