Rijswijk

# Implementatie Cyberbeveiligingswet

Stand van zaken en vervolg

| | |
|---|---|
| Datum | 6 oktober 2026 |
| Kenmerk (Corsanr) | 26.138663 |
| Opsteller | Peter van de Vaate |
| Versie | 1.0 |

# 1 Inleiding

Op 15 augustus 2026 is de Cyberbeveiligingswet (Cbw) in werking getreden. De Cbw heeft als doel om de maatschappij weerbaarder maken tegen cyberdreigingen en de continuïteit van essentiële dienstverlening te beschermen. Gemeenten zijn essentiële entiteiten in het kader van deze wet. Dat betekent dat de gemeente moet voldoen aan de bepalingen van de Cbw.

Uiteraard beginnen we niet op nul. Zorgen over cyberveiligheid spelen al langer. Om de risico's op dit gebied te beheersen heeft de gemeente in 2011 voor het eerst Informatiebeveiligingsbeleid vastgesteld. Dit beleid is gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO). In 2013 hebben alle gemeenten zich via de Vereniging van Nederlandse Gemeenten geconformeerd aan deze overheidsbrede norm voor informatiebeveiliging. Sindsdien wordt het beleid regelmatig geactualiseerd. Jaarlijks wordt er een informatiebeveiligingsplan opgesteld, waarin de belangrijkste risico's in beeld worden gebracht en waarin acties worden geformuleerd om die risico's te mitigeren.

Ook in de Cbw is de BIO het uitgangspunt voor de organisatie van de informatiebeveiliging voor de overheid. Het belangrijkste verschil is dat de BIO door de inwerkingtreding van de Cbw een verplichtend karakter heeft gekregen. De Rijksinspectie Digitale Infrastructuur (RDI) zal toezicht gaan houden op de naleving van de verplichtingen uit de Cbw. Op grond van de Cbw kan de RDI naleving van de wettelijke bepalingen afdwingen door het opleggen van een last onder dwang of door een boete op te leggen.

De belangrijkste bepalingen uit de Cbw waar de gemeente aan moet voldoen zijn:

- De zorgplicht
- De meldplicht
- De registratieplicht
- De opleidingsplicht

In het vervolg van dit document zal worden uitgelegd wat onder deze verplichtingen wordt verstaan en hoe we daar in Rijswijk gevolg aan (gaan) geven.

# 2 De Zorgplicht

De zorgplicht is de verplichting om passende en evenredige technische, operationele en organisatorische maatregelen te nemen om de netwerk- en informatiesystemen van de gemeente te beveiligen. Het doel is om proactief risico's te beheersen, cyberincidenten te voorkomen en de continuïteit van de dienstverlening te waarborgen.

De Cbw kent 10 zorgplichtmaatregelen:

1. Maak een risicoanalyse
2. Versterk de beveiliging op het gebied van personeel, toegang en assetbeheer
3. Maak een Bedrijfscontinuïteitsplan (BCP)
4. Richt Incident Response in
5. Zorg dat cyberhygiëne op orde is
6. Schrijf beleid op de beveiliging van netwerk- en informatiesystemen
7. Maak je toeleveringsketen veilig
8. Maak beleid op cryptografie en encryptie
9. Gebruik MFA of andere beveiligde authenticatieoplossingen
10. Hanteer processen om de effectiviteit van maatregelen te beoordelen

In de volgende paragrafen van dit hoofdstuk zal elk van deze 10 maatregelen afzonderlijk worden toegelicht. Daarin zal ook worden aangegeven op welke manier de maatregel in Rijswijk vorm is gegeven of welke acties nog nodig zijn voor de uitvoering van de maatregel.

## 2.1 Maak een risicoanalyse

Het maken van een risicoanalyse is de eerste stap in het verbeteren van de cyberweerbaarheid van de gemeente. Het geeft inzicht in welke risico's het zwaarst wegen en waar maatregelen het hardst nodig zijn. Het Nationaal Cybersecurity Center (NCSC) adviseert daarom om met een risicoanalyse te beginnen.

De gemeente Rijswijk heeft hier gevolg aan gegeven door het uitvoeren van een risicoanalyse NIS2. De NIS2 is de Europese richtlijn die in de Cbw is uitgewerkt in nationale wetgeving. In deze een analyse is bepaald welke processen en systemen binnen de scope van de wet vallen. Dit zijn de processen waarop de maatregelen uit de BIO van toepassing zijn. In het tweede deel van de inventarisatie is per systeem gekeken welke maatregelen zijn ingevoerd en welke nog niet (helemaal).

De managers die verantwoordelijk zijn voor de betreffende systemen hebben op die manier inzicht gekregen waar de grootste risico's liggen. Zij zijn ervoor verantwoordelijk dat ontbrekende maatregelen alsnog worden uitgevoerd om die risico's tot een aanvaardbaar niveau terug te brengen.

Door deze analyse jaarlijks te herhalen blijft het inzicht in de risico's actueel.

Naast deze specifieke risicoanalyse wordt jaarlijks in het kader van de zelfevaluatie ENSIA gekeken naar de uitvoering van de generieke beveiligingsmaatregelen. Voor maatregelen die volgens die analyse onvoldoende of niet worden uitgevoerd worden acties opgenomen in het informatiebeveiligingsplan.

De uitvoering van het risicomanagement langs deze lijn is beschreven in het nieuwe informatiebeveiligingsbeleid.

### 2.2 Versterk de beveiliging op het gebied van personeel, toegang en assetbeheer

Deze maatregel heeft als doel inzicht te krijgen in de informatiesystemen die de gemeente gebruikt en wie daar gebruik van mogen maken. Daarvoor moet beleid worden opgesteld hoe je medewerkers toegang verleent tot systemen en informatie. De gemeente moet een actuele inventaris bijhouden van de relevante IT-middelen en er moet een screeningsbeleid zijn voor het personeel.

In 2025 is het logisch toegangsbeleid voor de gemeente Rijswijk vastgesteld. Hierin is beschreven hoe de toegangsprocedures voor informatiesystemen ingericht moeten zijn. Inclusief de periodieke controle van de gebruikers van die systemen.

De inventaris van alle informatiesystemen is opgenomen in TopDesk. Dit fungeert als de CMDB (configuration management database) van de gemeente Rijswijk. Hierin wordt ook de inventaris van de IT-hardware bijgehouden.

De gemeente Rijswijk vraagt van alle medewerkers een VOG. In 2021 is nader uitgewerkt hoe hiermee wordt omgegaan bij interne doorstroom naar risicovolle functies.

### 2.3 Maak een Bedrijfscontinuïteitsplan (BCP)

Ondanks alle maatregelen die je treft kan (langdurige) uitval altijd gebeuren. De gemeente dient zich daarom voor te bereiden om de organisatie in dat soort situaties zo snel mogelijk weer te kunnen herstellen.

Voor het opstellen van continuïteitsplannen voor de kritische processen is al jaren een actie geformuleerd in het informatiebeveiligingsplan. Daardoor zijn er nu voor 10 processen min of meer uitgewerkte continuïteitsplannen. De variatie in volwassenheid van deze plannen is groot.

Uit de risicoanalyse NIS2 blijkt bovendien dat daarnaast voor 16 applicaties behoefte bestaat aan de uitwerking van een continuïteitsplan.

De aandacht voor de ontwikkeling van bedrijfscontinuïteitsmanagement wordt breder in de organisatie geuit. Vanuit het project Maatschappelijk weerbaarheid wordt aangedrongen op een professionalisering door het aanstellen van een bedrijfscontinuïteitsmanager. Zij benadrukken dat de organisatie goed voorbereid moet zijn op mogelijke verstoringen en dat tijdens rampen en crisisscenario's de maatschappelijke functies aangepast overeind blijven. Dit vraagt om het actualiseren en borgen van continuïteitsplannen voor kritische processen en om een overkoepelend beeld met een helder prioriteringskader. Om dit duurzaam te organiseren is het noodzakelijk dat er duidelijke regie wordt belegd en een stevige aanjagersrol wordt vervuld binnen de organisatie. Vanuit dat project wordt dat in een voorstel uitgewerkt.

De aanstelling van een bedrijfscontinuïteitsmanager zal zeker bijdragen aan de ontwikkeling van continuïteitsplannen voor de kritieke applicaties in het kader van de Cyberbeveiligingswet.

### 2.4 Richt Incident Response in

De gevolgen van verstoringen, uitval, datalekken of cyberaanvallen kunnen ernstig zijn. Daarom is het cruciaal om bij een incident adequaat te reageren om negatieve gevolgen te beperken. Een Incident Response Plan (IRP) helpt daarbij.

| |
|---|
| Het IT-beheer van de gemeente Rijswijk wordt verzorgd door de gemeenschappelijke regeling bedrijfsvoering Rijswijk-Delft (GRB). De GRB heeft een Cybersecurity incidentresponse plan opgesteld. In aansluiting op dat plan heeft de gemeente Rijswijk een proceskaart kritieke informatiebeveiligingsincidenten vastgesteld. De samenhang tussen deze processen is beschreven in het proces voor incidentmanagement. |

## 2.5 Zorg dat cyberhygiëne op orde is

Met een goede cyberhygiëne hanteert de gehele organisatie de basisprincipes van cyberveiligheid. Dit kan door medewerkers bewust te maken van risico's, ze te trainen in het omgaan met incidenten en een cultuur te creëren waarin mensen veilig melding kunnen maken als er onverhoopt iets misgaat. Technische oplossingen kunnen hierbij helpen. Denk aan spamfilters om phishing te herkennen, inloggen in 2 stappen of het gebruik van wachtwoordmanagers.

Alle nieuwe medewerkers van de gemeente Rijswijk zijn verplicht om een basistraining iBewust te volgen. De training bestaat uit twee onderdelen:

1. De AVG (Algemene verordening gegevensbescherming)
2. Informatiebeveiliging

In de training wordt de privacywetgeving uitgelegd. Zodat medewerkers het belang ervan kennen en weten waaraan ze moeten denken om bij de uitvoering van hun werkzaamheden de rechten van de burgers te borgen. In het onderdeel Informatiebeveiliging leren medewerkers de belangrijkste risico's op dit gebied kennen, en wordt uitgelegd hoe ze die risico's kunnen verkleinen.

Er is een speciale pagina op intranet waarop de medewerkers alle informatie over informatiebeveiliging (en de bescherming van persoonsgegevens) kunnen terugvinden. Op deze pagina worden ook berichten gedeeld met de medewerkers over nieuwe dreigingen en nieuwe maatregelen.

Op incidentele basis wordt er een test uitgevoerd (bijvoorbeeld in de vorm van een phishingsimulatie) om de bewustwording van de medewerkers te vergroten.

Een belangrijke rol bij het creëren van bewustwording en het handhaven van cyberhygiëne is weggelegd voor de managers. Door de ciso worden zij aangespoord dit onderwerp te agenderen in hun gesprekken met medewerkers en op werkoverleggen.

Geconcludeerd kan worden dat er voldoende aandacht is voor bewustwording maar dat een gestructureerde aanpak ontbreekt om de kennis die nieuwe medewerkers bij de verplichte training hebben opgedaan over de naleving van de AVG en informatiebeveiliging op peil te houden.

Om die structurele aanpak te borgen zal een team worden gevormd dat een opleidingsplan en communicatieagenda opstelt en gaat toezien op de uitvoering daarvan.

De technische onderdelen die bijdragen aan de cyberhygiëne hangen samen met de uitvoering van de maatregelen uit de BIO. Dit krijgt voldoende aandacht in de jaarlijkse verantwoordingscyclus (zie ook *2.1 Maak een risicoanalyse* en *2.6 Schrijf beleid op de beveiliging van netwerk- en informatiesystemen*).

## 2.6 Schrijf beleid op de beveiliging van netwerk- en informatiesystemen

De gemeente is afhankelijk van netwerk- en informatiesystemen voor de uitvoering van primaire bedrijfsprocessen. Als je geen toegang hebt tot deze systemen of als informatie openbaar wordt, kan dit grote gevolgen hebben voor de organisatie. De gemeente dient te beschrijven hoe ze deze netwerk- en informatiesystemen beveiligd.

De gemeente heeft Informatiebeveiligingsbeleid opgesteld. Hierin wordt op strategisch niveau beschreven op welke manier de gemeente de informatiebeveiliging organiseert. Dit beleid wordt regelmatig geactualiseerd. Belangrijkste uitgangspunt in dit beleid is dat de gemeente zich conformeert aan de BIO.

Het strategisch beleid is conform de BIO uitgewerkt in beleid op tactisch niveau en op operationeel niveau in richtlijnen, procedures, procesbeschrijvingen en werkinstructies. Voor een deel ligt dit vast in het tactisch beleid van de GRB. Voorbeelden hiervan zijn het logisch toegangsbeleid, het inkoopbeleid (Gibit), het Protocol Informatieveiligheid bij hybride werken, de wijzigingsprocedure, het incidentresponseplan, de specifieke instructies in Topdesk. In de jaarlijkse verantwoordingscyclus (die ook beschreven staat in het Informatiebeveiligingsbeleid) wordt beoordeeld of in voldoende mate gevolg wordt gegeven aan de beleidsvorming. Voor onderdelen die onvoldoende scoren wordt een actie geformuleerd in het jaarlijkse Informatiebeveiligingsplan.

## 2.7 Maak je toeleveringsketen veilig

De gemeente is afhankelijk van de producten of diensten van toeleveranciers. Dit houdt ook in dat je afhankelijk bent van de digitale weerbaarheid van je toeleveranciers, zelfs als je eigen digitale weerbaarheid op orde is. Digitale verbindingen tussen bedrijven vergroten deze afhankelijkheid. Daarom is het van belang maatregelen te nemen om de toeleveringsketen te beveiligen.

De gemeente kiest ervoor om steeds meer applicaties als cloudservice af te nemen (software as a service, SAAS). De software wordt dan niet aangeschaft en op de apparatuur van de gemeente geïnstalleerd. In plaats daarvan wordt met de leverancier een contract afgesloten voor het gebruik van de software op een door de leverancier beheerde locatie. Het gebruik van dit soort applicaties is aan een aantal randvoorwaarden gebonden. De belangrijkste daarvan is dat de beveiliging op orde is conform de BIO. De gemeente mag er dan vanuit gaan dat de leverancier voldoende maatregelen heeft getroffen op gebieden zoals de toegangsvoorziening en het kwetsbaarhedenbeheer. Om te toetsen of de organisatie en leverancier gereed zijn, is de Cloud Readiness Checklist opgesteld. Het gebruik van de checklist is opgenomen in de richtinggevende principes van het informatiebeveiligingsbeleid.

Bij aanbestedingen voor nieuwe informatiesystemen worden standaard informatiebeveiligingseisen gesteld. Uitgangspunt daarbij is dat de leverancier informatiebeveiligingsbeleid heeft vastgesteld op basis van de ISO27001.

Door de komst van de AVG is de verwerkersovereenkomst een verplicht onderdeel geworden van contracten met SAAS-leveranciers als er persoonsgegevens in het spel zijn. Als onderdeel van die overeenkomst dient de leverancier aan te tonen hoe ze zorgen voor een passende beveiliging. Met de invoering van de Cyberbeveiligingswet wordt dat verder aangescherpt. Leveranciers dienen nu jaarlijks aan te tonen dat aan de gestelde eisen wordt voldaan.

Dat vraagt wat van de inrichting van het contractmanagement en leveranciersmanagement bij de gemeente. Uit de risicoanalyse NIS2 blijkt dat dit nog niet bij alle applicaties op orde is. Vanuit het domein Bedrijfsvoering loopt er een initiatief om IT-contracten voor alle domeinen centraal te gaan registreren en beheren. Daarnaast is er bij ieder domein een kwartiermaker actief, die ervoor moet zorgen dat er binnen het domein een proces wordt ingericht waarin de verantwoordelijkheid voor het contractmanagement is vastgelegd.

De Vereniging Nederlandse Gemeenten (VNG) werkt aan een standaard voorziening om de jaarlijkse uitvraag richting leveranciers te centraliseren. Een dergelijke voorziening gaat de gemeente helpen om de jaarlijkse beoordeling van de naleving van de beveiligingseisen door leveranciers efficiënter te organiseren. Uiteraard wordt die ontwikkeling op de voet gevolgd.

### 2.8 Maak beleid op cryptografie en encryptie

Cryptografie en encryptie vormen de basis voor de vertrouwelijkheid en integriteit van informatie. De gemeente dient de maatregelen te beschrijven die worden genomen om de vertrouwelijkheid en integriteit van informatie op deze wijze te beschermen.

| |
|---|
| Cryptografie wordt op veel plekken door de gemeente toegepast. Denk aan de versleuteling van de berichten die via internet worden verstuurd. Bij aanbestedingen van nieuwe informatiesystemen worden door de gemeente eisen gesteld aan de versleutelde opslag en verzending van informatie. Een overkoepelend beleidsdocument ontbreekt nog. In het laatste informatiebeveiligingsplan is het opstellen daarvan als actie geformuleerd.<br><br>Het IT-beheer van de gemeente wordt uitgevoerd door de GRB. Een belangrijk deel van de cryptografische maatregelen wordt binnen de GRB genomen. Het beleid van de gemeente Rijswijk moet daarop aansluiten. Op dit moment wordt het cryptografiebeleid van de GRB geactualiseerd. Zodra de conceptversie daarvan is opgeleverd, zal dat in Rijswijk worden gebruikt om daarop aanvullend het gemeentelijk cryptografiebeleid te formuleren. |

### 2.9 Gebruik MFA of andere beveiligde authenticatieoplossingen

Om de toegang tot informatie te beschermen is het gebruik van een wachtwoord alleen allang niet meer veilig genoeg tegen moderne cyberaanvallen. Door het toepassen van MFA (multi-factor authenticatie) voeg je een extra beveiligingslaag toe.

| |
|---|
| In het logisch toegangsbeleid van de gemeente is het gebruik van MFA verplicht gesteld. Bij aanbestedingen van nieuwe informatiesystemen is dat al langer als eis opgenomen. De beveiligde authenticatie is ook onderdeel van de BIO. De beoordeling van de toepassing daarvan is op die manier onderdeel van de jaarlijkse verantwoordingscyclus. |

## 2.10 Hanteer processen om de effectiviteit van maatregelen te beoordelen

Het beoordelen van de effectiviteit van cyberveiligheidsmaatregelen helpt om risico's te beheren, zorgt voor naleving van wetten en identificeert verbeterpunten.

De jaarlijkse verantwoordingscyclus is momenteel gericht op de aanwezigheid van beveiligingsmaatregelen. De effectiviteit van die maatregelen speelt bij de jaarlijkse beoordeling geen expliciete rol.

Om daar verandering in aan te brengen wordt nu onderzocht hoe de beoordeling van de effectiviteit van beveiligingsmaatregelen een vast onderdeel kan worden van de testprocedure. Gezocht wordt naar een manier om nieuwe informatiesystemen en nieuwe versies daarvan standaard te testen op bekende kwetsbaarheden.

De beveiliging van DigiD-systemen wordt ieder jaar al uitgebreid getest. Daarnaast wordt er door de GRB ieder jaar opdracht gegeven voor een penetratietest op een specifiek onderdeel van de IT-infrastructuur.

In het kader van de Cbw zijn leveranciers verplicht om jaarlijks aan te tonen dat ze aan de gestelde eisen voldoen in opzet, bestaan en werking. Ze moeten daarbij gebruik maken van onafhankelijke derden.  Het toezicht op de naleving daarvan door de leveranciers wordt op dit moment ingericht in Rijswijk (zie *2.7 Maak je toeleveringsketen veilig*).

De beoordeling van de effectiviteit van beveiligingsmaatregelen is ook onderdeel van de evaluatie van beveiligingsincidenten.

# 3 De Meldplicht

De meldplicht betekent dat organisaties significante incidenten moeten melden bij het centrale meldpunt. Voor de gemeente is dat het NCSC (Nationaal Cybersecurity Center).

Wat moet je melden?

De meldplicht geldt voor significante incidenten. Dat zijn incidenten die de dienstverlening ernstig verstoren, financiële schade veroorzaken of grote schade bij andere organisaties kunnen aanrichten.

De meldplicht bestaat uit verschillende meldmomenten:

- Vroegtijdige waarschuwing: binnen 24 uur nadat de organisatie kennis heeft genomen van een significant incident.
- Incidentmelding; binnen 72 uur na kennisname van het incident. Deze melding bevat een eerste beoordeling van het incident, waaronder de ernst en impact.
- Eindverslag: uiterlijk één maand na incidentmelding. Hierin wordt onder meer ingegaan op het incident, de oorzaak, de gevolgen en de genomen en lopende herstelmaatregelen.

Na een melding kan het NCSC ondersteuning bieden bij de afhandeling van het incident. Deze ondersteuning kan bijvoorbeeld bestaan uit:

- Advies over het beperken van de gevolgen van een incident.
- Ondersteuning bij herstel
- Informatie over dreigingen, kwetsbaarheden en aanvalsmethoden
- Het delen van relevante kennis en expertise.

De meldplicht draagt daarmee niet alleen bij aan het toezicht en het inzicht in incidenten, maar zorgt er ook voor dat organisaties ondersteuning kunnen krijgen bij de afhandeling van een incident.

| |
|---|
| Het maken van een melding bij het NCSC is onderdeel van het proces voor incidentmanagement van de gemeente Rijswijk. |

# 4 De Registratieplicht

Organisaties die onder de Cyberbeveiligingswet vallen, moeten zich registreren in het landelijke entiteitenregister. In Nederland gebeurt dat bij het Nationaal Cyber Security Centrum (NCSC). Na registratie kunnen organisaties gebruikmaken van de dienstverlening van het CSIRT dat voor hun sector is aangewezen. Voor de gemeente is dat het NCSC.

| |
|---|
| De gemeente Rijswijk is op 6 maart 2026 geregistreerd in het entiteitenregister. De ciso en de manager Informatie zijn als contactpersoon opgegeven. |

# 5 De Opleidingsplicht

Onder de Cyberbeveiligingswet is cyberbeveiliging nadrukkelijk een verantwoordelijkheid van het bestuur. Het bestuur moet de maatregelen voor het beheersen van de cyberbeveiligingsrisico's goedkeuren en toezien op de uitvoering daarvan.

Bestuurders moeten voldoende kennis en vaardigheden hebben om cyberbeveiligingsrisico's en de gevolgen daarvan voor de organisatie te kunnen begrijpen en beoordelen. Hiervoor moeten zij een training volgen.

De training behandelt onder meer:

- risico's voor de beveiliging van netwerk- en informatiesystemen;
- mogelijke gevolgen van deze risico's voor de organisatie;
- het identificeren en beheersen van cyberbeveiligingsrisico's;
- maatregelen om deze risico's te beheersen;
- de kennis en vaardigheden die nodig zijn om risico's en maatregelen te beoordelen en hierover op bestuurlijk niveau afgewogen besluiten te nemen.

Bestuurders moeten uiterlijk twee jaar na inwerkingtreding van de Cyberbeveiligingswet over de vereiste kennis en vaardigheden beschikken en deze vervolgens aantoonbaar actueel houden.

**Certificaat**

Na het volgen van de training ontvangt de bestuurder een certificaat. Daarop staat dat de training is gevolgd en welke onderwerpen zijn behandeld. De eisen aan de training zijn vastgelegd in het Cyberbeveiligingsbesluit.

De Rijksoverheid schrijft geen specifieke training of opleidingsaanbieder voor. Organisaties kunnen gebruikmaken van een externe aanbieder, maar kunnen de training ook zelf organiseren, bijvoorbeeld met ondersteuning van een CISO, zolang de training aan de wettelijke eisen voldoet.

Op dit moment zijn het Rijk en de verschillende bestuurslagen bezig met het vormgeven van de gewenste inhoud voor deze training.

Op dit moment zijn er in Rijswijk nog geen concrete plannen voor de opleiding van de bestuurders. Het lijkt raadzaam om de ontwikkelingen die op dit gebied gaande zijn binnen het Rijk en de VNG af te wachten.

Het streven is om de training aan het bestuur in de loop van 2027 te organiseren. Hier zal in overleg met de verantwoordelijke portefeuillehouder (de wethouder Bedrijfsvoering) een voorstel voor worden uitgewerkt.

# 6 Samenvatting en conclusie

Op 15 augustus 2026 is de Cyberbeveiligingswet (Cbw) in werking getreden. Uit de Cbw volgen een viertal verplichtingen waar de gemeente aan moet voldoen:

- De zorgplicht
- De meldplicht
- De registratieplicht
- De opleidingsplicht

De Cyberbeveiligingswet is in grote lijnen een voortzetting van het al jaren geleden ingezette informatiebeveiligingsbeleid in Rijswijk. De gemeente voldoet daardoor op veel punten al aan de verplichtingen uit de Cbw.

Bij de zorgplicht zijn er aandachtspunten bij:

- Het opstellen van een Bedrijfscontinuïteitsplan
  Bij de kritieke applicaties(/processen) zijn bedrijfscontinuïteitsplannen opgesteld. De noodzaak van professionalisering en coördinatie op dit onderwerp wordt gevoeld. Om die ontwikkeling op gang te brengen wordt gepleit voor het aanstellen van een bedrijfscontinuïteitsmanager. Vanuit het project Maatschappelijke Weerbaarheid wordt dat in een voorstel uitgewerkt.
- Het op orde brengen van de cyberhygiëne
  Er worden in Rijswijk verschillende activiteiten ontplooit om de cyberhygiëne op orde te brengen. Om de continuïteit van die activiteiten beter te borgen en om meer samenhang aan te brengen tussen die activiteiten wordt voorgesteld om een team samen te stellen dat een opleidingsplan en communicatieagenda gaat opstellen en gaat toezien op de uitvoering daarvan.
- De toeleveringsketen veilig maken
  Het toezicht op de naleving van de informatiebeveiligingseisen aan de leveranciers wordt onder de Cbw strikter geregeld. De gemeente zal hier een aantal aanpassingen voor moeten doen in de organisatie van het contract- en leveranciersmanagement. Die veranderingen zijn in gang gezet. In de jaarlijkse verantwoordingscyclus zal worden beoordeeld of dat volstaat of dat hier extra inzet op nodig is.
- Opstellen Cryptografiebeleid
  Een overkoepelend beleidsdocument ontbreekt nog. Dit beleid zal in samenspraak met de GRB geformuleerd moeten worden. In het laatste informatiebeveiligingsplan is dit als actie opgenomen.

Op de onderdelen Meldplicht en Registratieplicht handelt de gemeente volledig volgens de Cbw.

De gemeente voldoet nog niet aan de Opleidingsplicht voor bestuurders. Door het Rijk en de VNG wordt op dit moment gewerkt aan een trainingsaanbod. Het streven is om in de loop van 2027 een training te organiseren voor het bestuur. Hiervoor zal de ciso in overleg met de wethouder Bedrijfsvoering een voorstel opstellen.

De bevindingen en aanbevelingen uit deze notitie krijgen met ingang van 2027 een plek in het jaarlijkse informatiebeveiligingsplan.