Risico-inventarisatie en evaluatie Informatiebeveiliging BRP & Waardedocumenten

Versie : 1.0

Status : definitief

Auteur : de heer H. Timmerman

Datum : 23 januari 2016

BMC

Inhoudsopgave

1 RISICO ANALYSE 4

1.1 INLEIDING 4
1.2 HET HOE EN WAAROM VAN EEN RISICO ANALYSE 5
1.3 WAARSCHIJNLIJKHEID EN EFFECT 6
1.4 PRIORITEITSTELLING 7
1.5 ANALYSE MATRIX 9
1.6 TOELICHTING OP DE ANALYSE 21

2 BIJLAGEN 23

2.1 BIJLAGE 1 KENMERKEN COMPUTERRUIMTE 23
2.2 BIJLAGE 2 KENMERKEN FYSIEKE BEVEILIGING 24
2.3 BIJLAGE 3 KENMERKEN BRP SYSTEEM 25
2.4 BIJLAGE 4 KENMERKEN BRP APPLICATIE 26
2.5 BIJLAGE 5 KENMERKEN GEMEENTELIJK LAN 26

1 Risico analyse

1.1 Inleiding

Het optreden van een gebeurtenis welke, bij het ontbreken van passende maatregelen, duidelijk waarneembare gevolgen (materieel dan wel immaterieel) voor de organisatie heeft, noemen we een calamiteit. Calamiteiten zijn niet uit te sluiten daar het niet mogelijk is om voor alle mogelijk gebeurtenissen beheersmaatregelen te treffen. Daarnaast dient in ogenschouw te worden genomen dat beheersmaatregelen tijd en geld kosten zowel bij de opzet als in het onderhoud. Het is dus van belang om een goede analyse te maken van de calamiteiten die in de organisatie kunnen optreden om zodoende de juiste maatregelen te kunnen treffen.

Risico's zijn altijd gerelateerd aan de doelstelling van de organisatie. Daar veel diensten en producten afhankelijk zijn van de informatievoorziening is het van belang om een goede analyse te maken.
De risico's die een organisatie loopt ten aanzien van de informatiebeveiliging zijn in veel gevallen gelijk.
De onderstaande risico's kunnen worden onderkend:

- De klant[1] krijgt geen informatie;
- De klant krijgt niet tijdig de gewenste informatie;
- De klant krijgt verkeerde informatie;
- De klant krijgt onvolledige informatie;
- Vertrouwelijke informatie komt in verkeerde handen.

Hoewel voor elke organisatie verschillend, is het toch mogelijk een aantal gevolgen van een calamiteit te noemen:

- Vitale informatie gaat verloren;
- Controle is niet meer mogelijk;
- Informatie is niet meer beschikbaar;
- Goederen en diensten kunnen niet geleverd worden;
- Demotivatie bij medewerkers;
- Chaos;
- Fraude;
- Vertrouwelijke informatie lekt uit.

[1] Met klant bedoelen we zowel de interne als de externe klant.

1.2 Het hoe en waarom van een risico analyse

Voordat de uitgangspunten waaraan de informatiebeveiliging moet voldoen bepaald worden, wordt een risico analyse inclusief een gevolgschade onderzoek uitgevoerd om de risico's voor de bedrijfsprocessen te analyseren. Later kunnen dan voor de kritieke bedrijfsprocessen de kans van optreden (waarschijnlijkheid) of de mogelijke schade (het effect) worden weggenomen of beperkt. Wordt deze analyse overgeslagen dan worden maatregelen gekozen welke wellicht het beoogde doel niet waarborgen.

Een *risico analyse* kan op een aantal manieren plaatsvinden. Een veel gebruikte manier is *de kwantitatieve methode* waarbij de risico's voor het optreden van alle onderkende bedreigingen/calamiteiten (dit wordt ook het manifest worden van bedreigingen genoemd) voor de organisatie bepaald worden

Bij een *gevolgschade onderzoek* (dat aan de hand van de risico analyse uitgevoerd kan worden) wordt de materiële (en wellicht ook de immateriële) schade die optreedt bij het manifest van een calamiteit per gebeurtenis gekwantificeerd en daarna gesommeerd. De totale schadeverwachting per jaar geeft het management team gereedschap in handen om de kosten van voorzieningen te relateren aan de te vermijden risico's.

In de laatste jaren komt de kwalitatieve methode meer in zwang. Hierbij worden risico's niet meer in cijfers achter de komma bepaald maar worden klassen samengesteld en kan het management team vervolgens een keuze te maken ten aanzien van welke risico's men wil kunnen overleven.
Deze methode levert meer 'tastbare' handvatten. Het management team ziet hierdoor in een oogopslag welke processen de hoogste prioriteit dienen te krijgen. De kwalitatieve methode wordt in het voorliggend Informatiebeveiligingsplan toegepast.

1.3 Waarschijnlijkheid en effect

Om de beveiliging verder te verbeteren, moet een risico analyse worden uitgevoerd. Er dient eerst bewustwording te zijn voordat men adequate maatregelen kan treffen.

Er zijn een aantal generieke bedreigingen die kunnen worden onderscheiden ten aanzien van de informatiebeveiliging. Deze kunnen worden onderverdeeld in 3 hoofdgroepen:

- Fysieke bedreigingen;
- Personele bedreigingen;
- ICT technische bedreigingen.

In de analysematrix (1.5) wordt gebruik gemaakt van bedreigingen per kwaliteitsaspect (data-integriteit, beschikbaarheid, vertrouwelijkheid en controleerbaarheid) van de informatiebeveiliging. Sommige bedreigingen hebben betrekking op meer dan één aspect en in die gevallen is de bedreiging ondergebracht in de meest logische categorie.

Niet alle bedreigingen zijn even groot. Om toch een inschatting te maken van de ernst van de risico's worden twee factoren ingevoerd waarmee de risico's ten opzichte van elkaar kunnen worden gewogen: **waarschijnlijkheid** en **effect**.

Waarschijnlijkheid
Het begrip waarschijnlijkheid heeft betrekking op de kans dat een incident zich zal voordoen. Deze inschatting is moeilijk te maken. Niet alles over wat zich aan ongewenste incidenten voordoet, is bekend. In de risico analyse is expertkennis gekoppeld aan interviews met betrokkenen bij de gemeente Stadskanaal. De bevindingen hiervan hebben geleid tot de beveiligingsmaatregelen zoals opgesomd in paragraaf 1.5.

Effect
De schade van genoemde incidenten kan aanzienlijk zijn. Niet alleen omdat waardevolle documenten of informatie verloren kunnen c.q. kan gaan, maar ook omdat de gevolgen voor medewerkers groot kunnen zijn. Het incident kan tevens nadelige gevolgen hebben voor het beeld van de gemeente bij het publiek.

1.4 Prioriteitstelling

De risico's zijn in de risicoanalyse ten opzichte van elkaar gewogen op de aspecten "waarschijnlijkheid" en "effect" conform de CRAMM methode. Uit de combinatie van "waarschijnlijkheid" en "effect" kan de grootte van het risico worden bepaald. Dit leidt vervolgens tot een zogenoemde prioriteitstelling: een volgorde van de risico's waar men zich tegen moet wapenen.

WAARSCHIJNLIJKHEID	**EFFECT**
Vier niveaus van waarschijnlijkheid	*Vier niveaus van gevolgschade*
1. ONBEDUIDEND ▪ geen geregistreerde of aantoonbare incidenten, wel procedure aanwezig; ▪ geen recente incidenten.	**1. ONBEDUIDEND** ▪ geen meetbaar effect; ▪ te verwaarlozen invloed op imago bij het publiek.
2. LAAG ▪ zeer weinig geregistreerde incidenten; ▪ wel vermoeden maar geen aantoonbare incidenten.	**2. GERING** ▪ er zijn aantoonbare kosten op lokaal niveau, niet op centraal niveau; ▪ implicatie voor imago bij het publiek op lokaal niveau.
3. GEMIDDELD ▪ regelmatig geregistreerde incidenten of een zichtbare trend; ▪ sterke aanwijzing uit meerdere bronnen.	**3. BEDUIDEND** ▪ kan een merkbaar gevolg hebben op de bedrijfsvoering; ▪ serieuze schade aan het imago bij het publiek met aanmerkelijke kosten voor herstel.
4. HOOG ▪ aantal incidenten wijst op een kritieke situatie of een campagne tegen de gemeente; ▪ grote waarschijnlijkheid van toekomstige incidenten gebaseerd op geïdentificeerde factoren.	**4. KRITIEK** ▪ ernstige ontwrichting van de bedrijfsvoering; ▪ bedrijfsvoering op lange termijn wordt aangetast; ▪ ernstige aantasting van het imago van de gemeente bij het publiek met hoge kosten en grote inspanning voor herstel.

Figuur 1 Verduidelijking prioriteitstelling

Het informatiebeveiligingsbeleid van de gemeente Stadskanaal stelt dat de beschikbaarheid van de gegevensprocessen moet zijn afgestemd op het betreffende bedrijfsproces. In dit kader zijn technische en organisatorische maatregelen noodzakelijk om een passend beveiligingsniveau te bereiken.
Deze maatregelen moeten zijn gebaseerd op een zorgvuldige risico analyse, waarbij de lokale omstandigheden bepalend zijn voor de omvang van de bedreigingen. Teneinde deze risico's te inventariseren en adequate voorzieningen te treffen om de beschikbaarheid van de gegevensprocessen te garanderen is op 30 november 2015 een risico analyse uitgevoerd met de volgende leden van de de Projectgroep Informatiebeveiliging van de gemeente Stadskanaal:

- De heer W. ter Horst, de beveiligingsbeheerder;
- De heer M. Westerhof, de CISO;
- De heer H. Panneman, medewerker burgerzaken B;
- De heer H. van der Burgh, gebouwenbeheerder;
- Mevrouw E. Kloen, medewerker burgerzaken A;

Daarbij is een afweging gemaakt van de kans op het optreden van deze bedreigingen en het effect hiervan. Het product van de kans op het optreden van de bedreiging maal het effect heeft geleid tot een prioriteitsstelling in de genoemde risico's. Het resultaat hiervan is zichtbaar gemaakt in de volgende tabel.

1.5 Analyse matrix

Kwaliteitsaspect / Bedreiging	Getroffen maatregelen (de vet gedrukte onderdelen zijn verplicht bij de BRP-audit)	Waar-schijn-lijkheid	Effect	Score	Prio-riteit*	Rest risico	Nog te nemen maatregelen	Planning	Verant-woordelijke
Data-integriteit	**Norm: Het beveiligingsbeleid kent een concrete en meetbare doelstelling over integriteit: opgenomen in het Basisdocument**								
Onvolledigheden/ Onjuistheden • Fouten in handmatige invoer • Foute in externe aanlevering • Systeemfouten	• **Procedure Gegevensverwerking** • **Procedure Correctie** • **Rapportage controle gegevensverwerking** • Functiebeschrijving van de beveiligingsfunctionaris rijbewijzen en reisdocumenten • Regelmatige terugkoppeling tussen afdelingen • Voorlichtingsbijeenkomsten over raadplegingen systeem en wijze van Terugmelden • Procedure Ontvangst en beheer waardedocumenten • Procedure Aanvraag en uitreiking waardedocumenten • Bijlage Ontvangstbewijs Identificatiekaart • Rapportage Evaluatie rijbewijzen • Rapportage Evaluatie reisdocumenten • Extern Onderzoek Reisdocumenten 2010 • **Bijlage Bewerkersovereenkomst** • **Uitvoeren controle door middel van Vragenlijst**	1	2	2	5	**----**	**----**	**----**	**----**

Kwaliteitsaspect / Bedreiging	Getroffen maatregelen (de vet gedrukte onderdelen zijn verplicht bij de BRP-audit)	Waar-schijn-lijkheid	Effect	Score	Prio-riteit*	Rest risico	Nog te nemen maatregelen	Planning	Verant-woordelijke
	bewerker								
Externe fraude • Hoe zijn de controle maatregelen rond het verkrijgen van waardedocumenten ingericht etcetera. • Op welke wijze worden deze gecontroleerd	• Training • Interne controle • Naleving procedures • Toepassing functiescheiding • Procedure Identificatie • Formulier Identificatievragen • Procedure Aanvraag en uitreiking waardedocumenten • Procedure Gegevensverwerking • Alertheid bij management op kwetsbare situatie personeel	1	2	2	5	**----**	**----**	**----**	**----**
Interne fraude • Hoe zijn de controle maatregelen rond de kritische processen geregeld • Op welke wijze worden deze gecontroleerd	• Interne controle • Voorlichtingsbijeenkomsten over logging • Toepassing functiescheiding • Naleving procedures • Procedure Aanvraag en uitreiking waardedocumenten • Procedure Gegevensverwerking • Integriteitsverklaring	1	2	2	5	**----**	**----**	**----**	**----**
Kwantitatieve onderbezetting • Hoeveel personen zijn per functie (ICT en Burgerzaken) beschikbaar	• Bijlage functieverdeling • Voldoende formatie • Vervanging geregeld • Raamcontract voor noodgevallen	3	4	12	1	Te geringe bezetting vergroot de kwetsbaarheid van de bedrijfsvoering tot	Onderzoeken wat mogelijkheid is van extra inhuur (extra inhuur is wenselijk en noodzakelijk)	Q1 2016	Het MT

Kwaliteitsaspect / Bedreiging	Getroffen maatregelen (de vet gedrukte onderdelen zijn verplicht bij de BRP-audit)	Waar-schijn-lijkheid	Effect	Score	Prio-riteit*	Rest risico	Nog te nemen maatregelen	Planning	Verant-woordelijke
(houd rekening met ziekte en verlof) • Is vervanging voldoende geborgd	• Budget voor ondersteuning					niet acceptabele niveau's Kans op kwaliteitsvermindering en fouten groter			
Kwalitatieve onderbezetting • Ervaringsniveau van kritische functies • Opleidingsniveau van kritische functies	• Opleidingen • Coaching • Vervanging geregeld • Raamcontract voor noodgevallen • Budget voor ondersteuning	1	2	2	5	Kans op kwaliteitsvermindering en fouten groter	Meer opleiding voor de medewerkers Burgerzaken is gewenst	Q1 2016	MT
Controleerbaarheid	**Norm: Het beveiligingsbeleid kent een concrete en meetbare doelstelling over controleerbaarheid: opgenomen in het basisdocument**								
Onvolledige controle • Vastlegging in procedures • Vastlegging van taken, bevoegdheden en verantwoordelijkheden (functiescheiding) • Logging • Log controle	• **Rapportage evaluatie beveiligingsbeleid en plan** • **Taken, bevoegdheden en verantwoordelijkheden systeembeheer, applicatiebeheer, informatiebeheer, privacybeheer, gegevensbeheer en beveiligingsbeheer zijn eenduidig vastgelegd in de Bijlage Beheerregeling BRP** • **Er is sprake van functiescheiding tussen degenen die beveiligingsmaatregelen**	1	1	1	6	**----**	**----**	**----**	**----**

Kwaliteitsaspect / Bedreiging	Getroffen maatregelen (de vet gedrukte onderdelen zijn verplicht bij de BRP-audit)	Waar-schijn-lijkheid	Effect	Score	Prio-riteit*	Rest risico	Nog te nemen maatregelen	Planning	Verant-woordelijke
	opstellen, uitvoeren en controleren: opgenomen in de Beheerregeling BRP en in het basisdocument • **Audit trail is mogelijk (loggen) voor alle mutaties** • Audit trail is mogelijk (loggen) voor alle raadplegingen • **Procedure Protocollering** • **Rapportage Controle gegevensverstrekking en protocollering** • Bijlage Uitdraai Beveiligingsnet • Extern onderzoek reisdocumenten • Functiebeschrijving de beveiligingsfunctionaris reisdocumenten en rijbewijzen • **Bijlage Bewerkersovereenkomst** • **Uitvoeren controle middels Bijlage Vragenlijst bewerker**								
Beschikbaarheid	**Norm: Het beveiligingsbeleid kent een concrete en meetbare doelstelling over beschikbaarheid: opgenomen in het basisdocument.**								
Beschikbaarheidsvoorzie-	• **Een actueel**	1	2	2	5	**----**	**----**	**----**	**----**

Kwaliteitsaspect / Bedreiging	Getroffen maatregelen (de vet gedrukte onderdelen zijn verplicht bij de BRP-audit)	Waar-schijn-lijkheid	Effect	Score	Prio-riteit*	Rest risico	Nog te nemen maatregelen	Planning	Verant-woordelijke
ningen • Welke continuïteitsmaatregelen zijn getroffen • Uitwijkregeling (ook facilitaire zaken) • Back-up	**Informatiebeveiligings-plan is aanwezig** • **Jaarlijkse risico- en maatregelenanalyse is uitgevoerd en vastgesteld inclusief evaluatie eerder vastgestelde maatregelen** • **Het BRP systeem wordt gemonitord op beschikbaarheid** • **Periodieke back-up** • **Berichtenverkeer wordt afgehandeld vóór back-up** • **De datasave van de periodieke back-up wordt bewaard in een beveiligde ruimte buiten de serverruimte** • **Procedure Back-up** • **Procedure Restore** • **Brondocumenten worden zodanig bewaard dat aansluiting kan worden gevonden met de datum en het tijdstip van de laatste periodieke back-up** • **Procedure Herstel mutaties BRP** • **Er is een uitwijkcontract voor het BRP systeem waarin wordt gegarandeerd dat het**								

Kwaliteitsaspect / Bedreiging	Getroffen maatregelen (de vet gedrukte onderdelen zijn verplicht bij de BRP-audit)	Waar-schijn-lijkheid	Effect	Score	Prio-riteit*	Rest risico	Nog te nemen maatregelen	Planning	Verant-woordelijke
	BRP systeem binnen 24 uur operationeel is op de locatie van de uitwijkleverancier of op een eigen locatie • **Procedure Uitwijk** • **Uitwijknoodplan: Bijlage intern uitwijkplan geautomatiseerde systemen** • **Jaarlijkse uitwijktest** • **Rapportage test uitwijk** • **Rapportage test restore** • **Rapportage test herstel**								
Brand • Bouwmateriaal gebouw • Materiaal dakbedekking • Leeftijd gebouw • Vrijstaand of aangebouwd • Wat zit in de omgeving	• Brandmelders • Brandhaspels (gecertificeerd) • Brandblussers • Controle op gebruik verdeeldozen • Rookmelders (en doormelding naar alarmcentrale)	1	3	3	4	**----**	**----**	**----**	**----**
Explosie • Gasaansluiting • Wat zit in de omgeving	• Brandmelders • Brandhaspels • Brandblussers	1	4	4	3	**----**	**----**	**----**	**----**
Bliksem • Blikseminslag	• Blikseminstallatie (binnen/buiten) • Conform nieuwe normering	1	1	1	6	**----**	**----**	**----**	**----**
Invloed stof, vuil en water	• Stof afzuiging in	1	2	2	5	**----**	**----**	**----**	**----**

Kwaliteitsaspect / Bedreiging	Getroffen maatregelen (de vet gedrukte onderdelen zijn verplicht bij de BRP-audit)	Waar-schijn-lijkheid	Effect	Score	Prio-riteit*	Rest risico	Nog te nemen maatregelen	Planning	Verant-woordelijke
• Hoe zijn kritische onderdelen gepositioneerd in het gebouw. • Maatregelen in de computerruimte (stofafzuiging) • Hoe zijn brondocumenten opgeborgen (niet te droog of te vochtig)	serverruimte • Waterdrempels • Waterbakken onder leidingen • Airco niet boven servers • Waterdetectie • Contract met schoonmaakbedrijf (met bestek)								
Te hoge temperatuur • Hoe is de koeling geregeld van de werkruimte (concentratiestoringen) • Hoe is de koeling geregeld van de computerruimte (zit deze op de noodstroom voorziening)	• Airco-systeem • 2e airco (back-up) in serverruimte • Onderhoudscontract op airco-systeem • Alarmeringssysteem op airco-systeem in serverruimte • Luchtbehandelingssysteem	1	2	2	5	**----**	**----**	**----**	**----**
Stroomstoring • Is er een noodstroom voorziening? • Wat is hierop aangesloten	• UPS • Noodstroom • Generator beschikbaar • Airco op noodstroomvoorziening aangesloten	1	1	1	6	**----**	**----**	**----**	**----**

Kwaliteitsaspect / Bedreiging	Getroffen maatregelen (de vet gedrukte onderdelen zijn verplicht bij de BRP-audit)	Waar-schijn-lijkheid	Effect	Score	Prio-riteit*	Rest risico	Nog te nemen maatregelen	Planning	Verant-woordelijke
Hardware storingen • Hoe is het wijzigingenbeheer geregeld • Hoe is het incidenten beheer geregeld • Hoe is het probleembeheer geregeld • Welke continuïteitsmaatregelen zijn getroffen	• Afspraken over wijziging hardware • Incidentenbeheer • Zie maatregelen bij beschikbaarheids-voorzieningen	1	3	3	4	**----**	▪ Netwerk herziening (is deels uitgevoerd)	Q42015	J. Lukens
Software storingen • Hoe is het testproces geregeld. • In hoeverre zijn storingen te achterhalen (logging) • Welke continuïteitsmaatregelen zijn getroffen	• Procedure Goedkeuren updates applicatie BRP • Testomgeving aanwezig • Patch en update beleid • Incidentenbeheer • Zie maatregelen bij beschikbaarheids-voorzieningen • Testomgeving/Testplan	1	3	3	4	**----**	Herziening patch/update beleid	**----**	**----**
Inbraak • Welke maatregelen in preventieve sfeer (braak-werend glas / camera's / inbraakdetectie) • Geen waardevolle zaken dichtbij de ramen	• Camera's (intern) • Bewaking • Alarmeringssysteem (muw BUZA en ICT)	1	1	1	6	**----**	**----**	**----**	**----**
Diefstal • Welke maatregelen in preventieve sfeer camera's / kluis / kasten / controle waardevolle goederen) • Geen waardevolle spullen	• Camera's • Sociale controle • Clean desk procedure • Fysieke beveiliging • Aanwezigheid policy	1	1	1	6	**----**	**----**	**----**	**----**

Kwaliteitsaspect / Bedreiging	Getroffen maatregelen (de vet gedrukte onderdelen zijn verplicht bij de BRP-audit)	Waar-schijn-lijkheid	Effect	Score	Prio-riteit*	Rest risico	Nog te nemen maatregelen	Planning	Verant-woordelijke
dicht bij de ramen									
Overval • Welke maatregelen in preventieve sfeer camera's / noodknop) • Waarde beperking	• Procedure Overvalinstructie en agressief publiek • Noodknoppen • Alarmopvolging • Afspraken gebruik noodknoppen bij medewerkers bekend	1	3	3	4	**----**	**----**	**----**	**----**
Sabotage • Motivatie knelpunten • Gevolgen reorganisatie	• Oog voor de medewerker (management) • Interne controle • Alertheid bij management op kwetsbare situatie personeel	1	2	2	5	**----**	**----**	**----**	**----**
Virussen • Aansluitmogelijkheden op het systeem (USB / Externe harddisk) • Draadloos netwerk • Virus controle	• Procedure Antivirus voorzieningen • USB beleid • Restrictie internettoegang • E-mail en internet protocol	1	3	3	4	**----**	**----**	**----**	**----**
Hacking • Heeft er een test plaatsgevonden op de firewall en de website • Wordt de firewall extern gehost • Wordt de firewall extern onderhouden	• Aansluiting op Gemnet • Firewall • Hack-test	1	3	3	4	**----**	**----**	**----**	**----**
Fysiek geweld • Hoe zijn medewerkers	• Training • Procedure Overvalinstructie	2	2	4	3	**----**	**----**	**----**	**----**

Kwaliteitsaspect / Bedreiging	Getroffen maatregelen (de vet gedrukte onderdelen zijn verplicht bij de BRP-audit)	Waar-schijn-lijkheid	Effect	Score	Prio-riteit*	Rest risico	Nog te nemen maatregelen	Planning	Verant-woordelijke
beschermd tegen agressieve bezoekers (noodknop)	en agressief publiek • Noodknoppen • Alarmopvolging • Bijstandsteam								
Verbaal geweld • Hoe zijn medewerkers beschermd tegen agressieve bezoekers (noodknop)	• Training • Noodknoppen • Alarmopvolging • Bijstandsteam • Agressietraining	2	2	4	3	**----**	**----**	**----**	**----**
Vernieling • Welke preventieve maatregelen zijn getroffen		1	2	2	5	**----**	**----**	**----**	**----**
Vertrouwelijkheid	**Norm: Het beveiligingsbeleid kent een concrete en meetbare doelstelling over vertrouwelijkheid: opgenomen in het basisdocument**								
Schenden vertrouwelijkheid / Uitlekken gevoelige informatie • Regels gegevensverstrekking • Elektronisch verstrekking (verkeerd mailadres) • Verstrekking op papier (verkeerd adres) / • Prullenbakken / Papiercontainer / Laten slingeren documenten • Wat mogen technische applicatiebeheerders en systeembeheerders • Hoe gaan mensen in de organisatie om met vertrouwelijke gegevens	• **Het beveiligings-bewustzijn wordt gestimuleerd** • **Instructie medewerkers over risico's Informatiebeveiliging en over de Privacyvoorschriften** • Bijlage Parafenlijst • **Gebruik Formulier Autorisaties** • Gebruik Geheimhoudings-verklaring • **Procedure Geheimhouding** • **Procedure Identificatie en Machtiging** • **Procedure Verstrekken**	1	3	3	4	**----**	**----**	**----**	**----**

Kwaliteitsaspect / Bedreiging	Getroffen maatregelen (de vet gedrukte onderdelen zijn verplicht bij de BRP-audit)	Waar-schijn-lijkheid	Effect	Score	Prio-riteit*	Rest risico	Nog te nemen maatregelen	Planning	Verant-woordelijke
	binnengemeentelijk uit de BRP met o.a. regeling omtrent telefonische verstrekking van gegevens • **Procedure Autorisatie tot het systeem** • **Rapportage controle autorisaties** • **Procedure Verstrekken buitengemeentelijke afnemers/derden** • **Procedure Inzagerecht** • **Procedure Identificatie en Machtiging** • Procedure Verstrekkingen via alternatief medium • **Er is een privacybeheerder BRP aangesteld** • **Beheerregeling BRP** • **Rapportage controle privacyregelgeving** • **Rapportage Controle gegevensverstrekking en protocollering** • Rapportage test verstrekking via alternatief medium • Bijlage Proces verbaal vernietiging van verwijderbare media • Procedure Afvoeren van computers • Procedure vernietiging papier met vertrouwelijk								

Kwaliteitsaspect / Bedreiging	Getroffen maatregelen (de vet gedrukte onderdelen zijn verplicht bij de BRP-audit)	Waar-schijn-lijkheid	Effect	Score	Prio-riteit*	Rest risico	Nog te nemen maatregelen	Planning	Verant-woordelijke
	gegevens								
Ongeautoriseerd gebruik systeem • Is er een adequate gebruikersprocedure • Voorziet P&O in informatie over instroom, doorstroom en uitstroom van medewerkers.	• **Er is een Verordening/Reglement waarin opgenomen vrije derden regeling en verstrekking aan binnengemeentelijke afnemers** • **Individuele identificatie van alle gebruikers** • Voorkomen wachtwoord uitwisseling (kluisprocedure**) • **Procedure Autorisatie tot het systeem** • **Gebruik Formulier autorisaties** • **Rapportage controle autorisaties** • **Eisen aan wachtwoorden conform BRP audit vragenlijst** • Mutatieformulier	2	2	4	3	Blijvend risico ondanks voldoende aandacht	Periodiek aandacht voor vragen bij MT-vergaderingen en afdeling P&O. Awareness	Q1 2016	M. Westerhoff
Onbevoegde aanwezigheid • Hoe is de fysieke toegangsbeveiliging geregeld • Is er een bezoekersregeling • Is er een afsluitcontrole	• Bezoek begeleiden • Bewegingssensoren • Compartimentering gebouw • Alarmeringssysteem • Bewegingssensoren	1	2	2	5	Geen bzoekersregeling (inschrijven uitschrijven)	**----**	**----**	**----**
Attitude personeel	• Voorlichting • Inspraak • Houding	2	3	6	2	**----**	Awareness	Q1 2016	M. Westerhoff

Kwaliteitsaspect / Bedreiging	Getroffen maatregelen (de vet gedrukte onderdelen zijn verplicht bij de BRP-audit)	Waar-schijn-lijkheid	Effect	Score	Prio-riteit*	Rest risico	Nog te nemen maatregelen	Planning	Verant-woordelijke
	• Voorbeeld gedrag management								

* prioriteit 1 = hoogste prioriteit *(waarschijnlijkheid x effect)*

** Het bewaren van een password in de kluis voor noodgevallen. Na gebruik hiervan dient controle plaats te vinden van de gepleegde mutaties.

Figuur 2 Risico en prioriteitsstelling

1.6 Toelichting op de analyse

Op grond van de fysieke technische en personele aspecten voor zover bekend bij de aanwezigen is op grond van de vakkennis en de getroffen maatregelen een inschatting gemaakt van het effect en de waarschijnlijkheid van een bepaalde bedreiging.

Voor een groot aantal bevindingen geldt dat de waarschijnlijkheid en soms mede daardoor het effect in deze voor de gemeente Stadskanaal onbeduidend of laag/gering zijn. Alle deze risico's zijn met een score van 6 of kleiner uit de risico analyse gekomen.

Het onderdeel "Kwantitatieve onderbezetting" kreeg een zeer hoge score van 12.

De nog te nemen maatregelen opgenomen in de 7^{e} kolom kunnen beschouwd worden als een actielijst voor de gemeente, waarvan de voortgang jaarlijks moet worden beoordeeld en waarover moet worden gerapporteerd.

2 Bijlagen

2.1 Bijlage 1 Kenmerken computerruimte

Om aan de in het Informatiebeveiligingsplan beschreven vereisten voor de beschikbaarheid te voldoen heeft de computer- of serverruimte waarin het BRP systeem van de gemeente Stadskanaal is opgesteld, op 30 november 2015 de volgende kenmerken ter voorkoming van gegevensverlies:

	De computerruimte heeft een verhoogde vloer.
X	De computerruimte heeft een temperatuur regeling.
X	De computerruimte kent luchtbehandeling.
	De computerruimte is een apart (brand) compartiment.
X	Toegangscontrole.

Aankruisen indien van toepassing.

2.2 Bijlage 2 Kenmerken fysieke beveiliging

Om aan de in het Informatiebeveiligingsplan beschreven vereisten voor de beschikbaarheid, vertrouwelijkheid en controleerbaarheid te voldoen hebben de in het Informatiebeveiligingsplan beschreven kritische ruimten, op 30 november 2015 de volgende kenmerken ter voorkoming van gegevensverlies en de bescherming van het eigen personeel:

X	Er zijn bewegingsmelders in de onmiddellijke nabijheid.
X	Er zijn (interne) alarmknoppen in de onmiddellijke nabijheid.
X	Er zijn overvalknoppen in de onmiddellijke nabijheid.
X	Er is een bliksemafleider.
X	Er zijn rook- en brandmelders in de onmiddellijke nabijheid.
X	Er zijn brandblussers in de onmiddellijke nabijheid.
	Er zijn detectiepoorten in de onmiddellijke nabijheid.

*) aankruisen indien van toepassing

2.3 Bijlage 3 Kenmerken gemeentelijke voorziening

Om aan de in het Informatiebeveiligingsplan beschreven vereisten voor de beschikbaarheid te voldoen heeft het door de gemeente Stadskanaal ingezette systeem op 30 november 2015 de volgende kenmerken ter voorkoming van gegevensverlies.

X	Het BRP systeem kent een UPS als noodstroomvoorziening welke het systeem in staat stelt minimaal binnen 15 minuten af te sluiten.
X	Het BRP systeem kent eigen stroomvoorziening (dieselgenerator).
X	Het BRP systeem kent RAID 5 beveiliging.
X	Het BRP systeem kent gespiegelde schijven (mirroring).
X	Het door het BRP systeem gebruikte databasemanagement systeem kent een re do log waardoor het herstellen van mutaties mogelijk is.
X	De gebruikers worden geïdentificeerd middels een logische toegangsbeveiliging welke minimaal bestaat uit een wachtwoord van minimaal 6 posities met een levensduur van maximaal 60 dagen waarbij na maximaal 3 foutieve inlogpogingen het gebruikersprofiel automatisch wordt uitgezet.
X	Een nieuw wachtwoord verschilt op minimaal 4 posities ten opzichte van de 3 voorgaande wachtwoorden.
X	Het BRP systeem wordt tijdens de openingstijden gemonitord op beschikbaarheid.
X	Het gemeten beschikbaarheidpercentage van het BRP systeem tijdens de openingstijden is conform de garantie gedurende het afgelopen jaar.
X	BRP systeem wordt buiten de openingstijden gemonitord op beschikbaarheid.
X	Het gemeten beschikbaarheidpercentage van het BRP systeem buiten de openingstijden is conform de garantie gedurende het afgelopen jaar.
X	Er is een balie uitwijksysteem.

Aankruisen indien van toepassing.

2.4 Bijlage 5 Kenmerken gemeentelijk LAN

Om aan de in het Informatiebeveiligingsplan beschreven vereisten voor de beschikbaarheid, vertrouwelijkheid en controleerbaarheid te voldoen heeft het door gemeente Stadskanaal gebruikte Local Area Netwerk op 30 november 2015 de volgende kenmerken ter voorkoming van gegevensverlies.

X	Het lokaal netwerk is gesegmenteerd.
X	Het netwerk is dusdanig ingericht dat het aantal netwerkstoringen zoveel mogelijk wordt beperkt.
X	Er worden alleen standaard netwerkcomponenten gebruikt.
X	Het lokaal netwerk wordt afgeschermd van publieke netwerken door het gebruik van een firewall.
X	Alle netwerkcomponenten worden beheerd en worden voortdurend gemonitord.
X	De gebruikers worden geïdentificeerd middels een logische toegangsbeveiliging welke minimaal bestaat uit een wachtwoord van minimaal 6 posities met een levensduur van maximaal 90 dagen waarbij na maximaal 3 foutieve inlogpogingen het gebruikersprofiel automatisch wordt uitgezet.
X	Een nieuw wachtwoord verschilt op minimaal 4 posities ten opzichte van de 3 voorgaande wachtwoorden.
X	BRP gegevens worden bij datacommunicatie via netwerk buiten fysieke beveiligde zone versleuteld. Dit gebeurt o.a. bij het werken op afstand (= telewerken).
X	BRP gegevens worden bij opslag buiten fysieke beveiligde zone versleuteld opgeslagen. Dit gebeurt o.a. bij het werken op afstand (= telewerken).
X	Wachtwoorden zijn niet door eindgebruikers op te vragen.
X	Bij het in gebreke blijven van de gebruiker vervalt het wachtwoord automatisch.

Aankruisen indien van toepassing.