Rekenkamer ede

De hacker een stap voor blijven

Rekenkamerrapport informatieveiligheid in Ede

Colofon

De Rekenkamer van Ede wil met haar werkzaamheden bijdragen aan de kwaliteit van het lokale bestuur in Ede. Rechtmatigheid, doelmatigheid en doeltreffendheid staan daarbij voorop. Ook draagt de Rekenkamer met haar werkzaamheden bij aan de transparantie van het openbaar bestuur en aan de publieke verantwoording. De werkzaamheden van de Rekenkamer bestaan voornamelijk uit het verrichten van evaluatieonderzoek binnen de beleidscyclus en uit het rapporteren daarover. De Rekenkamer doet dit alles vanuit een onafhankelijke positie; de leden hebben naast hun rekenkamerwerk geen binding met de bestuurlijke noch met de ambtelijke organisatie. De Rekenkamer wordt ondersteund door een ambtelijk secretaris.

De huidige samenstelling van de Rekenkamer is als volgt:
Leden:

- Michel Bergshoef (voorzitter)
- Corry-Anne van der Tang
- Ine van de Vlierd
- Martijn Bakker
- Harmen Binnema

Secretaris/onderzoeker:

- Hessel Boom

Tweede secretaris/onderzoeker:

- Monique Jongenburger

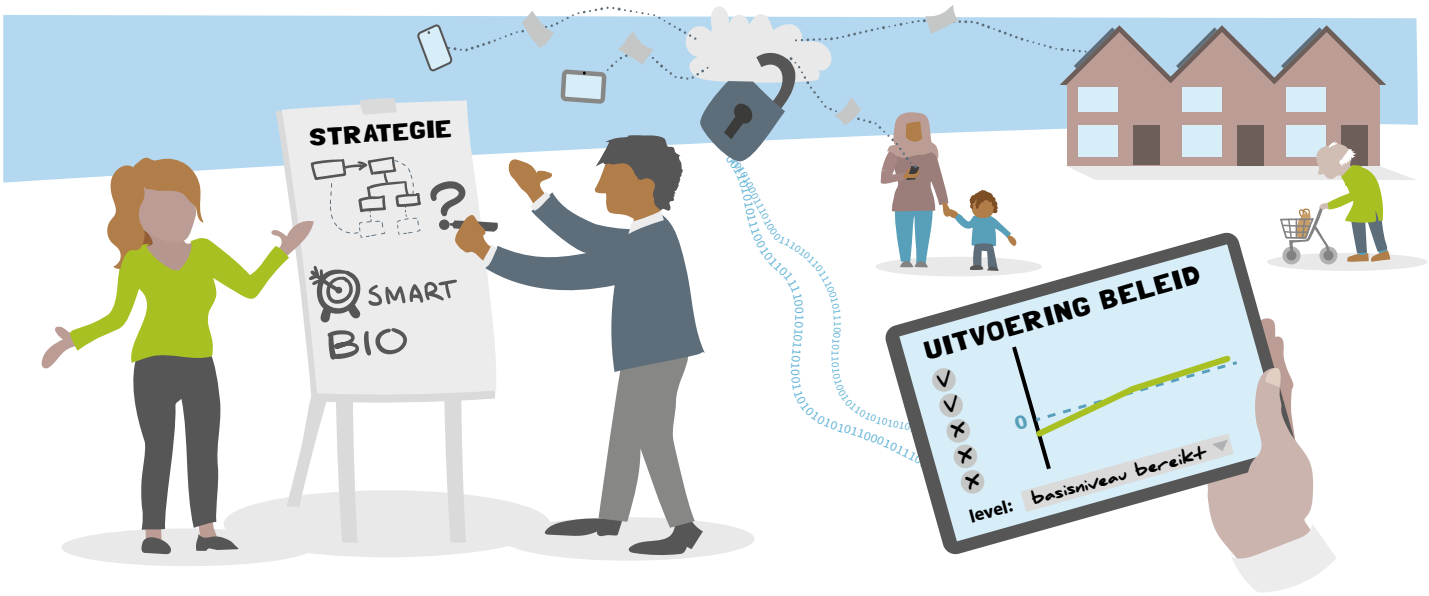
Contactgegevens:
Secretaris/onderzoeker van de Rekenkamer Ede:
Hessel Boom
Postbus 9022
6710 HK Ede

Rekenkamer ede

Informatie veilig houden vereist strategische keuzes door Ede

Een onderzoek naar het beleid voor informatieveiligheid in Ede

Het ontbreekt de gemeente Ede aan het maken van strategische keuzes en beleid. De gegevens van burgers, bedrijven en ambtenaren kunnen beter beschermd worden tegen toekomstige bedreigingen door er eerder over na te denken. Dit concludeert de Rekenkamer Ede in haar onderzoek naar de informatieveiligheid van de gemeente.



CONCLUSIES

HET BELEID
Het beleid is niet SMART geformuleerd en voldoet niet aan actuele standaarden zoals de BIO. Het beleid wordt niet periodiek getoetst, geoefend en/of geëvalueerd.

DE UITVOERING VAN HET BELEID
Het beleid wordt in de basis goed uitgevoerd, maar het ontbreken van een strategisch besluit en focus zorgt dat dit niveau niet wordt ontstegen.

RISICO'S EN INCIDENTEN EN HET LEREND VERMOGEN
Hoewel risico's worden gemonitord en gemitigeerd, is er alleen lerend effect bij incidenten. Het ontbreken van een PDCA-cyclus houdt professionalisering tegen.

DOELSTELLINGEN EN NORMEN
Of Ede de door haar gestelde doelen voor informatieveiligheid heeft behaald kan maar gedeeltelijk worden vastgesteld. Het Edese informatieveiligheidsbeleid voldoet niet volledig omdat het beleid niet geactualiseerd is en een aantal verplichte maatregelen niet zijn genomen.

DE GEMEENTERAAD
De gemeenteraad wordt via de raadswerkgroep Digitalisering incidenteel, maar niet structureel geïnformeerd over het beleid en de uitvoering rondom informatieveiligheid. Ook bij het bepalen van de strategische uitgangspunten van het informatieveiligheidsbeleid is de raad niet aantoonbaar betrokken.

EN NU VERDER... AANBEVELINGEN

RAAD
1 Meebesluiten uitgangspunten
Geef als raad invulling aan je rol bij het bepalen van de ambities en strategische uitgangspunten voor het nieuwe informatie-veiligheidsbeleid.

RAAD
2 Verstevig eigen informatiepositie
Zorg als raad voor structurele informatie en controleer en beoordeel het beleid regelmatig.

COLLEGE
3 Nieuw beleid
Stel als college nieuw beleid vast op basis van de laatste BIO-standaarden inclusief SMART-geformuleerde doelstellingen.

COLLEGE
4 Integraal risicobeeld
Stel als college een integraal risicobeeld op om zo de strategische keuzes te onderbouwen.

Rekenkamer ede

Inhoudsopgave

I. Bestuurlijke nota

1. Inleiding

Gemeenten zijn de afgelopen decennia meer digitaal gaan werken. Daarmee ontstaan nieuwe risico's voor de veiligheid van informatie. Ook worden gemeenten steeds meer geconfronteerd met digitale dreigingen en cyberaanvallen die de continuïteit van dienstverlening bedreigen of kunnen zorgen voor een datalek. Daaruit volgende schade is niet alleen financieel van aard. Datalekken en beveiligingsincidenten tasten ook het vertrouwen in de overheid aan. De digitale dreigingen veranderen continu. Dat betekent dat er constant aandacht voor veiligheid moet zijn. Er zijn ook veranderende (maatschappelijke) omstandigheden die impact kunnen hebben. Zo roept bijvoorbeeld de grote toename van thuiswerken, gestimuleerd door de 'Corona-omstandigheden', nieuwe vragen op met betrekking tot het garanderen van informatieveiligheid.

In dit onderzoek is onderzocht hoe de gemeente Ede haar informatie heeft beveiligd. Voor u ligt de Bestuurlijke Nota met de belangrijkste bevindingen, conclusies en aanbevelingen van het rekenkameronderzoek naar informatieveiligheid in Ede. Dit onderzoek heeft plaatsgevonden in de periode mei tot en met september 2023 en beslaat de periode vanaf 2017 tot september 2023.

In het volgende hoofdstuk volgt eerst de kernboodschap: een korte weergave van de uitkomsten van het onderzoek. Daarna volgt een samenvatting van de bevindingen en conclusies. Ten slotte doen wij aanbevelingen aan de raad en het college. In de bijgevoegde Nota van Bevindingen (inclusief bijlagen) worden de bevindingen beschreven waarop de rekenkamer haar conclusies en aanbevelingen heeft gebaseerd.

2. Kernboodschap

Dit onderzoek is gericht op hoe de gemeente Ede haar informatie heeft beveiligd. Daarbij is gekeken naar het Edese beleid en de uitvoering daarvan, maar ook of het beleid voldoet aan actuele standaarden, wat het lerend vermogen van de organisatie is en hoe de raad wordt betrokken. De volgende vraag stond centraal:

In hoeverre is het Edese informatieveiligheidsbeleid doeltreffend?

Uit het onderzoek blijkt dat het Edese informatieveiligheidsbeleid voor een deel doeltreffend is. De praktische uitvoering is op afdoende niveau: de belangrijke taken worden uitgevoerd en voorzieningen zijn aanwezig. Er is een basisniveau bereikt en er wordt gehandeld in het geval van incidenten en/of actuele ontwikkelingen.

Het Edese informatieveiligheidsbeleid voldoet echter niet volledig, met name op het strategische niveau. Er wordt relatief veel tijd besteed aan de operationele uitvoering van informatiebeveiliging ten opzichte van de strategische taken en het bij- en uitwerken van beleid.

Zo stamt het overkoepelende strategische beleid uit 2017 en is dit nog gebaseerd op het verouderde normenkader. Ook zijn een aantal verplichte maatregelen niet genomen. Het structureel risicomanagement stamt uit 2018. De strategische doelen van informatieveiligheid en de manier waarop de voortgang gemeten kan worden zijn niet geactualiseerd. Dit hindert in een groei in volwassenheid en professionaliteit op dit gebied. Het is van belang de structuren en governance op orde te hebben om te zorgen dat de gemeente in de toekomst niet in de problemen komt.

3. Conclusies

3.1 Het beleid

Het beleid voor informatieveiligheid is vindbaar en uitgedrukt in meerdere documenten, waaronder leveranciersmanagement, incidentmanagement, privacy, technisch management, etc. Een deel van het beleid is recent, een deel is van een oudere datum. Het overkoepelende strategische beleid voor informatieveiligheid stamt uit 2017. Dit beleid is gebaseerd op het verouderde normenkader Baseline Informatiebeveiliging Gemeenten. Het voldoet niet aan de actuele standaarden omdat het niet op het geldende normenkader, de Baseline Informatiebeveiliging Overheid (BIO)[1], is gestoeld. Er zijn wel voorbereidende activiteiten ontplooid om het beleid te herzien. Voor zover bekend heeft dit echter niet geleid tot het vaststellen van een (SMART) ambitieniveau.

Conclusie: Het beleid is vindbaar, maar niet SMART geformuleerd en voldoet niet aan actuele standaarden zoals de BIO. Het beleid wordt niet periodiek getoetst, geoefend en/of geëvalueerd.

3.2 De uitvoering van het beleid

Organisatie en proces van informatieveiligheid
Er wordt relatief veel tijd besteed aan de operationele uitvoering van informatiebeveiliging ten opzichte van de strategische taken. Over het algemeen is de praktische uitvoering binnen het domein informatiebeveiliging op afdoende niveau. Niet alle onderdelen die in het beleid zijn beschreven worden in de praktijk uitgevoerd. Het beleid moet nog worden uitgewerkt. In de praktijk werkt de gemeente al wel grotendeels volgens de BIO.
Rollen en verantwoordelijkheden worden in praktijk anders ingevuld dan in het beleid beschreven. Een voorbeeld daarvan zijn de verantwoordelijkheden van proceseigenaren (afdelingsmanagers) ten aanzien van informatieveiligheid. Niet alle afdelingsmanagers lijken voldoende kennis en competenties te hebben om risico's goed in te schatten en de juiste maatregelen te kiezen. Daarnaast is bijvoorbeeld een structurele uitvoering van risicomanagement en de informatieveiligheidsanalyse niet gevonden.

Het bestuurlijk aspect
Er is bestuurlijke aandacht voor informatieveiligheid. Het onderwerp informatieveiligheid staat periodiek op de agenda bij directie en bestuur, maar het ontbreekt aan een strategisch gesprek en strategische besluitvorming.
Op techniek en medewerkersniveau kunnen nog stappen worden gezet. In algemene zin geldt dat beleid beter kan worden uitgewerkt en herijkt naar de huidige situatie. Ook het praktische handelen van dag tot dag zou daarbij op papier gezet moeten worden. Door het

1 BIO betreft de Baseline Informatiebeveiliging Overheid, het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen). De BIO is in december 2018 vastgesteld en per 1-1-2019 is gestart met de implementatie van de BIO. De overheid heeft zich verplicht de BIO te implementeren.

vastleggen van deze processen wordt het risico verkleind dat een proces leunt op individuen. Uit de interviews begrijpen wij dat werkdruk en capaciteitsgebrek een oorzaak kunnen zijn. Het bij- en uitwerken van beleid blijft achter bij het handelen op dagelijkse issues en actualiteiten. De afwezigheid van strategische keuzes of een ambitieniveau kunnen hier een oorzaak van zijn. Wanneer geen doel is geformuleerd, is het risico dat de aandacht gericht blijft op de operationele taken die op dat moment voorliggen.

Conclusie: Het beleid wordt in de basis goed uitgevoerd, maar het ontbreken van een strategisch besluit en focus zorgt dat dit niveau niet wordt ontstegen.

3.3 Risico's en incidenten en het lerend vermogen

Ede werkt aan de hand van een procedure voor incidenten. Na incidenten worden evaluaties uitgevoerd op basis waarvan geïdentificeerde risico's, aanbevelingen en geplande acties en wijzigingen worden vastgelegd. De gemeente probeert daarmee te leren van incidenten. Conform de berichten uit de jaarrapportages is ervaring opgedaan met de incidentprocedure in de praktijk. Voor zover wij hebben kunnen beoordelen werkt dit naar behoren, al is niet op incidentniveau onderzoek gedaan.
Binnen de gemeente is geen structureel risicomanagement ingericht waarbij op voorhand keuzes en afwegingen worden gemaakt door het management over de beveiliging van processen. De laatste gevonden informatieveiligheidsanalyse zoals beschreven in het beleid stamt uit 2018. Door het ontbreken van een strakke structurele sturing op de organisatorische en procesmatige maatregelen uit het beleid lijken veel van de activiteiten en de risicoanalyses ad hoc te worden ingezet.
Een PDCA-cyclus (Plan-Do-Check-Act) is formeel onderdeel van beleid, maar in de praktijk kan het lerend vermogen nog sterk worden ontwikkeld. Dit komt terug in het ontbreken van gap- en informatieveiligheidsanalyses en opvolging op actieplannen. In algemene zin geldt dat het goed uitvoeren van alle vier de elementen (plannen maken en ontwikkelen, uitvoeren, controleren en toetsen en vervolgens bijsturen) maakt dat de organisatie verder kan groeien in haar professionaliteit, binnen de actuele en algemene context voor gemeenten waaronder druk op de middelen en druk vanuit de huidige arbeidsmarkt (personeelsverloop in combinatie met moeizame invulling van sommige vacatures).
Conclusie: Hoewel risico's worden gemonitord en gemitigeerd, is er alleen lerend effect bij incidenten. Het ontbreken van een PDCA-cyclus houdt professionalisering tegen.

3.4 Doelstellingen en normen

De doelstellingen van de gemeente Ede ten aanzien van informatieveiligheid zijn in het strategisch beleid opgenomen. Het doel van informatieveiligheid is geformuleerd als het behoud van continuïteit, integriteit en betrouwbaarheid van de gegevens, vertrouwelijkheid en exclusiviteit en controleerbaarheid. In hoeverre de doelen worden behaald, kan nu alleen worden beoordeeld aan de hand van incidenten (diegene die er zijn worden afgehandeld en datalekken worden gemeld). Dit onderzoek heeft niet getracht een uitputtend overzicht te geven van de stand van zaken van de gemeente op alle normen uit de BIO. Wel is uit het onderzoek het beeld ontstaan dat de gemeente de basis op orde heeft en voor een groot deel voldoet aan de BIO. Een deel van de normen vanuit de BIG zijn hetzelfde als die uit de BIO. Echter mede omdat het strategisch informatieveiligheidsbeleid van Ede uit 2017 stamt en gebaseerd is op de het verouderde normenkader BIG, voldoet de gemeente niet (volledig) aan de geldende normen voor informatieveiligheid.

Conclusie: Of Ede de door haar gestelde doelen voor informatieveiligheid heeft behaald kan maar gedeeltelijk worden vastgesteld. Het Edese informatieveiligheidsbeleid voldoet echter niet volledig omdat het beleid niet geactualiseerd is en een aantal verplichte maatregelen niet zijn genomen.

3.5 De gemeenteraad

In 2022 is een raadswerkgroep digitalisering gestart waarbij elke fractie de gelegenheid heeft gehad één raadslid af te vaardigen. De raadswerkgroep wordt uitgebreider dan de volledige raad geïnformeerd over digitalisering en wordt ook betrokken bij het informatieveiligheidsbeleid. De fractievertegenwoordigers dienen hun eigen fracties te informeren en de stukken van de raadswerkgroep zijn voor alle raadsleden te benaderen.

Het actief controleren en beoordelen van het informatieveiligheidsbeleid door de raad is een punt van aandacht. Er is (afgezien van jaarrapportages in de jaren 2018-2022) geen structurele informatievoorziening over de stand van zaken. Er is geen goed en/of gedeeld beeld van de informatie die de raad voor deze taak nodig zou hebben. De raad geeft aan op basis van de informatie die zij wél hebben vertrouwen te hebben in het niveau van beveiliging en het risico op incidenten niet hoog in te schatten. Tegelijkertijd geven ze aan dat zij het geheel niet kunnen overzien, dat de impact van een informatiebeveiligingsincident groot kan zijn en dat het wel nodig is om gezamenlijk een beter beeld te hebben van de stand van zaken en het daadwerkelijke risicoprofiel. De raad geeft aan graag te willen zien dat zij benaderd worden met scenario's zodat er een gesprek over afweging en ambitie plaats kan vinden.

Conclusie: De raad wordt regelmatig, maar niet structureel geïnformeerd over het beleid en de uitvoering rondom informatieveiligheid. De raad is niet aantoonbaar betrokken bij het bepalen van de uitgangspunten van het informatieveiligheidsbeleid. Het aantoonbaar actief controleren en beoordelen van het informatieveiligheidsbeleid door de raad is een punt van aandacht.

4. Aanbevelingen

Voor de gemeenteraad

1. Vul de kaderstellende rol met betrekking tot informatieveiligheid in door mee te besluiten over strategische uitgangspunten (of ambitieniveau) voor het informatieveiligheidsbeleid.
2. Verstevig de eigen informatiepositie en controleer en beoordeel het beleid periodiek. Zorg ervoor dat er minimaal jaarlijks wordt gesproken over informatieveiligheid, bijvoorbeeld over de ambitie en kaders.

Voor het college van B&W

3. Stel nieuw beleid vast conform de BIO waarbij het strategisch gekozen ambitieniveau uitgangspunt is voor SMART-geformuleerde doelstellingen.
4. Stel een integraal risicobeeld op om strategische keuzes op het gebied van informatieveiligheid te onderbouwen. Stel dit risicobeeld gestructureerd en periodiek bij op basis van (onder andere) informatie over dreigingen en veranderingen in processen en systemen. Stimuleer het lerend vermogen door de PCDA-cyclus beter in te richten.

5. Reactie van het college

Burgemeester en Wehouders

Rekenkamer
postbus 9022
6710 HK Ede

Onderwerp: Bestuurlijke reactie Rekenkameronderzoek beleid informatiebeveiliging Ede

Ede, 5 december 2023

Geachte leden van de Rekenkamer,

Het college spreekt haar waardering uit voor de uitvoering van het onderzoek informatie-veiligheid in Ede bij gemeente Ede. U heeft hierin onderzocht in hoeverre het Edese informatieveiligheidsbeleid doeltreffend is.

Het college heeft met interesse het rapport gelezen en hecht belang aan de uitkomsten van dit onderzoek en beschouwt het rapport als een waardevolle bijdrage aan het verbeteren van het beleid. In het kader van bestuurlijk wederhoor richten wij ons op de door u aangegeven aanbevelingen die aan ons als college zijn gericht.

Wij waarderen de grondigheid van uw rapport. Kijkend naar de kernboodschap herkennen wij ons in de opgave om een verdere professionaliseringslag op het gebied van informatiebeveiliging te maken en blijven daar ook aan werken. Wij nemen de aanbevelingen aan het college dan ook over. Gedurende het onderzoek is het herzien van het beleid tot afronding gekomen wat een aantal deelconclusies raakt. In de bijlage treft u daar een toelichting waar dit van toepassing is.

Aanbevelingen voor het college van B&W

Aanbeveling 3: Stel nieuw beleid vast conform de BIO waarbij het strategisch gekozen ambitieniveau uitgangspunt is voor SMART-geformuleerde doelstellingen.

Reactie van college aanbeveling 3:
Deze aanbeveling nemen wij over. Het herzien van het beleid had al onze aandacht. Het nieuwe beleid is inmiddels geactualiseerd conform de BIO en vastgesteld door het college, waarbij het belang van goede informatiebeveiliging bij gemeente Ede wordt onderstreept in zowel visie, als bestuurlijke principes, als doelstellingen. Het dient als strategisch uitgangspunt voor verdere planvorming.

Aanbeveling 4: Stel een integraal risicobeeld op om strategische keuzes op het gebied van informatieveiligheid te onderbouwen. Stel dit risicobeeld en periodiek bij op basis van (onder andere) informatie over dreigingen en veranderingen in processen en systemen. Stimuleer het lerend vermogen door de PDCA-cyclus beter in te richten.

Reactie van college aanbeveling 4:
Deze aanbeveling nemen wij over. De doelstelling om te komen tot een integraal risicobeeld is ook vastgelegd in het nieuwe strategische beleid 2023-2027. Hierin worden een omgevingsanalyse gecombineerd met een organisatie brede risicoanalyse. Met dit inzicht valt met een brede blik input te leveren aan de organisatie en haar afdelingen om conform de PDCA-cyclus bedrijfsprocessen op de BIO baseline in te richten of bij te stellen.

Dankwoord
Graag bedanken wij u voor het onderzoek en het uitbrengen van het rapport. De samenwerking met de Rekenkamer gedurende het onderzoek hebben wij als prettig ervaren.

Hoogachtend,
burgemeester en wethouders,

drs. R.F. Groen MPA	mr. L.J. Verhulst
secretaris	burgemeester

Bijlage 1: Reacties deelconclusies

Conclusie 3.1 het beleid
Het beleid is vindbaar, maar niet SMART geformuleerd en voldoet niet aan actuele standaarden zoals de BIO. Het beleid wordt niet periodiek getoetst, geoefend en/of geëvalueerd.

Reactie college 3.1:
Het actualiseren van het beleid stond al op de planning, maar was nog niet tot afronding gekomen.
Recent is strategisch beleid voor informatiebeveiliging geheel herzien. De herziening is conform de actuele standaarden en beschrijft specifieke doelen op basis van de BIO. Ook heeft, na evaluatie, het nieuwe beleid bijstellingen daar waar het oude beleid minder goed voldeed.

Conclusie 3.2 de uitvoering van het beleid
Het beleid wordt in de basis goed uitgevoerd, maar het ontbreken van een strategisch besluit en focus zorgt dat dit niveau niet wordt ontstegen.

Reactie college 3.2:
We onderschrijven de conclusie, maar zien hier ook het bredere perspectief: de overige bevindingen weergegeven bij 3.2 in het rapport. We zien dat zowel omvang als complexiteit van aandachtsgebieden binnen informatiebeveiliging door de jaren heen snel zijn toegenomen, wat ook continue een uitdaging geeft om dat binnen de huidige organisatie te blijven adresseren. Er is veel aandacht geweest aan informatiebeveiliging op operationeel niveau, vaak intensief begeleid door tactische en strategische adviseurs op informatiebeveiliging en daarmee is een basis gelegd die ook direct in de dagelijkse praktijk nodig is. Er worden continue verbeteringen doorgevoerd en ook het verbeteren van de strategische sturing (de governance) op informatiebeveiliging is een punt van aandacht.

Conclusie 3.3: Risico's en incidenten en het lerend vermogen
Hoewel risico's worden gemonitord en gemitigeerd, is er alleen lerend effect bij de incidenten. Het ontbreken van de PDCA-cyclus houdt professionalisering tegen.

Reactie college 3.3:
Dit is een constatering die door alle partijen wordt onderschreven. Het nieuw vastgestelde strategische beleid heeft een nieuwe uitwerking van het benodigde Information Security Management System (ISMS), de governance-structuren voor informatiebeveiliging. Hiermee wordt dan ook de PDCA-cyclus beter verankerd in de organisatie.

Conclusie 3.4: Doelstelling en normen
Of Ede de door haar gestelde doelen voor informatieveiligheid heeft behaald kan maar gedeeltelijk worden vastgesteld. Het Edese informatieveiligheidsbeleid voldoet echter niet volledig, omdat het beleid niet geactualiseerd is en een aantal verplichte maatregelen niet zijn genomen.

Reactie college 3.4:
Het beleid is inmiddels geactualiseerd. Zoals het onderzoek vaststelt werkt gemeente Ede al grotendeels conform de BIO. De BIO gaat uit van risico gebaseerde aanpak. Praktisch gezien kijk je dan ook naar het beoogde effect van een (verplichte) maatregel. Dit heeft ook de volgorde bepaald welke BIO implementaties eerst moesten en elkaar versterken. We blijven de implementaties doorvoeren om naar een hoger organisatie volwassenheidniveau te komen voor zowel verplichte als niet verplichte beheersmaatregelen.

Conclusie 3.5 De gemeenteraad
De raad wordt regelmatig, maar niet structureel geïnformeerd over het beleid en de uitvoering rondom informatieveiligheid. De raad is niet aantoonbaar betrokken bij het bepalen van de uitgangspunten van het informatiebeveiligingsbeleid. Het aantoonbaar actief controleren en beoordelen van het informatieveiligheids-beleid door de raad is een punt van aandacht.

Reactie college 3.5:
Het bestuurlijke gesprek over informatiebeveiliging kan nog verder ontwikkeld worden. De raad krijgt jaarlijks zowel via de paragraaf bedrijfsvoering in de jaarrekening en via het jaarverslag informatiebeveiliging structureel informatie aangeboden. De uitgangspunten bij informatiebeveiliging zijn rigide. De BIO laat als afgeleide van internationale kwaliteitstandaarden (ISO 27001 en 27002) weinig ruimte voor eigen invulling. De bestuurlijke dialoog leent zich juist voor (nieuwe) taken die op de gemeente afkomen, nieuwe (Europese) wetgeving, onze rol als centrumgemeente en de voortgang van doorgaande ontwikkelingen. Dit kan goed in samenhang met hoe we risico's, waaronder informatiebeveiligingsrisico's, beheersbaar houden.

6. Nawoord Rekenkamer

De Rekenkamer bedankt het college van B en W voor zijn reactie op het rapport. Het is goed om te lezen dat het college zich herkent in de kernboodschap en conclusies. Het college neemt de aanbevelingen gericht aan het college over, en geeft aan dat deze voor een deel inmiddels uitgevoerd.

De Rekenkamer vindt het positief dat het college het beleid inmiddels heeft geactualiseerd conform de BIO. In dit 'Strategisch beleid informatiebeveiliging 2023-2027' is ook de doelstelling uit de vierde aanbeveling opgenomen om te komen tot een integraal risicobeeld. Daarnaast herkent het college ook dat het ontbreken van een PDCA-cyclus professionalisering tegenhoudt. In het nieuwe beleid wordt het Information Security Management System (ISMS) uitgewerkt en wordt de PDCA-cyclus daarin beter verankerd. We hopen dat de daadwerkelijke implementatie van het ISMS in de praktijk bij zal dragen aan het lerend vermogen van de organisatie.

Een van de conclusies van het rapport is dat de raad niet aantoonbaar betrokken is bij het bepalen van de uitgangspunten voor het informatieveiligheidsbeleid. Ook het aantoonbaar actief controleren en beoordelen van informatieveiligheidsbeleid door de raad is een punt van aandacht. De aanbevelingen aan de gemeenteraad zijn dan ook gericht op het invullen van de kaderstellende rol bij de uitgangspunten van het beleid en het verstevigen van de eigen informatiepositie.

In november 2023 heeft het college het nieuwe beleid, 'Strategisch beleid informatiebeveiliging 2023-2027', vastgesteld. Dit nieuwe beleid is vastgesteld na de onderzoeksperiode van dit onderzoek en de Rekenkamer heeft dus niet kunnen beoordelen of het beleid nu voldoet. Het beleid is daarnaast niet in de gemeenteraad besproken en het beleid is ook niet ter kennisgeving met de raad gedeeld. De raad is daarmee niet in de gelegenheid gesteld dit beleid te beoordelen.

Tot slot wil de Rekenkamer graag nogmaals het belang van het betrekken van de raad bij het bepalen van de strategische uitgangspunten voor het informatieveiligheidsbeleid benadrukken. Het college geeft in haar reactie aan dat uitgangspunten bij informatieveiligheid rigide zijn en de BIO weinig ruimte laat voor eigen invulling. De Rekenkamer wil meegeven dat de BIO basisrichtlijnen betreft. Bestuurlijk kan met de raad worden besproken of verdere ambities gewenst zijn. De raad kan bijvoorbeeld worden betrokken bij verdergaande digitalisering en daarbij behorende kansen en risico's voor informatieveiligheid en hoe de gemeente daarin wil staan.

De Rekenkamer ziet de behandeling van dit rapport door de raad met belangstelling tegemoet en zal de verdere ontwikkelingen met betrekking tot informatieveiligheid blijven volgen.

I I. Nota van bevindingen

1. Inleiding

1.1 Aanleiding

Gemeenten zijn de afgelopen decennia meer digitaal gaan werken. Daarmee ontstaan nieuwe risico's voor de veiligheid van informatie. Ook worden gemeenten steeds meer geconfronteerd met digitale dreigingen en cyberaanvallen die de continuïteit van dienstverlening bedreigen of kunnen zorgen voor een datalek. Daaruit volgende schade is niet alleen financieel van aard. Datalekken en beveiligingsincidenten tasten ook het vertrouwen in de overheid aan. De digitale dreigingen veranderen continu. Dat betekent dat er constant aandacht voor veiligheid moet zijn. Er zijn ook veranderende (maatschappelijke) omstandigheden die impact kunnen hebben. Zo roept bijvoorbeeld de grote toename van thuiswerken, gestimuleerd door de 'Corona-omstandigheden', nieuwe vragen op met betrekking tot het garanderen van informatieveiligheid.
Een goede omgang met informatie betreft niet alleen de technische (ICT-)beveiliging en het bewustzijn bij de verwerkers van informatie, maar ook het waarborgen van een verstandige en wettelijk toelaatbare toepassing van die informatie. Als het gaat om informatieveiligheid moet de gemeente onder meer voldoen aan diverse wettelijke vereisten uit de Algemene Verordening Gegevensbescherming (AVG) en de Baseline Informatiebeveiliging Overheid (BIO)[2]. Gemeentelijke accountants hebben hier ook aandacht voor.

Informatieveiligheid
Informatieveiligheid gaat over de maatregelen en procedures om beschikbaarheid, integriteit en vertrouwelijkheid van informatie te garanderen en in het bijzonder om de continuïteit van de informatie en informatievoorziening te waarborgen en de gevolgen van incidenten tot een acceptabel niveau te beperken. De maatregelen die in het kader van informatiebeveiliging worden genomen zijn bedoeld om te beschermen tegen bedreigingen zoals menselijke fouten, technisch falen en cybercriminaliteit.
Nederlandse gemeenten moeten aan een aantal kaders voor informatiebeveiliging voldoen. Eén van deze kaders is de Baseline Informatiebeveiliging Overheid (BIO). Ook worden er regelmatig onderzoeken uitgevoerd naar informatiebeveiliging, zoals de jaarlijkse ENSIA (Eenduidige Normatiek Single Information Audit) met betrekking tot basisadministraties, Suwinet[3] en DigiD. Daarnaast kan de gemeente zelf ook onderzoek naar informatiebeveiliging (laten) doen, bijvoorbeeld in de vorm van een penetratietest[4] of een volwassenheidsonderzoek. De gemeente heeft een verantwoordelijkheid om te voldoen aan deze kaders en verplichte of eigen onderzoeken uit te voeren om aan te tonen dat er aan deze kaders wordt voldaan.

2 BIO betreft de Baseline Informatiebeveiliging Overheid, het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen). De BIO is in december 2018 vastgesteld en per 1-1-2019 is gestart met de implementatie van de BIO. De overheid heeft zich verplicht de BIO te implementeren.
3 Suwinet is zowel een applicatie als de digitale infrastructuur om gegevens over werk en inkomen te delen met mede-overheden (Suwi partijen).
4 Een technische test van een informatiesysteem waarbij de tester zich gedraagt als een hacker en van buiten probeert binnen te dringen.

Dit rekenkameronderzoek heeft niet tot doel om de rol van andere onderzoeken over te nemen of op detailniveau aan te tonen in welke mate de gemeente voldoet aan verplichte kaders. Met behulp van het onderzoek wordt inzicht gegeven in hoeverre het Edese informatieveiligheidsbeleid doeltreffend is (zie de onderzoeksvragen), waarbij de genoemde kaders en onderzoeken een belangrijke rol spelen maar niet op detailniveau getoetst worden of over worden gedaan. Als het gaat om de BIO, richt dit onderzoek zich op de beheersing van informatiebeveiliging door de gemeente op basis van de BIO. Als het gaat om specifieke onderzoeken of audits, richt dit onderzoek zich op welke onderzoeken de gemeente uitvoert, hoe bevindingen worden opgevolgd en welke blinde vlekken er mogelijk zijn ten aanzien van informatieveiligheid.

1.2 Onderzoeksvragen

Voor dit onderzoek staat de volgende vraag centraal:

In hoeverre is het Edese informatieveiligheidsbeleid doeltreffend?

Deze centrale onderzoeksvraag is uitgewerkt in de volgende deelvragen:

1. Wat is het Edese beleid op het gebied van informatieveiligheid en voldoet dit aan actuele standaarden?
2. Hoe wordt dit beleid uitgevoerd (bestuurlijk, organisatorisch, technisch, op proces- en medewerkersniveau)?
3. Hoe reageert Ede op risico's en incidenten op het gebied van informatieveiligheid en wat is het lerend vermogen van de organisatie (plan – do – check – act)?
4. Worden de geformuleerde doelstellingen gehaald en voldoet Ede aan de geldende normen voor informatieveiligheid (BIO)?
5. Hoe is de raad betrokken bij (de uitvoering van) het beleid ten aanzien van de informatieveiligheid?

In de onderzoeken van de rekenkamer is het gebruikelijk om een normenkader te hanteren. Dit normenkader wordt primair gebruikt om de betrokkenen een spiegel voor te houden waar zij ten opzichte van hun eigen beleidsvoornemens staan. De normen zijn direct gerelateerd aan de deelvragen. Op basis van het onderzoek wordt na kennisname en analyse van de praktijk een oordeel gegeven op deze normen. De deelvragen en bijbehorende normen zijn te vinden in Bijlage 1: Normenkader.

1.3 Aanpak

Voor dit onderzoek is de volgende aanpak (onderzoeksactiviteiten) gehanteerd:

- Het onderzoek is gestart met een bijeenkomst met de ambtelijke organisatie waarbij een toelichting is gegeven op het onderzoek, er een mogelijkheid was voor het stellen van vragen en waar afspraken voor de uitvoering van het onderzoek zijn gemaakt.
- Er is een documentstudie uitgevoerd.
- Er zijn interviews afgenomen bij sleutelfunctionarissen, zoals de portefeuillehouder, de concerndirecteur, de Chief Information Security Officer (CISO) en andere medewerkers.
- Op basis van de bevindingen uit de interviews en documentstudie zijn twee casussen geselecteerd voor verdiepend onderzoek[5] (bestaande uit zowel documentstudie als een bijeenkomst met betrokken functionarissen).

5 De onderzochte processen zijn opgenomen in bijlage 5 (geheim)

- Ten slotte is er een discussiebijeenkomst met de gemeenteraad georganiseerd om nader inzicht te krijgen in hun kaderstellende, controlerende en volksvertegenwoordigende rol ten aanzien van informatieveiligheid.

De onderzoeksresultaten zijn geland in een rapport van bevindingen dat bij de ambtelijke organisatie is neergelegd voor wederhoor. Vervolgens is de rapportage inclusief conclusies en aanbevelingen voor bestuurlijk wederhoor aan het college aangeboden.

1.4 Leeswijzer

In hoofdstuk twee wordt ingegaan het beleid aan de hand van de centrale beleidsdocumenten- en voornemens van de gemeente op het gebied van informatieveiligheid. In hoofdstuk drie wordt geschetst hoe deze beleidsuitgangspunten in de praktijk door de gemeente worden uitgevoerd op bestuurlijk, organisatorisch, technisch, en proces- en medewerkersniveau. Daarbij wordt ook aandacht besteed aan het reageren op risico's en incidenten en het lerend vermogen van de gemeente én of Ede voldoet aan haar doelstellingen en de BIO. Het vierde hoofdstuk besteedt aandacht aan de rol van de gemeenteraad. In het laatste hoofdstuk worden de deelvragen en centrale vraag beantwoord.
In bijlage één is het normenkader inclusief waardering opgenomen. Daarnaast is een overzicht te vinden van de bestudeerde achtergronddocumenten (bijlage twee) en geïnterviewde personen (bijlage drie). Ten slotte is in bijlage vier een verklarende woordenlijst toegevoegd. In bijlage 5 zijn onderdelen opgenomen waar geheimhouding is opgelegd.

2. Het beleid

De gemeente Ede heeft verschillende beleidsstukken die betrekking hebben op informatieveiligheid. In dit rapport wordt eerst het strategisch beleid behandeld, vervolgens het tactisch en operationeel beleid. Er wordt een beschrijving gegeven van het beleid dat is aangetroffen bij de documentstudie en verwijzingen uit de gevoerde interviews. Ook wordt beschreven wat de status van de beleidsstukken is. Hieronder wordt in samenvattende teksten de inhoud van het beleid weergegeven zoals daarin beschreven. Daarbij hebben wij niet de intentie gehad om volledig te zijn. Het is bedoeld een indruk te geven van belangrijke onderdelen. In hoofdstuk drie is vervolgens opgenomen wat de bevindingen uit de praktijk zijn ten aanzien van het beleid.

2.1 Strategisch beleid

Het strategisch beleid is geformuleerd in het gemeentebreed informatieveiligheidsbeleid 'Vrijheid in gebondenheid'. Dit beleid stamt uit 2017[6] en is gebaseerd op het toenmalige, inmiddels verouderde normenkader Baseline Informatiebeveiliging Gemeenten (BIG)[7]. Het strategisch beleid wordt uitgewerkt in onderliggende 'informatieveiligheidsanalyse' en 'actieplannen informatieveiligheid' waarin de implementatie van het beleid is opgenomen. Daaronder liggen specifieke beleidsstukken en procesbeschrijvingen.
Ede stelt in dit momenteel geldende beleid dat de bestuurs- en bedrijfsprocessen van de overheid een grootschalige verwerking van vaak vertrouwelijke gegevens vereisen. "Informatieveiligheid garandeert dat deze gegevensverwerking betrouwbaar is (in termen van beschikbaarheid, integriteit en vertrouwelijkheid) door een proces in te richten dat bestaat uit het maken, onderhouden en controleren van een samenhangend stelsel van maatregelen."[8]
Het doel van informatieveiligheid wordt in het beleid geformuleerd als het behoud van:

- beschikbaarheid / continuïteit (voorkomen van uitval van systemen);
- integriteit / betrouwbaarheid (gegevens zijn juist, actueel en volledig);
- vertrouwelijkheid / exclusiviteit (onbevoegden kunnen geen kennis nemen van gegevens die niet voor hen bestemd zijn);
- controleerbaarheid.

2.1.1 Rollen en Verantwoordelijkheden

In het strategische beleid zijn diverse rollen en verantwoordelijkheden ten aanzien van informatieveiligheid uitgebreid beschreven. Hier worden de relevante rollen en verantwoordelijkheden beknopt beschreven. De rol van de gemeenteraad wordt in het

6 Tijdens het onderzoek hebben wij vernomen dat wordt gewerkt aan een update van dit beleid, gebaseerd op de BIO. Een nieuw beleid is nog niet geëffectueerd.

7 De BIG, de Baseline Informatie Gemeenten, is een door de VNG opgestelde systematiek om een goede basis voor de informatiebeveiliging te realiseren. Voorheen hadden alle bestuurslagen een eigen baseline, de BIR (Rijk), BIG (gemeenten), IBI (provincies) en BIWA (waterschappen). Deze baselines waren (met uitzondering van de BIR2017) voor een groot deel nog gebaseerd op de ISO-normering uit 2005 en lopen achter op de actuele ISO uit 2013 (NEN-ISO 27002). In afstemming met waterschappen, provincies en het rijk zijn de baselines, waaronder BIG, doorontwikkeld naar de Baseline Informatiebeveiliging Overheid (BIO). De BIO verschilt op een aantal punten van de BIG. De BIO legt meer nadruk op risicomanagement dan de BIG, die meer gaat over specifieke maatregelen. De rol van de bestuurder en lijnmanager is ten aanzien van risicomanagement explicieter dan de BIG aangaf. Daarnaast zijn BIO maatregelen altijd verplicht en is de BIO meer risico georiënteerd (het begint met een Baselinetoets BIO).

8 Gemeentebreed Informatieveiligheidsbeleid Ede (2017), pagina 6.

beleid expliciet genoemd. Daarnaast komen diverse andere rollen en functionarissen aan bod waarvan de belangrijkste hieronder genoemd worden. De mate waarin de praktijk overeenkomt met het beschreven beleid wordt behandeld in hoofdstuk 3.

De **gemeenteraad** draagt een specifieke bevoegdheid voor de controle en de toetsing op de werking van beleid binnen de gemeente, zo ook voor informatieveiligheid. Het **college van B&W** is verantwoordelijk voor het beleid en de implementatie daarvan. Dit is operationeel gedelegeerd aan de algemeen directeur/gemeentesecretaris. De **algemeen directeur** is onder andere verantwoordelijk voor het stellen van kaders en het geven van sturing ten aanzien van de veiligheid van informatie, het sturen op risico's en het periodiek evalueren van het beleid. De algemeen directeur stelt met de **concerndirectie** (het directieteam) het gewenste niveau van informatieveiligheid vast voor de gemeente. Het college van burgemeester en wethouders is dus eindverantwoordelijk, de algemeen directeur en de concerndirecteur[9] met de portefeuille bedrijfsvoering zijn gemandateerd verantwoordelijk voor informatieveiligheid.

Binnen de gemeente Ede zijn **afdelingsmanagers** aangewezen als eigenaar van informatiesystemen en operationeel verantwoordelijk. Zij zijn verantwoordelijk voor de (informatie)veiligheid en de betrouwbaarheid van de informatieprocessen en systemen binnen hun afdeling. Daaronder valt onder andere classificatie van systemen op basis van risicoanalyses en het inrichten van maatregelen om beveiligingsrisico's te beheersen. Daarbij worden zij geacht medewerkers mee te nemen in de verantwoordelijkheid ten aanzien van informatieveiligheid in het dagelijkse werkproces.

De **Chief Information Officer (CIO)** is verantwoordelijk voor strategie en beleid en is daarnaast eigenaar van clusteroverstijgende systemen. De rol CIO is gecombineerd met de rol afdelingshoofd IPPM (Informatie, Proces- en Projectmanagement).

Er is volgens het strategisch beleid een **coördinator informatieveiligheid** voor de uitvoering van het beleid op het gebied van informatieveiligheid. Deze rol valt onder verantwoordelijkheid van de CIO / hoofd afdeling IPPM (Informatie, Project- en Procesmanagement). De coördinator informatieveiligheid draagt zorg voor het formuleren van het beleid en het opstellen en actualiseren van de informatieveiligheidsanalyses. Daarnaast houdt hij zich bezig met de prioritering van maatregelen uit risicoanalyses en de uitvoering van het actieplan informatieveiligheid[10].

Het strategisch beleid identificeert ook een **controller informatieveiligheid**, deze is o.a. verantwoordelijk voor het periodiek toetsen van de naleving, werking en effectiviteit van maatregelen. Daarnaast controleert hij op voortgang op het actieplan en op de actualisatie van het beleid en risico-analyses. Deze rol valt onder verantwoordelijkheid van de Concerncontroller.

De **Functionaris Gegevensbescherming (FG)** informeert en adviseert over de verplichtingen die de gemeente heeft voortvloeiende uit de AVG en andere wet- en regelgeving omtrent gegevensbescherming. De FG ziet toe op de naleving hiervan met inbegrip van het toewijzen van verantwoordelijkheden, bewustwording en opleiding van medewerkers van de gemeente die persoonsgegevens verwerken. De **privacybeheerder** is verantwoordelijk voor de uitvoering en naleving van het privacybeleid en de AVG.

9 De rol van de concerndirecteur is niet geformuleerd in de desbetreffende uitgangspunten in het strategisch beleid. In praktijk is er wel een rol en zijn er verantwoordelijkheden voor de concerndirecteur, omdat deze gemandateerd is.

10 In de praktijk wordt deze rol benoemd als de rol van de CISO (Chief Information Security Officer).

De afdeling **IPPM** houdt zich bezig met ontwikkeling en strategie. Dat omvat het op- en bijstellen van de strategische richting voor de informatievoorziening, adviseren over de informatievoorziening en het *voorbereiden* en *managen* van veranderingen. Voor zowel informatiemanagement, procesmanagement als projectmanagement geldt dat informatiebeveiliging een factor is waar rekening mee gehouden moet worden.

Afdeling **BIAS** (Beheer Infrastructuur, Applicaties en Services) draagt zorg voor beheer, het leveren van diensten en het *uitvoeren* van veranderingen. De afdeling verzorgt onder andere het technische (wijzigings-)beheer van databases, bedrijfsapplicaties en kantoorautomatiseringshulpmiddelen. Zij zijn medeverantwoordelijk voor alle technische aansluitingen op andere ketenpartners en landelijke voorzieningen én voor de implementatie van ICT-technische beveiligingsmaatregelen. Verantwoording over het gevoerde beheer van de getroffen beveiligingsmaatregelen wordt aan de procesverantwoordelijken voor (informatie)systemen afgelegd.

Er zijn volgens het strategisch beleid decentrale **beveiligingsbeheerders** die voor het toegewezen deelgebied verantwoordelijk zijn voor de activiteiten die noodzakelijk zijn vanuit dit beleid. Deze beveiligingsbeheerders worden in ieder geval benoemd bij de afdeling BIAS (Beheer Infrastructuur, Applicaties en Services), P&O (Personeel & Organisatie), H&S (Huisvestiging & Services) en DIV (Documentaire Informatievoorziening) en daarnaast benoemd voor een aantal specifieke aandachtsgebieden waar specifieke beveiligingsnormen van toepassing zijn: DigiD, BRP (Basisregistratie Personen), WD (Waardedocumenten), BAG (Basisregistratie Adressen en Gebouwen) en SUWI (Structuur Uitvoeringsorganisatie Werk en Inkomen). Daarnaast kent ieder cluster een beveiligingsbeheerder.

Vanuit de afdeling BIAS is een **beveiligingsbeheerder ICT** verantwoordelijk voor het beheer, de coördinatie en advies ten aanzien van de informatieveiligheid van specifieke gegevensverzamelingen.

Namens afdeling BIAS sluit de beveiligingsbeheerder ICT aan bij het **informatieveiligheidsoverleg**. IPPM en BIAS werken samen; de CIO / afdelingshoofd IPPM heeft geen hiërarchische relatie tot BIAS. IPPM, BIAS en de CIO vallen binnen de concerndirectie portefeuille bedrijfsvoering.

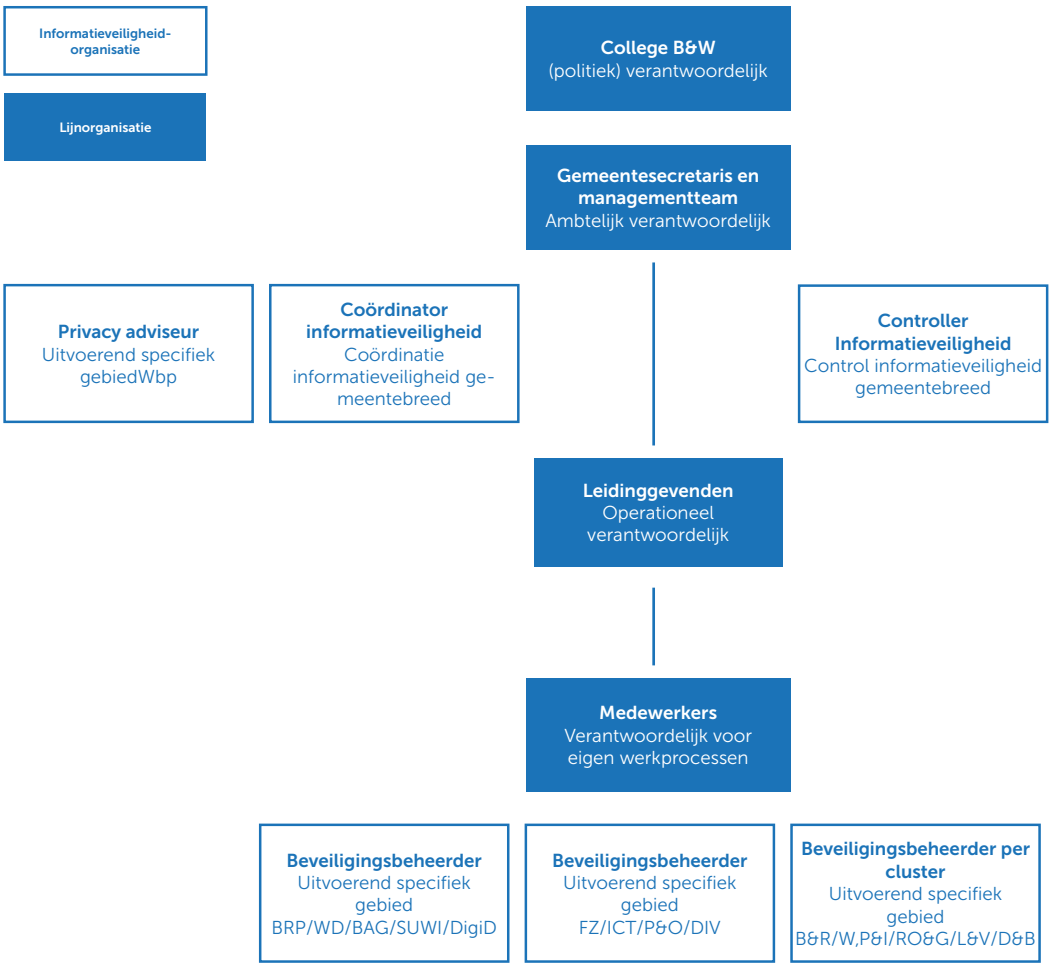
Onderstaande afbeelding uit het Gemeentebreed Informatieveiligheidsbeleid geeft een aantal belangrijke rollen[11] ten aanzien van informatieveiligheid schematisch weer. Er wordt onderscheid gemaakt tussen de informatieveiligheidsorganisatie en de lijnorganisatie.

2.1.2 Uitgangspunten en scope

Het strategisch beleid is gericht op de hele gemeentelijke organisatie en beschrijft op strategisch en tactisch niveau welke uitgangspunten ten aanzien van de informatieveiligheid gelden voor alle domeinen van de gemeente Ede.
De scope van het strategisch beleid omvat alle gemeentelijke informatieprocessen, hieronder vallen alle ambtelijke en bestuurlijke informatieprocessen. Het beleid heeft betrekking op de verwerking, uitwisseling en opslag van alle (digitale) informatie en bevat uitgangspunten voor handelen ten aanzien van informatieprocessen met keten- en uitvoeringspartners.
Vanuit het strategisch beleid zijn voor de organisatie van informatieveiligheid een aantal uitgangspunten geformuleerd. In de paragraaf hierboven zijn de rollen en verantwoordelijkheden beschreven. Een relevante selectie van overige uitgangspunten is hieronder overgenomen:

- Er behoort een actieplan te zijn voor het coördineren van verbeteracties voor de informatieveiligheid, als leidraad voor het werk van de beveiligingsorganisatie.
- Er moet periodiek overleg plaatsvinden tussen de coördinatoren en de beheerders.

11 De rol van CIO wordt in dit schema niet geduid.



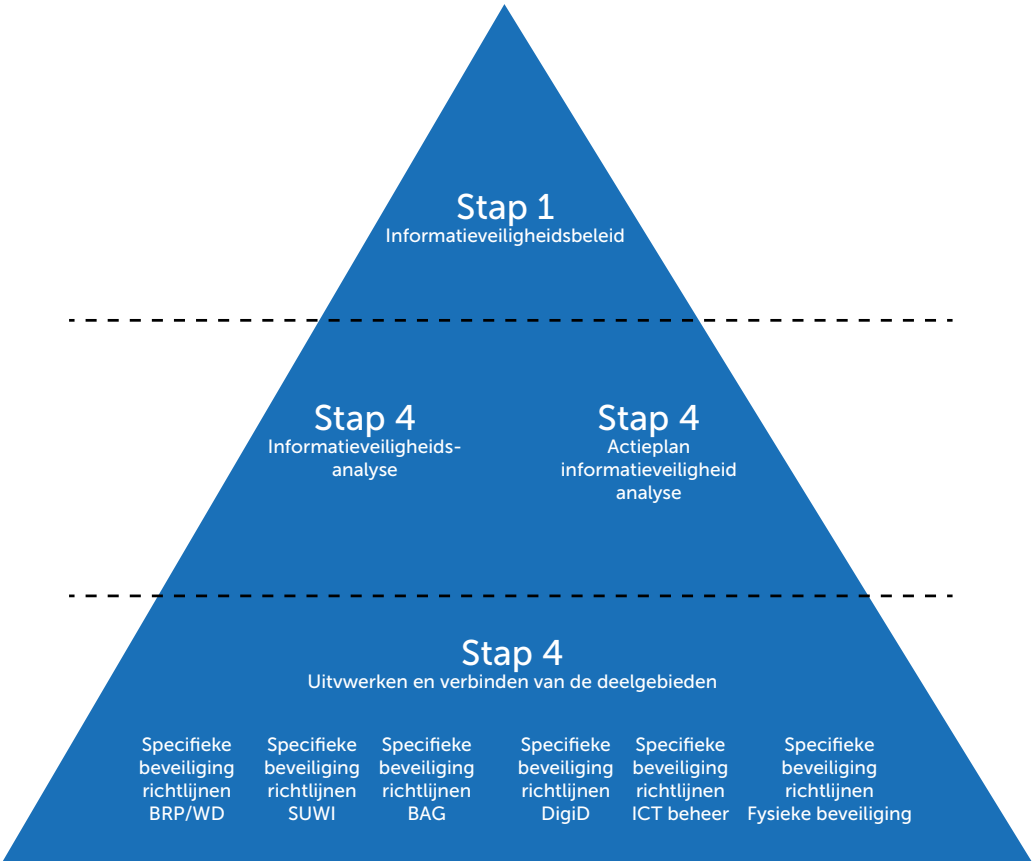
Figuur 1: Functies en rollen in informatieveiligheidsorganisatie, uit Gemeentebreed Informatieveiligheidsbeleid 2017 (pagina 21).

Binnen dit overleg wordt de voortgang van het actieplan informatieveiligheid besproken, geëvalueerd en geactualiseerd.

- De procesverantwoordelijke leidinggevende heeft de primaire verantwoordelijkheid voor de controle op en evaluatie van de naleving.
- De kwaliteit van de informatieveiligheid behoort periodiek via audits te worden vastgesteld, in de P&C-cyclus moet hierover worden gerapporteerd.
- De wijze van toekennen van toegangsrechten behoort te worden aangepast (gebaseerd op iemands functie) en moet periodiek worden toegezien/gecontroleerd worden op de verstrekte toegangsrechten.

2.1.3 Opbouw beleid

De gemeente onderscheidt in het strategisch beleid een aantal niveaus van informatieveiligheid. Het eerste niveau, het organisatiebreed informatieveiligheidsbeleid, schetst de uitgangspunten, normen en kaders voor de gemeentelijke informatieprocessen. De tweede laag is gericht op de implementatie en toetst het beleid middels een risico-inventarisatie aan de praktijksituatie. Ook worden risico's gewogen en geprioriteerd en eventueel van maatregelen voorzien. Het laagste niveau is gericht op specifieke onderdelen, zoals processen en applicaties.



Figuur 2: De informatieveiligheidspiramide, uit Gemeentebreed Informatieveiligheidsbeleid 2017

2.1.4 Uitwerking strategisch beleid en toetsing

Het strategisch beleid wordt uitgewerkt in de onderliggende 'informatieveiligheidsanalyse' en 'actieplannen informatieveiligheid' waarin de implementatie van het beleid is opgenomen. Daaronder liggen specifieke beleidsstukken en procesbeschrijvingen.

2.1.4.1 Informatieveiligheidsanalyse

Het strategisch beleid schrijft voor dat de Informatieveiligheidsanalyse met het actieplan informatieveiligheid door de concerndirectie worden vastgesteld. Hierin wordt aangegeven op welke wijze het beleid uitgevoerd zal worden.
De kernelementen in de informatieveiligheidsanalyse zijn:

- Beschrijving van het huidige niveau van informatieveiligheid en de mate waarin aan de beveiligingseisen en -prioriteiten uit het strategische beleidsdocument en aan alle onderdelen van de informatieveiligheidsanalyse wordt voldaan. Recente ontwikkelingen worden ook beschreven, zoals het in productie nemen van een nieuw informatiesysteem of technische infrastructuur die gevolgen kunnen hebben voor het beveiligingsniveau.
- Een analyse ten aanzien van de bedrijfsprocessen op gebied van de ICT-omgeving om de afhankelijkheden en risico's te bepalen. Naar aanleiding van deze analyse zijn minimaal de volgende aandachtspunten voor het plan onderkend:
  - Risico's die onvoldoende af te dekken zijn door maatregelen.
  - Risico's die zijn gerelateerd aan de kritische bedrijfsprocessen en/of (informatie) systemen.
  - Een overzicht van verbeterpunten, aangevuld met een kostenaanduiding voor uitvoering en de wijze en termijn waarop zij uitgevoerd zullen worden.
  - Een overzicht van de aanwezige (informatie)systemen waarbij is aangegeven welke systemen bedrijfskritisch zijn. Dit overzicht kan als bijlage aan het uitvoeringsplan worden toegevoegd.

2.1.4.2 Actieplan informatieveiligheid

In het onderliggende Actieplan informatieveiligheid is de implementatie van het beleid opgenomen. Het Actieplan wordt opgesteld op basis van: de huidige situatie, de vereisten vanuit het strategisch beleid, de BIG en de Informatieveiligheidsanalyse. Het Actieplan Informatieveiligheid bevat de concrete geprioriteerde acties volgend uit de informatieveiligheidsanalyse. Aan de hand van het Actieplan wordt de voortgang op de realisatie van de afgesproken acties en maatregelen gemonitord en besproken in het informatieveiligheidsoverleg.

2.1.4.3 Borging beleid

Om het beleid te borgen heeft de gemeente een Plan, Do, Check, Act (PDCA) cyclus in haar beleid opgenomen. Het informatieveiligheidsbeleid, inclusief de visie op informatieveiligheid, wordt binnen een cyclus van vier jaar bijgesteld. De Informatieveiligheidsanalyse, de toets aan de praktijk, vindt elke 1 tot 2 jaar plaats. Het Actieplan informatieveiligheid wordt twee tot vier keer per jaar bijgesteld.

Over de beoordeling van de naleving staat in het beleid het volgende opgenomen:

"De procesverantwoordelijke leidinggevenden zorgen voor de controle en evaluatie op de naleving van wettelijke voorschriften van het informatieveiligheidsbeleid. Zij beoordelen of alle beveiligingsprocedures binnen hun verantwoordelijkheidsgebied correct worden uitgevoerd en of hun processen en (informatie)systemen voldoen aan relevante wet- en regelgeving, beveiligingsbeleid, normen en andere beveiligingseisen. De procesverantwoordelijken zien erop toe dat de naleving van technische normen wordt gecontroleerd door productiesystemen te onderzoeken op de effectiviteit van de geïmplementeerde beveiligingsmaatregelen, bijvoorbeeld door het laten uitvoeren van een security scan. Daarnaast worden controles uitgevoerd door externe auditors (bv BRP-, SUWI- en BAG-audit en de externe accountant) of door middel van zelfevaluaties.
Naast de controle op de naleving van technische normen dienen de procesverantwoordelijkheden erop toe te zien dat medewerkers de maatregelen die worden getroffen aan de zachte kant, ten behoeve van alertheid, naleven. Hierbij gaat het onder meer om het begeleiden van bezoekers, het vergrendelen van beeldschermen, het opbergen van vertrouwelijke documentatie, veilig omgaan met (mobiele) apparatuur en het melden van incidenten."[12]

2.2 Tactisch en operationeel beleid

Naast het in de vorige paragraaf behandelde strategisch beleid zijn er diverse onderliggende beleidsstukken en procesbeschrijvingen van toepassing op het gebied van informatieveiligheid. Tactische en operationele beleidstukken[13] zijn hieronder beschreven op organisatorisch, proces-, medewerkers- en technisch niveau.

2.2.1 Organisatorisch en procesniveau

Op organisatorisch niveau zijn er over diverse onderwerpen beleidsregels en processen vastgesteld. Onder andere op gebied van incidenten, bedrijfscontinuïteit, het voortbrengingsproces[14] en het aansluitbeleid Gezamenlijke elektronische Voorzieningen SUWI (GeVS) die hieronder worden uiteengezet zoals beschreven in het beleid.

12 Gemeentebreed Informatieveiligheidsbeleid Ede (2017), pagina 54.
13 Ten behoeve van de leesbaarheid worden niet alle onderliggende beleidsstukken inhoudelijk behandeld.
14 Het voortbrengingsproces is een proces ten behoeve van de ontwikkeling van of het doorvoeren van wijzigingen in informatiesystemen.

2.2.1.1. Incidenten

De gemeente Ede definieert een beveiligingsincident als een gebeurtenis waarbij de mogelijkheid bestaat dat de beschikbaarheid, de integriteit of de vertrouwelijkheid van informatie of informatiesystemen in gevaar is of kan komen. Hierbij staat beschikbaarheid voor de garanties over het afgesproken niveau van dienstverlening en over de toegankelijkheid en bruikbaarheid van informatie(systemen) op de afgesproken momenten. Integriteit staat voor de juistheid, volledigheid en tijdigheid van informatie(systemen). Vertrouwelijkheid heeft betrekking op exclusiviteit van informatie en de privacybescherming. Hiermee wordt bedoeld dat uitsluitend gemachtigden toegang mogen hebben tot informatie(systemen).

Vanuit het strategisch beleid heeft Ede het uitgangspunt gesteld een actief beleid te voeren op het melden van beveiligingsincidenten. Er is een procedure voor het rapporteren van beveiligingsgebeurtenissen vastgesteld, in combinatie met een reactie- en escalatieprocedure voor incidenten, waarin de handelingen worden vastgelegd die moeten worden genomen na het ontvangen van een rapport van een beveiligingsincident. Dit betreft het Calamiteitenplan gemeente Ede (2020), de Handleiding consignatiedienst BIAS (2018) en de Procesbeschrijving major incident (2018). In het Calamiteitenplan zijn instructies, informatie en hulpmiddelen opgenomen voor alle mogelijke soorten calamiteiten: gebeurtenissen waarbij de voortgang van de kritische bedrijfsprocessen van de gemeente ernstig worden verstoord, boven de aanvaardbare uitvalsduur. De Handleiding consignatiedienst BIAS gaat over de beschikbaarheid van ICT buiten de reguliere support tijden, ook in geval van crisis. De consignatiedienst regelt het beschikbaar zijn van collega's op oproepdienst.
De Procesbeschrijving Major Incident richt zich vooral op grote incidenten waarbij de dienstverlening van de informatievoorziening ernstig wordt verstoord en de rol van BIAS daarin.

2.2.1.2 Bedrijfscontinuïteitsbeleid en bedrijfscontinuïteitshandboek

Bedrijfscontinuïteitsmanagement (BCM) is gericht op het voorkomen van en de reactie op calamiteiten waardoor de bedrijfsvoering en dienstverlening van de gemeente negatief wordt beïnvloed. De gemeente Ede heeft een Bedrijfscontinuïteitsbeleid dat in mei 2020 door het directieteam is vastgesteld. Het beheersen van risico's vraagt om technische, procesmatige en organisatorische maatregelen. In het beleid worden de beleidsprincipes beschreven.
In het handboek wordt beschreven hoe bedrijfscontinuïteit als managementproces wordt geïmplementeerd, aan de hand van een Plan, Do, Check, Act (PDCA) cyclus.

De gemeente Ede hanteert vijf beleidsprincipes met betrekking tot bedrijfscontinuïteit:
- bedrijfscontinuïteitsmanagement is een continu proces;
- bedrijfscontinuïteitsmanagement is risico-gebaseerd;
- bewust verantwoordelijkheid nemen voor bedrijfscontinuïteit (iedereen die werkzaam is binnen de gemeente dient een bepaald basis bewustzijnsniveau te hebben);
- bedrijfscontinuïteit 'by design' (vanaf de start van elk nieuw project, proces, locatie, etc.);
- informatiebeveiliging & privacy dienen ook tijdens een calamiteit te worden gewaarborgd.

2.2.1.3 Voortbrengingsproces

De gemeente heeft een voortbrengingsproces voor Informatievoorziening[15] voor het doorvoeren van veranderingen. In het geval van een grote verandering zoals de aanschaf en implementatie van een nieuwe applicatie geldt dat er een haalbaarheidsonderzoek wordt gedaan en een projectvoorstel wordt geschreven waarin geldend beleid kan worden toegepast en gecontroleerd. In het voortbrengingsproces is er daarmee ook aandacht voor beveiligingseisen. Een van de vaste stappen in het proces is het betrekken van de privacy officer en CISO voor review van het projectvoorstel, zodat aandachtpunten voor privacy (zoals een Privacy impact Analyse) of specifieke beveiligingsmaatregelen (conform BIO) aandacht hebben. De security officer neemt daarnaast deel aan het Change Advisory Board (CAB) en levert een bijdrage aan de impact en risicoanalyses. Ook kleine veranderingen

15 Voortbrenging IV toepassingen procesbeschrijving (versie 05-06-2023)

worden langs het CAB geleid[16]. Een ander onderdeel van het voortbrengingsproces dat met informatieveiligheid te maken heeft is het Enterprise architectuuroverleg en met name de deelname van een Security Architect in dit architectuuroverleg.

2.2.14 Aansluitbeleid GeVS (Suwinet)

De gemeente Ede maakt bij het uitvoeren van de Participatiewet en bij het leggen van een loonbeslag door de gemeentelijke deurwaarder gebruik van de Gezamenlijke elektronische Voorzieningen SUWI (GeVS)[17]. De gemeente Ede heeft in 2018 een aansluitbeleid opgesteld voor Suwinet. In het beleid wordt het belang daarvan geduid: "Suwinet maakt het mogelijk om veel en vertrouwelijke werk- en inkomensgerelateerde gegevens van burgers in te zien. Daarmee is het een waardevolle gegevensbron maar ook een grote risicobron met betrekking tot de privacy van burgers."[18] Het gebruik van Suwinet is gebonden aan een aantal beveiligingsmaatregelen om deze risico's tot een minimum te beperken.

2.2.2. Medewerkersniveau

De gemeente Ede heeft, naast het uitwerken van verschillende rollen en verantwoordelijkheden, ook algemene uitgangspunten voor het personeel geformuleerd. Deze uitgangspunten en uitwerking staan onder andere benoemd in de gedragscode van de gemeente Ede. Hierin staat dat er wordt verwacht dat er integer en veilig met voorzieningen wordt omgegaan en de vertrouwelijkheid van gegevens in acht wordt genomen. De gedragscode wordt ondertekend.

Verder is de leidinggevende verantwoordelijk voor het juist afhandelen van de beveiligingsaspecten van het aangaan, wijzigen en beëindigen van een dienstverband of een overeenkomst met externen. Ook bepaalt de leidinggevende welke rol(len) de medewerker moet vervullen en welke autorisaties voor het raadplegen, opvoeren, muteren en afvoeren van gegevens moeten worden verstrekt. Bij inbreuk op de beveiliging gelden voor medewerkers de gebruikelijke disciplinaire maatregelen, zoals onder meer genoemd in het Ambtenarenreglement en gemeentelijke regelingen. Regels die volgen uit dit beleid en andere gemeentelijke regelingen gelden ook voor externen, die in opdracht van de gemeente werkzaamheden uitvoeren[19].

Ook zijn een aantal voorwaarden in het strategisch beleid geformuleerd. Zo moet iedere medewerker van de gemeente Ede de eed/belofte afleggen en worden alle medewerkers geacht te handelen conform de voorschriften zoals vermeld in het integriteitsprotocol[20]. Alle nieuwe medewerkers moeten eenmalig een Verklaring Omtrent Gedrag (VOG) overleggen.

Bij indiensttreding wijst de leidinggevende van de werknemer op de aanwezigheid van eventueel aanvullende, specifieke gedragsregels ten aanzien van een informatiesysteem, cluster of afdeling. Dit laatste gebeurt in ieder geval bij de Basisregistratie Personen (BRP), Waardedocumenten en SUWI. Voor 'externen' geldt dat zij wanneer zij toegang hebben tot vertrouwelijke informatie een geheimhoudingsverklaring tekenen, aanvullend op de regels die voor interne werknemers gelden.

Nieuwe medewerkers krijgen een training in procedures die binnen de gemeente of het cluster gelden voor informatieveiligheid. Zo krijgen nieuwe medewerkers tijdens hun introductie een presentatie over iBewustzijn te zien. Hierin wordt onder andere het belang

16 Het proces van voor het doorvoeren van kleine wijzigingen is in het onderzoek niet verder verkend.
17 GeVS wordt ook wel Suwinet genoemd.
18 Aansluitbeleid GeVS (Suwinet) (2018), pagina 2.
19 Hoe deze regels worden geborgd is niet onderzocht.
20 Gedragscode integriteit 2022

van informatieveiligheid en privacy in het werk besproken. Het beleid van de gemeente stelt ook dat een informatieveiligheidstraining regelmatig moet worden herhaald om het beveiligingsbewustzijn op peil te houden. In het beleid van de gemeente is in het kader van beveiligingsbewustzijn opgenomen dat de algemeen directeur/gemeentesecretaris, het MT en de leidinggevenden de algehele communicatie en bewustwording rondom informatieveiligheid bevorderen. Ook schrijft het beleid voor dat in werkoverleggen periodiek aandacht wordt geschonken aan informatieveiligheid.

In de gedragscode van de gemeente Ede staat een aantal algemene regels voor het gebruik van de verstrekte mobiele bedrijfsmiddelen zoals een mobiele telefoon. De gemeente heeft ook een gebruikersovereenkomst opgesteld voor het gebruik van mobiele apparaten (devices) en thuiswerkfaciliteiten (2021) waarin de gebruiksvoorwaarden zijn opgenomen voor deze middelen. In deze overeenkomst zijn ook een aantal voorwaarden ten aanzien van informatieveiligheid opgenomen.

2.2.3 Technisch niveau

De gemeente heeft ook op technisch niveau beveiligingsbeleid. De afdeling BIAS is samen met IT-leveranciers voor een belangrijk deel verantwoordelijk voor de technische invulling van het informatiebeveiligingsbeleid. Een deel van dit beleid is vastgelegd in het strategisch beleid, waaronder ten aanzien van controle en logging, beveiligingseisen voor systemen en cryptografische beveiliging. De gemeente heeft daarnaast aansluitvoorwaarden voor cloudgebaseerde diensten opgesteld. Ook is informatieveiligheid een belangrijk onderdeel in het voortbrengingsproces van de gemeente. Onderstaand worden belangrijke elementen beschreven zoals in de beleidsstukken staan opgenomen, zonder uitputtend te zijn.

2.2.3.1 Algemene technische maatregelen

De gemeente heeft een aantal algemene technische uitgangspunten opgesteld ten aanzien van de communicatie- en bedieningsprocessen. Zo wordt bij het openen en opslaan van bestanden automatisch gecontroleerd op virussen en malware. Ook inkomende en uitgaande e-mails worden gecontroleerd. Er wordt gebruik gemaakt van antivirussoftware en het is niet toegestaan om programma's te gebruiken en installeren op de gemeentelijk voorzieningen wanneer dezen niet geautoriseerd zijn. Updates ten behoeve van de veiligheid worden zo spoedig mogelijk doorgevoerd. Het netwerk bevat segmentatie en wordt gemonitord en beheerd zodat aanvallen, storingen of fouten ontdekt en hersteld kunnen worden.

2.2.3.2 Controle en logging

De gemeente heeft in haar beleid uitgangspunten voor controle en logging opgenomen. Het gebruik van informatiesystemen, alsmede uitzonderingen en informatiebeveiligingsincidenten, wordt vastgelegd in logbestanden. Daarbij maakt de gemeente een risicoafweging en moet worden voldaan aan wettelijke relevante eisen zoals opgenomen in bijvoorbeeld de BRP en SUWI. Zaken die worden gelogd, zijn bijvoorbeeld het type gebeurtenis (zoals back-up/restore, reset wachtwoord), handelingen met een speciale bevoegdheden, (poging tot) ongeautoriseerde toegang, systeemwaarschuwingen en (poging tot) wijziging van de beveiligingsinstellingen. Het beleid stelt dat er maatregelen worden getroffen om te verzekeren dat gegevens over logging beschikbaar blijven en niet gewijzigd kunnen worden door een gebruiker of systeembeheerder. Het beleid stelt dat de bewaartermijnen in overeenstemming zijn met de wettelijke eisen.

2.2.3.3 Beveiligingseisen voor (informatie)systemen

Het strategisch beleid schrijft voor dat beveiligingseisen vanaf aanvang in het ontwerpproces worden meegenomen bij de ontwikkeling van (informatie)systemen. Ook bij standaard systemen en onderhoud van (informatie)systemen moet informatieveiligheid een vast aandachtspunt zijn. De gemeente identificeert daarbij de volgende aspecten:

- "beveiligingseisen zijn zoveel mogelijk onderkend, gedocumenteerd en goedgekeurd

voordat een (informatie)systeem wordt ontwikkeld of aangekocht;
- benodigde beveiligingsmaatregelen met betrekking tot audittrails en validatie van invoergegevens, interne verwerking en uitvoergegevens zijn, waar mogelijk, ingebouwd;
- voor (informatie)systemen die vertrouwelijke of privacygevoelige gegevens bevatten, kunnen aanvullende beveiligingsmaatregelen nodig zijn die, op basis van classificatie en risicoanalyse, zijn vastgesteld;
- privacy by design en privacy by default[21];
- bij extern toegankelijke applicaties, bijvoorbeeld webapplicaties, wordt extra aandacht besteed aan het voorkomen van ongeautoriseerde toegang."

In het voorbrengingsproces van de gemeente is, zoals al beschreven, aandacht voor het voldoen aan beleid en kaders, waaronder beveiligingseisen. Bijzonderheden uit het voortbrengingsproces:
- Voor clusteroverstijgende informatiesystemen (generieke informatiesystemen) worden een aantal schriftelijke afspraken gemaakt met betrekking tot de voorwaarden waarbinnen deze gebruikt mogen worden.
- Voor relevante contracten met derden wordt eveneens een aantal specifieke afspraken gemaakt met betrekking tot het niveau van dienstverlening, inhuur van derden, toegang en aanbestedingen.
- Er wordt niet getest met vertrouwelijke data.

2.2.3.4 Cryptografische beveiliging

Cryptografische beveiliging is een beveiligingsmaatregel waarbij gegevens versleuteld worden. De gemeente past cryptografische systemen en technieken toe bij systemen die met vertrouwelijke en privacygevoelige gegevens werken en die onvoldoende door andere maatregelen kunnen worden beveiligd. De gemeente tracht bij de implementatie van nieuwe systemen cryptografische maatregelen toe te passen, onder andere door gebruik te maken van PKI-certificaten.

2.2.3.5 Leveranciersmanagement en uitbesteding

Met betrekking tot het deel van het systeemlandschap dat door externe leveranciers wordt geleverd heeft de gemeente ook beleid geformuleerd. Het strategisch informatiebeveiligingsbeleid schetst de belangrijkste uitgangspunten waarmee rekening moet worden gehouden bij uitbesteding, zoals voorwaarden met betrekking tot het uitvoeren van IT audits, het afgeven van een Third Party Memorandum, het uitvoeren van penetratietesten en (door de leverancier aangegeven) toereikende technische en organisatorische maatregelen met betrekking tot beveiliging.

De gemeente hanteert een algemeen inkoopbeleid en (algemene) voorwaarden zoals het GIBIT 2020, een landelijke standaard voor de inkoop van IT-diensten. Daarnaast heeft de gemeente ook specifieke aansluitvoorwaarden voor Cloudgebaseerde diensten opgesteld[22] waarin wordt ingegaan op de beveiligingsrichtlijnen voor (web-gebaseerde) diensten die extern toegankelijk zijn of worden gesteld door de gemeente. Deze voorwaarden worden meegenomen bij de ontwikkeling of aanschaf van systemen en diensten. Er worden verschillende maatregelen uitgewerkt die zijn gesplitst in een aantal categorieën: Algemeen, Koppelingen, Configuratie, Procedureel, Certificering en Uitsluitingen.

21 Men spreekt van Privacy by default wanneer de standaardinstellingen van programma's, websites, diensten of apparaten zodanig zijn afgesteld dat maximale privacy wordt betracht. Privacy by design geeft aan dat bij het ontwikkelen van informatiesystemen en diensten de bescherming van persoonsgegevens al vanaf het begin wordt omarmd en verankerd in het systeem of in de dienst.

22 Aansluitvoorwaarden Cloudgebaseerde diensten (versie 11-03-2022)

3. Uitvoering van het beleid: de praktijk

In het vorige hoofdstuk is beschreven welk beleid er aanwezig is binnen de gemeente Ede op het gebied informatieveiligheid, en wat het beleid op hoofdlijnen inhoudt. In dit hoofdstuk wordt de uitvoering van het beleid in praktijk beschreven aan de hand van dezelfde niveaus: organisatie en proces, bestuurlijk niveau, technisch niveau en medewerkersniveau. De inhoud van dit hoofdstuk is gebaseerd op de resultaten van de documentstudie, de uitkomsten van de interviewgesprekken en de casusbesprekingen.

3.1 Organisatie en proces

3.1.1 Strategisch beleid

Het informatiebeveiligingsbeleid uit 2017 is bekend bij medewerkers in de gemeente Ede die in het kader van dit onderzoek geïnterviewd zijn. Het beleid is echter verouderd vanwege het feit dat het gebaseerd is op de verouderde Baseline Informatiebeveiliging Gemeente. Het beleidsuitgangspunt dat er een vierjarige cyclus is van bijstelling is tevens niet gevolgd.
Er zijn tijdens het onderzoek initiatieven gevonden om het beleid te herzien. Zo is in 2020 een concept informatiebeveiligingsbeleid 2021-2023[23] opgesteld, dit beleid is echter niet vastgesteld. In mei 2022 is een discussienota opgesteld voor het directieteam. Als aanleiding voor de discussienota wordt enerzijds een benodigde herbeoordeling van het beleid genoemd, anderzijds wordt opgemerkt dat de organisatorische rollen en verantwoordelijkheden in het huidige beleid onvoldoende concreet zijn ingevuld. De discussienota is als bespreekstuk ingediend en legt een drietal ambitieniveaus voor: basis, ambitieus en optimaal. Aan het directieteam werd het ambitieniveau ambitieus geadviseerd. De discussienota heeft niet geleid tot een formeel besluit of vastgesteld ambitieniveau. Wel is naar aanleiding van deze bespreking gevraagd om het voorgestelde ambitieniveau verder uit te werken als basis voor het nieuwe beleid.

Uit de interviews is gebleken dat de gemeente ervoor heeft gekozen in eerste instantie een technisch fundament te leggen. Er is geïnvesteerd in technische maatregelen voor een basisweerbaarheid, maar op organisatorische componenten van informatiebeveiliging is nog een ontwikkeling te maken. De wens is om in het nieuwe beleid duidelijkheid te scheppen over eigenaarschap in verantwoordelijkheden en processen. Een verklaring die wordt gegeven voor het verouderde beleid is dat er in de organisatie veel hulp gevraagd wordt bij operationele vraagstukken waardoor de CISO niet goed toekomt aan de strategische taken.
In de interviews hebben medewerkers aangegeven in praktijk wel veelal volgens BIO-normen werken, al is het formele beleid nog op de verouderde BIG gebaseerd.

3.1.2 Actieplan en informatieveiligheidsanalyse

Voor de uitvoering van het informatieveiligheidsbeleid werkt de gemeente met actieplannen of informatieveiligheidsplannen. In het actieplan voor 2018 wordt verwezen naar de resultaten uit de informatieveiligheidsanalyse, waarmee een toetsing plaats heeft gevonden tussen het beleid en de praktijk en het bijbehorende risico daarbij.

23 Volgens jaarrapportage informatiebeveiliging 2020.

In 2019 is een plan gemaakt voor het eerste half jaar, waarin een aantal activiteiten is opgenomen. Deze zijn niet afgeleid van concrete BIG- of BIO-normen maar sluiten aan bij de "basis op orde"-insteek van het jaarplan van de afdelingen IPPM en BIAS. In dat plan wordt aangegeven dat medio 2019 een actieplan gereed is dat in lijn is met de BIO, waarbij de ambitie was om een plan te maken dat tot eind 2020 doorloopt.

Het volgende actieplan is van maart 2020 en is een meerjarenplan voor informatieveiligheid (2020-2023). Dit informatiebeveiligingsplan is er op gericht om de BIO tussen 2020 en 2022 geheel in de gemeente Ede te implementeren. Hierbij is gekozen voor een aanpak in vier onderdelen: 1) GAP-analyse (per BIO-maatregel vaststellen in hoeverre deze al is geïmplementeerd) 2) Bepalen urgentie (waarbij bekeken is of er maatregelen waren die directe urgentie hadden), 3) Clusteren van maatregelen in logische groepen (veel maatregelen zijn uitwerkingen van diverse aspecten van hetzelfde onderwerp) en 4) Plannen van de maatregelen. In het plan zijn de verschillende aandachtsgebieden en maatregelen beschreven en is een planning opgenomen voor het uitvoeren van de werkzaamheden tot en met eind 2022. Er wordt in het plan niet verwezen naar een informatieveiligheidsanalyse. Een organisatiebrede informatieveiligheidsanalyse is niet uitgevoerd: wel zijn er op basis van waargenomen risico's aanvullende maatregelen getroffen en/of later geplande handelingen naar voren gehaald. Ook is er door de CISO('s) een Omgevingsbeeld opgesteld in 2022. Dit Dreigingsbeeld 2022 gaat onder andere in op vormen van digitale criminaliteit en hoe de organisatie hier mee om gaat en mee om zou moeten gaan. Het stuk is in maart 2022 aangeboden aan het DT. Het is geen brede informatieveiligheidsanalyse die over álle factoren gaat, opgesteld met lijnmanagement en andere betrokkenen, leidend tot het nemen van maatregelen. Het structureel uitvoeren van periodiek terugkerende informatieveiligheidsanalyse met de juiste betrokkenen aan tafel, is als zodanig niet aangetroffen.

Voor 2021 is een kort plan gevonden voor het tweede halfjaar, waarin een korte update wordt gegeven over de reeds uitgevoerde activiteiten. Een planning voor de overige uit te voeren activiteiten is niet opgenomen. Voor het jaar 2022 is een uitgebreider informatiebeveiligingsplan opgesteld, waarin reguliere taken en verbetertrajecten (inclusief streefdatum voor gereedkomen) zijn opgenomen. Deze verbetertrajecten zijn onder andere een nieuw informatieveiligheidsbeleid vast laten stellen, een plan van aanpak voor structurele bewustzijnstraining en activiteiten, het versterken van de PDCA-cyclus en de overlegstructuren, veiliger inloggen met twee-factor-authenticatie, beheer van mobiele apparaten en betere centrale logging. Het is niet bekend of het plan voor 2022 mede is gebaseerd op de informatieveiligheidsanalyse zoals beschreven in het beleid.

In een aantal plannen wordt een toegelicht wat de stand van zaken is omtrent initiatieven. Er zijn echter geen rapportages gevonden waarin specifiek wordt aangegeven in hoeverre de plannen zijn uitgevoerd. Uit het onderzoek blijkt dat bepaalde initiatieven die in de plannen zijn beschreven wel zijn afgerond, zoals het inloggen met twee-factor-authenticatie, en dat andere nog moeten worden uitgevoerd, zoals een nieuw informatiebeveiligingsbeleid vast laten stellen.

3.1.3 Rollen en verantwoordelijkheden

De rol van coördinator informatieveiligheid zoals beschreven in het beleid komt in de praktijk overeen met de rol van Chief Information Security Officer (CISO)[24]. De CISO-rol is in 2020 formeel gemaakt, hiervoor zijn tevens aanpassingen gedaan in het functiehuis[25]. De rol van

24 De CISO-rol is in het beleid niet beschreven

25 Jaarrapportage informatiebeveiliging 2020

beveiligingsbeheerder ICT, zoals beschreven in het beleid, komt in praktijk overeen met de rol van Information Security Officers (ISO) en Technical Security Officer (TISO).
De uitvoering van het informatiebeveiligingsbeleid is deels[26] belegd bij de CISO, ISO en TISO. Zij zijn onder andere verantwoordelijk voor het oppakken van strategische en procedurele vraagstukken en het opstellen van richtlijnen. De meer strategische taken, het brede gemeentelijke beleid, ligt bij de CISO en daarmee de afdeling IPPM. De ISO en Technical Security Officer, vanuit de afdeling BIAS, zijn meer gericht op de taken in de uitvoering en het opzetten van protocollen en handboeken, zo blijkt uit de interviews. De CIO is hoofd van IPPM en geeft richting aan de afdeling BIAS. Er is echter geen hiërarchische relatie vanuit de CIO richting BIAS. De CISO valt hiërarchisch onder de CIO, maar de rol van de CISO heeft daarbij een grotendeels onafhankelijke rol richting directie en B&W ten aanzien van risicosignalering en incidentenoplossing. De operationele verantwoordelijkheid voor de informatiebeveiliging ligt bij de proceseigenaren (afdelingsmanagers). Zij worden daarin geadviseerd (en gecontroleerd) door de CISO en (T)ISO's.

Uit de casusbespreking en interviews is gebleken dat er meer werk ligt op gebied van informatieveiligheid dan dat er op dit moment door de daarvoor aangewezen personen uit te voeren is. Zo blijkt dat er veel operationele taken uitgevoerd moeten worden, waardoor de meer strategische taken rondom informatieveiligheid niet altijd de aandacht krijgen die men eraan zou willen geven. De CIO en de afdeling IPPM geven de organisatie richting door strategievorming en beleid. Uit de interviews blijkt dat wordt erkend dat hierin nog stappen gezet moeten worden, ook door de CIO[27] zelf. De CIO is voornemens te kijken bij andere gemeenten hoe daar de inrichting geregeld is.

Binnen de gemeente wordt vanuit informatieveiligheid ook samengewerkt met de Functionaris Gegevensbescherming en de privacy officer[28], bijvoorbeeld bij het bevorderen van bewustzijn en bij de afhandeling van incidenten. Er wordt onder andere samengewerkt middels een zogenaamde 'driehoek' waarin medewerkers vanuit informatiebeveiliging en privacy tweewekelijks samenkomen om de stand van zaken rond risico's en maatregelen te bespreken. Via deze driehoek wordt het 'speelveld' vanuit de verschillende disciplines in kaart gebracht en worden nieuwe ontwikkelingen in de gaten gehouden. Deze samenwerking wordt door de medewerkers als constructief en effectief ervaren.

Uit de interviews blijkt dat bepaalde rollen en verantwoordelijkheden over de domeinen heen verschillend zijn ingericht. Zo worden er in het sociaal domein veel applicaties functioneel beheerd door het sociaal domein zelf, dit is binnen dit domein centraal georganiseerd.
Bij andere domeinen en afdelingen ligt beheer bij BIAS of bij een afdeling zelf. Ook is vernomen dat in het verleden[29] is gewerkt werd met ambassadeurs. Deze rollen hadden echter geen formele status als functie of beschikbare uren, zodat in de praktijk de invulling van deze rollen onzeker was. Op dit moment zijn managers volgens het huidige beleid zelf verantwoordelijk voor de informatiebeveiliging rondom eigen processen en hebben zij integrale verantwoordelijkheid. Uit de interviews kan worden opgemaakt dat dit niet altijd op deze manier wordt ervaren op de afdelingen zelf of dat verantwoordelijkheid niet voldoende wordt genomen.

De gesprekspartners lieten ook weten dat bij de verscheidende vakafdelingen het verschil in kennis varieert. Hierdoor kunnen veel ad hoc vragen ontstaan over zaken gerelateerd aan informatiebeveiliging en privacy. Geïnterviewden geven aan dat het ad hoc aspect in

26 De primaire verantwoordelijkheid voor de (informatie)veiligheid en de betrouwbaarheid van de informatieprocessen en systemen ligt binnen de afdelingen.
27 De huidige CIO is gestart in het voorjaar in 2023.
28 De privacy beheerder zoals beschreven in het beleid wordt in praktijk ingevuld door de privacy officer rol.
29 Het gaat om de periode 2017-2018.

de uitvoering van informatiebeveiliging kan zorgen voor tekort aan tijd en onvoldoende slagkracht om te focussen op strategische ontwikkeling en de borging van governance taken. Ook bestaat onzekerheid of alle proceseigenaren hun rol rondom informatiebeveiliging goed (kunnen) invullen[30].

In het beleid wordt een controller informatiebeveiliging genoemd die o.a. verantwoordelijk is voor het periodiek toetsen van de naleving, werking en effectiviteit van maatregelen. Deze zou controleren op voortgang op het actieplan en op de actualisatie van het beleid en risico-analyses. Tijdens het onderzoek is de (uitvoering van deze) functie niet gevonden zoals beschreven in het beleid.

Het strategisch beleid schrijft voor dat de kwaliteit van informatieveiligheid periodiek via audits wordt vastgesteld en dat hierover in de P&C-cyclus wordt gerapporteerd. Buiten de jaarlijkse ENSIA-audits zijn geen periodieke audits gevonden. De concerncontroller heeft geen direct controlerende rol op het informatiebeveiligingsbeleid, maar is wel betrokken bij de ENSIA-audit. Daarnaast wordt een jaarlijkse informatiebeveiligingsrapportage[31] door de CISO opgesteld waarin een beeld wordt geschetst van de stand van zaken.

3.1.4 Risicomanagement en PDCA-cyclus

Risicomanagement speelt in de Baseline Informatiebeveiliging Overheid (BIO) een belangrijke rol. Dat betekent dat processen en informatiesystemen beveiligd worden op basis van de risico's die de gemeente loopt of wil lopen. Het management zal daarbij op voorhand keuzes en afwegingen moeten maken of informatie in nieuwe en bestaande processen adequaat beveiligd is in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

Het risicomanagement op het gebied van informatiebeveiliging binnen Ede is nog niet volledig ingericht. Het ontbreekt aan overkoepelend Information Security Management System (ISMS) en een risicoregister met bijbehorende risico-acceptatie door een verantwoordelijk manager. Het voortbrengingsproces voor het doorvoeren van veranderingen in de informatievoorziening helpt in de praktijk om de belangrijkste risico's in kaart te brengen, maar in de beheerfase en op technisch vlak worden beveiligingsrisico's niet expliciet geaccepteerd. Uit het onderzoek blijkt dat de gemeente de risicovolle processen in beeld heeft, maar op procesniveau zijn (nog) niet alle risicoanalyses uitgevoerd. Wij hebben niet gevonden dat risicoanalyses zoals BIO-baseline-toetsen[32] structureel worden uitgevoerd (overigens wel op deelgebieden of in andere risico-analyse vormen). Ook ontbreekt een impactanalyse nu de gemeente niet meer voor beveiligingsincidenten verzekerd is. De laatst gevonden gap-analyse stamt uit 2019. Wel wordt in het kader van de ENSIA-audit een jaarlijkse zelfevaluatie over BIO-normen gedaan.

Binnen de gemeente wordt in het kader van informatieveiligheid en privacy samengewerkt en ook vanuit de BIO wordt vereist dat privacy en bescherming van persoonsgegevens worden gewaarborgd in overeenstemming met relevante wet- en regelgeving. Ondanks het feit dat dit onderzoek zich niet specifiek richt privacy, zijn enkele bevindingen uit de FG-meting van 2022 ten aanzien van risico-analyses wel relevant in het kader van informatieveiligheid. Uit de FG-meting blijkt dat Ede niet voldoende in beeld heeft welke risicovolle verwerkingen er zijn.

30 Uit de FG-meting van 2022 blijkt ook dat er meer aandacht nodig is om de afdelingsmanagers te laten groeien in hun rol als ambtelijk verwerkingsverantwoordelijke.

31 De informatiebeveiligingsrapportage wordt in de volgende paragraaf verder toegelicht.

32 BIO-baseline-toetsen worden gebruikt om een beveiligingsniveau te bepalen voor een proces, informatiesysteem en/of informatie. De uitkomsten kunnen worden gebruikt om te bepalen of er meer maatregelen nodig zijn voor een proces en onderliggende informatiesystemen.

Er is geen planning voor het uitvoeren van risico-analyses, zoals bij het uitvoeren van DPIA's (Data Protection Impact Assesment). Een PDCA-cyclus zoals deze is beschreven in het beleid wordt in de praktijk niet structureel uitgevoerd. Actieplannen en jaarrapportages worden wel opgesteld, maar controles op de uitvoering en voortgang worden en zijn in de onderzochte periode niet (structureel) uitgevoerd of gevonden. Medewerkers geven aan dat er nog veel winst van te behalen door naast het maken van plannen ook te kijken of deze worden uitgevoerd aan de hand van evaluaties.

3.1.5 Business continuity en Incidenten

In het kader van Business Continuity Management zijn de belangrijke systemen en processen in kaart gebracht. Daarbij is een inventarisatie gemaakt van onder andere risico's ten aanzien van ICT met bijbehorende impact en kans.

Een aantal bevindingen ten aanzien van business continuity zijn opgenomen in bijlage 5.

Voor medewerkers is er een duidelijk incidentenbeleid. Er zijn vaste rollen en verantwoordelijkheden bij incidenten. Uit de gesprekken blijkt dat de incidenten- en datalekkenprocedure goed bekend zijn binnen de gemeente. Incidenten (inclusief datalekken) kunnen bij het serviceplein worden gemeld via een formulier. Security incidenten kunnen ook rechtstreeks bij de informatieveiligheidsfunctionarissen terecht komen. In interviews wordt het beeld geschetst dat deze procedures laagdrempelig zijn en gevolgd worden. In de jaarrapportage informatieveiligheid wordt over datalekken en security-incidenten gerapporteerd. Het beeld bij de geïnterviewden is dat de meeste incidenten voortkomen vanuit menselijk handelen. Medewerkers geven aan ook te evalueren na incidenten, waarbij wordt gekeken of er verbeteringen of aanpassingen in de processen noodzakelijk zijn.

3.1.6 Voortbrengingsproces[33]

Ten aanzien van het voortbrengingsproces en het toepassen en toetsen aan beleid en kaders, geldt dat de meeste betrokkenen die wij gesproken hebben het proces kennen. Het proces is conform de wijze waarop ook andere organisaties hun IV (informatievoorziening) voortbrengingsproces structureren. Sommige betrokkenen geven aan dat er vertragingen kunnen zijn (onder andere wegens capaciteitsissues) en dat het proces nog niet bij iedereen op acceptatie kan rekenen. Het verder bestendigen van dit proces – dat zo belangrijk is om veranderingen zo goed mogelijk en zo snel mogelijk te realiseren waarbij risico's worden verminderd en beoogde doelen worden behaald – is van belang. Wij hebben in dit onderzoek geen diepgaande analyse hiervan gemaakt. Betrokkenen geven aan dat informatieveiligheid waaronder bijv. technische en privacy-eisen voldoende aandacht krijgen in de praktijk zolang het proces wordt gevolgd. In die gevallen waarin het proces niet wordt gevolgd is er mogelijk geen goede risicoanalyse en is het mogelijk dat het onderdeel informatieveiligheid niet de aandacht krijgt die nodig is. Uit het onderzoek bleek dat dit in de praktijk inderdaad voor is gekomen, bijvoorbeeld als een afdeling zelf een applicatie aanschaft buiten het proces om. Meer recent wordt hier door de directie op gehandhaafd indien waargenomen, zoals ook blijkt uit een aangeleverde voorbeeldcasus.

3.2 Bestuurlijk niveau

Met het bestuurlijk niveau wordt bedoeld de rapportage aan én de sturing die voortkomt uit directie en college, en de rapportage en sturingslijnen van en naar de raad. Binnen het college van B&W heeft één wethouder de portefeuille 'ICT, data-security en privacy' en overigens

33 De gemeente heeft een voortbrengingsproces voor het doorvoeren van veranderingen aan de informatiesystemen.

ook de portefeuille 'Betrouwbare overheid en Wet open overheid'. De algemeen directeur/ gemeentesecretaris is onder andere verantwoordelijk voor de operationele uitvoering van vastgesteld beleid en het opstellen van kaders.

De wethouder wordt geïnformeerd over informatieveiligheid op het moment dat er nieuw beleid wordt voorbereid, maar ook bij keuzes aangaande investeringen. Daarnaast heeft de wethouder een rol op het moment dat er incidenten zijn. Het onderwerp informatieveiligheid staat periodiek op de agenda bij directie en bestuur: in ieder geval eens per vier weken heeft de wethouder een portefeuilleoverleg. Vanuit de interviews ontstaat het beeld dat de wethouder aandacht heeft voor informatieveiligheid en over voldoende kennis van de materie beschikt.

Eén van de periodieke rapportagelijnen van ambtelijke organisatie via college naar de raad betreft de ENSIA-audit. Meer hierover verderop in dit hoofdstuk en in hoofdstuk vier. Een andere periodieke rapportagelijn betreft de Jaarrapportages informatieveiligheid die eveneens door het college worden aangeboden aan de raad: in ieder geval voor de jaren 2018, 2019, 2020, 2021 en 2022. Deze rapportages worden niet openbaar behandeld. De rapportages behandelen de volgende thema's:

- Beleid en organisatie
- Personeel en toegang
- Continuïteit en incidenten
- Informatiesystemen
- Gegevensbescherming

Naast de jaarrapportages over informatieveiligheid is er in 2020 en 2022 ook een FG-rapportage verschenen. Deze rapportages zijn opgesteld door de Functionaris Gegevensbescherming, met input van de privacy officer en CISO. Zoals eerder benoemd heeft de FG een toezichthoudende taak. In de rapportage wordt aandacht besteed aan de elementen governance, beleid, werkprocessen, bewustwording & training en beheer & opslag van gegevens. Er staat beschreven dat het van belang is dat de verantwoordelijkheden op bestuurlijk en ambtelijk niveau goed zijn benoemd, belegd en vastgelegd. Volgens de rapportage zijn de periodieke overleggen met de wethouder geïntensiveerd en is een eerste aanzet gedaan voor een gesprekscyclus met de concerndirecteur.

Er kunnen ook gevraagde of ongevraagde rapportages of memo's over het onderwerp informatiebeveiliging richting het college gaan. Er is bijvoorbeeld een memo aan het college gestuurd in november 2021, waarin een algehele stand van zaken is opgenomen (de inhoud is niet openbaar).

Rapportages vanuit de CISO-functie geven een helder beeld en zijn volledig. Een terugkerend punt in de rapportages is dat wordt benoemd dat de dagelijkse zaken veel inzet vragen, en dat zaken als het werken aan het beleid en of strategie erbij in schieten.

3.3 Medewerkersniveau

De bevindingen uit deze paragraaf zijn in bijlage 5 (geheim) geplaatst.

3.4 Technische beveiliging

In de praktijk wordt door de geïnterviewden benoemd dat de (technische) beveiliging binnen de gemeente in het algemeen op orde is. De gemeente heeft op het gebied van beveiliging gekozen voor een aanpak om (eerst) een technisch fundament te leggen en heeft zodanig diverse technische maatregelen genomen, waaronder (vergaande) zonering van het netwerk/

de systemen, adequaat patchmanagement, malware-detectie, whitelisting van applicaties en actieve monitoring van het netwerk en de systemen. Onze indruk op basis van de gesprekken en documentatie is dat de gemeente en specifiek de afdeling BIAS zorgen voor een adequate en professionele beveiliging. De BIO-zelfevaluatie die in het kader van de ENSIA is gedaan laat zien dat er verbeteringen worden gemaakt in het voldoen aan de normen uit de BIO. Naast deze algemene constateringen zijn er een aantal bevindingen op specifieke onderwerpen.

Bevindingen uit deze paragraaf zijn in bijlage 5 (geheim) geplaatst.

4. Rol van de raad

Bescherming tegen beveiligingsincidenten gaat niet alleen over de betrouwbaarheid en beveiliging van de informatiesystemen van de gemeente en de (persoons-)gegevens die erin zijn opgeslagen. Informatieveiligheid gaat ook over de betrouwbaarheid en continuïteit van de belangrijkste processen van de gemeente, zoals dienstverlening aan burgers, de interne bedrijfsvoering en het democratische proces.

De gemeenteraad heeft een belangrijke rol bij informatieveiligheid. Deze rol is expliciet meegenomen in dit onderzoek. Door het gemeentelijke beleid voor de bescherming van persoonsgegevens en andere informatie te toetsen op doeltreffendheid, doelmatigheid en rechtmatigheid, geeft de raad invulling aan haar controlerende rol. Vanuit de volksvertegenwoordigende rol is het voor de raad van belang de weerbaarheid tegen cybercriminaliteit te toetsen en daarbij het belang en perspectief van de inwoner mee te nemen en op basis hiervan eventueel nadere kaders te stellen.

4.1 Informatievoorziening

Er zijn een aantal manieren waarop de raad geïnformeerd kan worden over het onderwerp informatieveiligheid. Ten eerste in het geval er raadsstukken zijn waarin informatieveiligheid een rol speelt, zoals de jaarrapportages informatieveiligheid en ENSIA audit. Daarnaast kunnen raadsleden vragen stellen aangaande bijvoorbeeld actualiteiten. Ten slotte, via de raadswerkgroep digitalisering (recent opgestart) en raadsinformatiebijeenkomsten (ad hoc). Deze worden hieronder kort toegelicht.

4.1.1 Raadsstukken omtrent informatieveiligheid

De Jaarrapportages Informatieveiligheid zijn opgesteld en door het college aangeboden aan de raad. Deze rapportages geven een overzicht van de stand van zaken rondom informatieveiligheid in de gemeente. Daarnaast is er de ENSIA-audit[34]. Dit is een jaarlijks terugkerende audit waarin gemeentes zich dienen te verantwoorden aangaande informatiebeveiliging van een aantal landelijke basisregistraties en basisvoorzieningen, waaronder DigiD, SUWI en BAG. Het college stelt een verklaring vast die (deels) wordt opgesteld door een externe auditor. Deze verklaring wordt naar de raad gestuurd voor akkoord. De afgelopen jaren zijn er een aantal bevindingen geweest vanwege een aantal eisen waaraan de gemeente niet voldeed. Het college heeft in die gevallen aangegeven welke maatregelen er getroffen zijn; de raad heeft hierop geen verdere (bij-)sturende rol (gespeeld). In de jaarrekening van 2022 van de gemeente wordt de top 10 risico's weergegeven maar die zijn financieel van aard. In de paragraaf bedrijfsvoering en daaronder 'ontwikkelingen' wordt digitalisering en informatievoorziening kort beschreven: dit is een korte algemene tekst over het ICT domein. Daarnaast is er een item 'auditing, privacy en security[35], daarin wordt in algemene zin gerapporteerd over informatieveiligheid en privacy.

4.1.2 Vragen van de raad

Raadsleden kunnen ook informatie opvragen en vragen stellen. Een voorbeeld in dat kader zijn de vragen van een raadslid naar aanleiding van het beveiligingsincident Hof van Twente in 2020. In december 2020 is aan de raad middels een memo antwoord gegeven op de vraag:

34 Zie voor aanvullende toelichting eerdere paragraaf 3.4.5 over ENSIA.

35 Auditing, privacy en security | Programmarekening 2022 (jaarverslag-2022.nl)

'Is de digitale basisveiligheid van de gemeente Ede voldoende op orde?'. In deze memo wordt aangegeven dat de gemeente Ede voldoende (technische) maatregelen heeft getroffen en dat incidenten als deze worden bestudeerd om te beoordelen in hoeverre Ede gelijksoortige risico's loopt. Op de tweede vraag, aangaande de weerbaarheid van medewerkers, is geantwoord dat medewerkers worden gewezen op de noodzaak zorgvuldig te handelen (onder andere in het personeelshandboek), er via email, intranet en afdelingshoofden wordt gecommuniceerd over ontwikkelingen op het gebied van informatieveiligheid en dat er technische beperkingen zijn ingevoerd die maken dat bijvoorbeeld verdachte websites actief worden geblokkeerd.

4.1.3 raadsinformatiebijeenkomsten en werkgroep digitalisering

Er zijn in de afgelopen jaren enkele raadsinformatiebijeenkomsten georganiseerd waarin er in meer algemene termen uitleg wordt gegeven aan de raad over informatievoorziening, ICT en informatiebeveiliging. Er is daarnaast deze raadsperiode een raadswerkgroep digitalisering opgestart. Aan deze raadswerkgroep nemen vanuit de verschillende fracties raadsleden deel met affiniteit met het onderwerp. De leden van de raadswerkgroep worden met meer detailniveau geïnformeerd en zouden nieuw beleid kunnen bespreken, in voorbereiding op behandeling in de raad. Stukken die met de werkgroep worden gedeeld zijn toegankelijk voor alle raadsleden. Daadwerkelijke besluitvorming vindt uitsluitend in de raad plaats.

4.2 Perspectief raadsleden

In het kader van dit onderzoek is met een vertegenwoordiging uit de gemeenteraad van gedachten gewisseld over informatiebeveiliging. Hierbij zijn diverse onderwerpen aan de orde gekomen, zoals de kennis die raadsleden hebben van informatiebeveiliging, ervaringen die zij als raadslid hebben met dit onderwerp en hoe zij informatiebeveiliging tot een onderwerp in de raad kunnen maken. Een (fictieve) casus was de leidraad in deze bijeenkomst, waarbij in de bespreking ervan de relatie is gelegd met informatiebeveiliging in de gemeente Ede. Het karakter van de bijeenkomst was informerend en inventariserend en niet gericht op het innemen van standpunten. De bevindingen in deze paragraaf moeten niet gelezen worden als 'opvattingen van de gemeenteraad', maar als opvattingen van raadsleden.

Raadsleden geven aan wisselende verstandshoudingen met het onderwerp informatieveiligheid te hebben. Het belang ervan wordt onderkend, maar er is een zeker kennisniveau nodig om informatie over dit onderwerp te interpreteren en te kunnen plaatsen, en raadsleden verschillen onderling in hun kennisniveau. Daarnaast zijn er verschillen tussen raadsleden over de onderwerpen die zij willen benadrukken en waar zij hun prioriteiten op leggen, en welke onderwerpen niet.

In de bespreking in de raad over het onderwerp informatiebeveiliging die er ten behoeve van dit onderzoek is geweest, gaven leden aan dat er minstens eens per jaar een moment zou moeten zijn waarop de raadswerkgroep de bredere raad informeert en bijpraat. Anders dreigt er een steeds dieper wordende kloof te ontstaan tussen de leden van de raadswerkgroep en de rest van de raad aangaande kennis over informatieveiligheid.

Raadsleden geven aan dat zij als raad vooral willen weten dat de informatieveiligheid 'goed is geregeld'. Er is een minder duidelijk beeld over wat ervoor nodig is om een inschatting hierover te kunnen maken. Welke informatie zou de raad daarvoor willen ontvangen? Sommige zaken zijn wel uit te drukken in feitelijke cijfers, maar andere niet. Raadsleden geven aan dat zij overwegend niet de details willen weten, maar dat ze op de momenten dat er besluiten moeten worden genomen met consequenties voor informatieveiligheid, graag scenario's willen zien voor het effect op informatieveiligheid. Het kan dan bijvoorbeeld gaan over het niveau van risico dat de raad acceptabel zou vinden of de relatie tussen

financiële investeringen en de afname van het risiconiveau, zodat er een gesprek kan zijn over afwegingen en ambities.

De raad geeft aan op basis van de informatie die zij wél hebben vertrouwen te hebben in het niveau van beveiliging en het risico op incidenten op zich niet hoog in te schatten. Tegelijkertijd geven ze aan dat zij het geheel niet helemaal kunnen overzien, dat zij daarom onzeker zijn over de vraag of alle risico's wel in beeld zijn, dat de impact van een informatiebeveiligingsincident groot kan zijn en dat het wel nodig is om gezamenlijk een beter beeld te hebben van de stand van zaken en het daadwerkelijke risicoprofiel.

5. Beantwoording onderzoeksvraag

Op basis van de bevindingen van het onderzoek worden de onderzoeksvragen beantwoord. Per deelvraag zijn de normen uit het normenkader opgenomen inclusief bijbehorende beoordeling. Normen worden positief (+), negatief (-) of neutraal (+/-) beoordeeld. Een neutrale beoordeling betekent dat de gemeente (groten)deels aan de norm voldoet, maar dat er één of enkele duidelijke verbeterpunten zijn. De beoordeling is onderbouwd op basis van bevindingen uit het onderzoek, waarbij de belangrijkste of doorslaggevende bevindingen worden meegegeven. Na beantwoording van de deelvragen volgt de beantwoording van de centrale vraag.

5.1 Deelvragen

5.1.1 Wat is het Edese beleid op het gebied van informatieveiligheid en voldoet dit aan actuele standaarden?

Het beleid voor informatieveiligheid is vindbaar en uitgedrukt in meerdere documenten, waaronder leveranciersmanagement, incidentmanagement, privacy, technisch management, etc. Een deel van het beleid is recent, een deel is van een oudere datum. Het overkoepelende strategische beleid stamt uit 2017 en is nog gebaseerd op de BIG. Dat voldoet niet aan de actuele standaarden omdat het niet op de BIO is gestoeld. Er zijn al wel voorbereidende activiteiten ontplooid om het beleid te herzien. Onder die activiteiten vallen ook het opstellen van een discussienota ter vaststelling van een ambitieniveau. Dit heeft echter voor zover bij ons bekend niet geleid tot het vaststellen van een (SMART) ambitieniveau.

Normen deelvraag 1	Beoordeling
Het beleid is vindbaar.	+
Het beleid voldoet aan actuele standaarden zoals de BIO en de Digitale Agenda van de VNG.	-
Het beleid is SMART geformuleerd.	-
Het beleid van de gemeente wordt periodiek getoetst, geoefend en/of geëvalueerd.	-

5.1.2 Hoe wordt dit beleid uitgevoerd (bestuurlijk, organisatorisch, technisch, op proces- en medewerkersniveau)?

Er wordt relatief veel tijd besteed aan de operationele uitvoering van informatiebeveiliging ten opzichte van de strategische taken. Over het algemeen is de praktische uitvoering binnen het domein informatiebeveiliging op afdoende niveau. Als het puur gaat om het beleid en de mate waarin dit wordt uitgevoerd geldt dat er onderdelen zijn uit het beleid die in de praktijk niet terug komen.

Het beleid moet nog worden uitgewerkt. In de praktijk werkt de gemeente al wel grotendeels volgens de BIO. Rollen en verantwoordelijkheden worden in praktijk anders ingevuld dan in het beleid beschreven. Een voorbeeld daarvan zijn de verantwoordelijkheden van proceseigenaren (afdelingsmanagers) ten aanzien van informatieveiligheid. Niet alle afdelingsmanagers lijken voldoende kennis en competenties te hebben om risico's goed in te schatten en de juiste maatregelen te kiezen. Daarnaast is bijvoorbeeld een structurele uitvoering van de informatieveiligheidsanalyse niet gevonden.

Er is bestuurlijke aandacht voor informatieveiligheid, maar het ontbreekt aan een strategisch gesprek en strategische besluitvorming. Uit de interviews blijkt dat capaciteitsgebrek een oorzaak zou kunnen zijn. Ook het risicomanagement kan meer gestructureerd worden aangepakt.

In algemene zin geldt dat beleid beter kan worden uitgewerkt en herijkt naar de huidige situatie. Ook het praktische handelen van dag-tot-dag zou daarbij op papier gezet moet worden. Bij het vastleggen van deze processen wordt het risico verkleind dat een proces leunt op individuen. Dit is belangrijk in een organisatie met een redelijk groot aantal medewerkers, snelle ontwikkelingen in de taken van de gemeente en informatieveiligheid in het bijzonder, en met een arbeidsmarkt die zorgt voor een hoger verloop van eigen personeel dan normaal en grotere moeite nieuw personeel te vinden. Uit de interviews begrijpen wij dat werkdruk en capaciteitsgebrek een oorzaak kunnen zijn: het bij- en uitwerken van beleid blijft achter bij het handelen op dagelijkse issues en actualiteiten. De afwezigheid van strategische keuzes of een ambitieniveau kunnen hier een oorzaak van zijn. Wanneer geen doel is geformuleerd, is het risico dat de aandacht gericht blijft op de operationele taken die op dat moment voorliggen.

Normen deelvraag 2	Beoordeling
Er is aantoonbaar op het niveau van het college en de directie aandacht voor het thema informatieveiligheid.	+
De gemeente heeft een duidelijk beleid en uitvoeringskader bij hoe zij omgaat met risico's van/aan systemen, mensen, gegevens, informatie en middelen.	-
De gemeente heeft maatregelen ontwikkeld en geïmplementeerd om te zorgen voor de continuïteit, bescherming en eventueel herstel van kritische processen en dienstverlening.	+/-
Op basis van het vastgelegde beleid en de maatregelen vinden regelmatig oefeningen met betrekking tot incidenten plaats.	+/-
Medewerkers zijn bekend met het beleid, werken volgens de afspraken en zijn zich bewust van eigen handelen en verantwoordelijkheid.	+/-

5.1.3 Hoe reageert Ede op risico's en incidenten op het gebied van informatieveiligheid en wat is het lerend vermogen van de organisatie (plan – do – check – act)?

Ede werkt aan de hand van een procedure voor incidenten. Na incidenten worden evaluaties uitgevoerd op basis waarvan geïdentificeerde risico's, aanbevelingen en geplande acties en wijzigingen worden vastgelegd. De gemeente probeert daarmee te leren van incidenten. Conform de berichten uit de jaarrapportages is ervaring opgedaan met de incidentprocedure in de praktijk. Voor zover wij hebben kunnen beoordelen werkt dit naar behoren, al is niet op incidentniveau onderzoek gedaan.

Binnen de gemeente is geen *structureel* risicomanagement ingericht waarbij op voorhand keuzes en afwegingen worden gemaakt door het management over de beveiliging van processen. Door het ontbreken van een strakke structurele sturing op het organisatorische en procesmatige maatregelen uit het beleid lijken veel van de activiteiten en de risicoanalyses ad hoc te worden ingezet.

Een PDCA-cyclus (Plan-Do-Check-Act) is formeel onderdeel van beleid, maar in de praktijk kan het lerend vermogen nog sterk worden ontwikkeld. Dit komt terug in het ontbreken van gap- en informatieveiligheidsanalyses en opvolging op actieplannen. In algemene zin geldt dat het goed uitvoeren van alle vier de elementen (plannen maken en ontwikkelen, uitvoeren, controleren en toetsen en vervolgens bijsturen) maakt dat de organisatie verder kan groeien in haar professionaliteit, binnen de actuele en algemene context voor gemeentes waaronder druk op de middelen en druk vanuit de huidige arbeidsmarkt (personeelsverloop in combinatie met moeizame invulling van sommige vacatures).

Normen deelvraag 3	Beoordeling
De gemeente heeft de belangrijkste processen, systemen en risico's in beeld.	+/-
Er is een procedure voor het melden van incidenten en medewerkers kennen en gebruiken deze procedure.	+
De gemeente heeft maatregelen/acties/processen geïmplementeerd om actie te (kunnen) ondernemen tegen/na potentiële cybersecurity incidenten. Het gaat bijvoorbeeld om een incidentrespons procedure en nood/ continuïteitsplannen.	+
De gemeente stelt het risicobeeld periodiek bij op basis van (onder andere) informatie over dreigingen en veranderingen in processen en systemen.	-
Incidenten op het gebied van informatiebeveiliging of cybersecurity worden geëvalueerd en leiden tot structurele verbetermaatregelen.	+

5.1.4 Worden de geformuleerde doelstellingen gehaald en voldoet Ede aan de geldende normen voor informatieveiligheid (BIO)?

De doelstellingen van de gemeente Ede ten aanzien van informatieveiligheid zijn in het strategisch beleid opgenomen. Hierin wordt het doel van informatieveiligheid geformuleerd als het behoud van continuïteit, integriteit en betrouwbaarheid van de gegevens, vertrouwelijkheid en exclusiviteit en controleerbaarheid. In hoeverre de doelen worden behaald kan nu alleen worden beoordeeld aan de hand van incidenten (degenen die er zijn worden afgehandeld en datalekken worden gemeld).

Dit onderzoek heeft niet getracht een uitputtend overzicht te geven van de stand van zaken van de gemeente op alle normen uit de BIO. Wel is het beeld dat ontstaat uit het onderzoek dat de gemeente een basis op orde heeft en voor een groot deel voldoet aan de BIO. Doordat het strategisch informatieveiligheidsbeleid van Ede uit 2017 stamt en gebaseerd is op het verouderde normenkader BIG voldoet de gemeente niet (volledig) aan de geldende normen voor informatieveiligheid. Een groot deel van de normen vanuit de BIG zijn hetzelfde als die uit de BIO. De BIO verschilt op een aantal punten van de BIG. De BIO legt meer nadruk op risicomanagement dan de BIG, die meer gaat over specifieke maatregelen. De rol van de bestuurder en lijnmanager is ten aanzien van risicomanagement explicieter dan de BIG aangaf. Daarnaast zijn BIO maatregelen altijd verplicht en is de BIO meer risico-georiënteerd.

Normen deelvraag 4	Beoordeling
Ede heeft de door haar gestelde doelen voor informatieveiligheid behaald.	+/-
Ede voldoet aan de BIO.	+/-

5.1.5 Hoe is de raad betrokken bij (de uitvoering van) het beleid ten aanzien van de informatieveiligheid?

In 2022 is een raadswerkgroep digitalisering gestart waarbij elke fractie de gelegenheid heeft gehad één raadslid af te vaardigen. De raadswerkgroep wordt uitgebreider geïnformeerd over digitalisering en wordt ook betrokken bij het informatieveiligheidsbeleid. De fractievertegenwoordigers dienen hun eigen fracties te informeren en de stukken van de raadswerkgroep zijn voor alle raadsleden te benaderen.

Het door de raad actief controleren en beoordelen van het informatieveiligheidsbeleid en de uitvoering daarvan is een punt van aandacht. Er is (afgezien van jaarrapportages in de jaren 2018-2022) geen structurele informatievoorziening over de stand van zaken. Er is geen goed en/of gedeeld beeld van de informatie die de raad voor deze taak nodig zou hebben. De raad geeft aan op basis van de informatie die zij wél hebben vertrouwen te hebben in het niveau van beveiliging en het risico op incidenten niet hoog in te schatten. Tegelijkertijd geven ze aan dat zij het geheel niet kunnen overzien, dat de impact van een informatiebeveiligingsincident groot kan zijn en dat het wel nodig is om gezamenlijk een beter beeld te hebben van de stand

van zaken en het daadwerkelijke risicoprofiel. De raad geeft aan graag te willen zien dat zij benaderd worden met scenario's zodat er een gesprek op strategisch niveau over afwegingen en ambities plaats kan vinden.

Normen deelvraag 5	Beoordeling
De raad wordt structureel en regelmatig geïnformeerd over het beleid en de uitvoering rondom informatieveiligheid.	+/-
De raad is aantoonbaar betrokken bij het bepalen van de uitgangspunten[<?>] van het informatieveiligheidsbeleid.	-
De raad is aantoonbaar actief in het controleren en beoordelen van het informatieveiligheidsbeleid.	+/-

5.2 Hoofdvraag - In hoeverre is het Edese informatieveiligheidsbeleid doeltreffend?

De Edese inspanningen voor informatieveiligheid zijn doeltreffend in de zin dat belangrijke taken en voorzieningen worden uitgevoerd en aanwezig zijn. Er is een basisniveau bereikt en er wordt gehandeld in het geval er incidenten zijn en/of er actuele ontwikkelingen zijn.

Het Edese informatieveiligheidsbeleid is niet doeltreffend in de zin dat het beleid niet up-to-date is en sommige gevallen niet volledig uitgewerkt. De strategische doelen van informatieveiligheid en de manier waarop de voortgang gemeten kan worden zijn niet geactualiseerd. Dit hindert in algemene zin een groei in volwassenheid en professionaliteit op dit gebied. Het is van belang de structuren en governance op orde te hebben om te zorgen dat de gemeente in de toekomst niet in de problemen komt. Dreigingen veranderen en beleid helpt de gemeente om ook op de langere termijn de veiligheid van informatie te borgen, in een wereld met snelle cyberontwikkelingen, veranderingen in de arbeidsmarkt en een groeiend eisen-niveau van zowel burgers als overheid.

Bijlagen

Bijlage 1: Normenkader

Onderstaand is een overzicht van het normenkader aan de hand van de deelvragen opgenomen:

Wat is het Edese beleid op het gebied van informatieveiligheid en voldoet dit aan actuele standaarden?
Het beleid is vindbaar.
Het beleid voldoet aan actuele standaarden zoals de BIO en de Digitale Agenda van de VNG.
Het beleid is SMART geformuleerd.
Het beleid van de gemeente wordt periodiek getoetst, geoefend en/of geëvalueerd.
Hoe wordt dit beleid uitgevoerd (bestuurlijk, organisatorisch, technisch, op proces- en medewerkersniveau)?
Er is aantoonbaar op het niveau van het College en de directie aandacht voor het thema informatieveiligheid.
De gemeente heeft een duidelijk beleid en uitvoeringskader bij hoe zij omgaat met risico's van/aan systemen, mensen, gegevens, informatie en middelen.
De gemeente heeft maatregelen ontwikkeld en geïmplementeerd om te zorgen voor de continuïteit, bescherming en eventueel herstel van kritische processen en dienstverlening.
Op basis van het vastgelegde en de maatregelen vinden regelmatig oefeningen met betrekking tot incidenten plaats .
Medewerkers zijn bekend met het beleid, werken volgens de afspraken en zijn zich bewust van eigen handelen en verantwoordelijkheid.
Hoe reageert Ede op risico's en incidenten op het gebied van informatieveiligheid en wat is het lerend vermogen van de organisatie (plan – do – check – act)?
De gemeente heeft de belangrijkste processen, systemen en risico's in beeld.
Er is een procedure voor het melden van incidenten en medewerkers kennen en gebruiken deze procedure.
De gemeente heeft maatregelen/acties/processen geïmplementeerd om actie te (kunnen) ondernemen tegen/na potentiële cybersecurity incidenten. Het gaat bijvoorbeeld om een incidentrespons procedure en nood/continuïteitsplannen.
De gemeente stelt het risicobeeld periodiek bij op basis van (onder andere) informatie over dreigingen en veranderingen in processen en systemen.
Incidenten op het gebied van informatiebeveiliging of cybersecurity worden geëvalueerd en leiden tot structurele verbetermaatregelen.
Worden de geformuleerde doelstellingen gehaald en voldoet Ede aan de geldende normen voor informatieveiligheid (BIO)?
Ede heeft de door haar gestelde doelen voor informatieveiligheid behaald.
Ede voldoet aan de BIO.
Hoe is de raad betrokken bij (de uitvoering van) het beleid ten aanzien van de informatieveiligheid?
De raad wordt structureel en regelmatig geïnformeerd over het beleid en de uitvoering rondom informatieveiligheid.
De raad is aantoonbaar betrokken bij het bepalen van de uitgangspunten van het informatieveiligheidsbeleid.
De raad is aantoonbaar actief in het controleren en beoordelen van het informatieveiligheidsbeleid.

Bijlage 2: Bestudeerde achtergronddocumenten

Documentatie
Aankondiging Rekenkamer onderzoek informatiebeveiliging
Aansluitbeleid suwi (2018 versie 1.0)
Aansluitvoorwaarden Cloudgebaseerde Diensten 2.8.1 (2022)
Actieplan informatieveiligheid (2017)
Agenda Tolpoort (20-03-2023)
Agenda Tolpoort (04-03-2021)
Agenda Tolpoort (13-01-2022)
Agenda Tolpoort (30-05-2023)
Algemene Inkoopvoorwaarden voor leveringen en diensten Gemeente Ede VNG Model
Baselinetoets BBN BIO bulk betalingen
Baselinetoets LMS(11809)
Beantwoording persvragen (002) MvE
Beantwoording PW en CvD Vragenuurtje : Algoritmes Thimo harmsen (04-02-2021)
Beantwoording raadsvragen SGP VVD Versteeg Omlo m.b.t. gebruik van Chinese technologie (2021)
Beantwoording vragen mbt ICT security (7-6-2021)
Bedrijfscontinuïteitsbeleid (v.1.0, 2019)
Bedrijfscontinuïteitshandboek (v.0.99, 2023)
Bevindingen AVG FG meting 2020 gemeente Ede gevuld
Bibob beleidslijn december 2016
Bijlage 5 Service Level Agreement Shinto Labs (v1.0, 2019)
BIO zelfevaluatie Gemeente Ede (19-04-2023)
Calamiteitenplan Gemeente Ede (v1.0, 2020)
Collegeverklaring ENSIA inzake informatiebeveiliging van DigiD en Suwinet (2018)
Collegeverklaring ENSIA inzake informatiebeveiliging van DigiD en Suwinet (2019)
Collegeverklaring ENSIA inzake informatiebeveiliging van DigiD en Suwinet (2020)
Collegeverklaring ENSIA inzake informatiebeveiliging van DigiD en Suwinet (2021)
Collegeverklaring ENSIA inzake informatiebeveiliging van DigiD en Suwinet (2022)
DAP - Shinto Labs (v0.4, 2022)
Discussienota Strategisch beleid Informatiebeveiliging BIO v0.6
Discussienota strategisch informatieveiligheidsbeleid (2022)
Dreigingsbeeld 2022 Informatieveiligheid
EDE gedragscode (2022)
Ede gedragscode integriteit (2019)
End Presentation Gemeente Ede, PWC PAM Scan for Logical Access Security (Jan 2022 v1.2)
Format agendapunt discussienota strategisch informatieveiligheidsbeleid v0.2
GAP analyse BIO - bundeling naar projecten (v2.01)
Gap analyse BIO (07-2019)
GAP analyse BIO (v2.1, 201907)
GAP Analyse Ede September 2017
GAP analyse Gemeente Ede (september 2017)
Gebruikersovereenkomst Mobiele devices en thuiswerk faciliteiten (2021)
Gemeentebreed informatieveiligheidsbeleid (v1.2, 2017)
GIBIT 2020 Artikelen
Halfjaarplan 2021, juli t/m december
Handleiding Consignatiedienst BIAS (2018)
Informatiebeveiliging gegevensuitwisseling SUWI (2016)

Documentatie
Inkoopbeleid Gemeente Ede incl drempels (2022)
Integraal Veiligheidsplan Ede 2019 2022 (v3.0)
Intranetpagina informatiebeveiliging en privacy (Screenshot)
Invulsheet BIA vitaal en niet vitaal (2021)
Jaarplan (2022 v0.9)
Jaarrapportage informatiebeveiliging gemeente Ede (2018)
Jaarrapportage informatiebeveiliging gemeente Ede (2019)
Jaarrapportage informatiebeveiliging gemeente Ede (2020, v1.0)
Jaarrapportage informatiebeveiliging gemeente Ede (v1.0, 2020)
Jaarrapportage informatieveiligheid gemeente Ede (2021, v1.1)
Jaarrapportage informatiebeveiliging gemeente Ede (2022)
Kick off project ondermijning -Requirements Ede (v04, 20220512)
Lessons learned mailbox hack
Loggegevens api ede
Major Incident Rapport - Kwetsbaarheid Apache log4j (14-12-2021)
Major Incident Rapport - Phishing mail aanval (16-11-2021)
Major Incident Rapport (MB2001 0862)- Onveilige situatie Citrix Netscaler CVE 2019 19781
Major Incident Rapport 2020 01 21 Onveilige situatie Citrix Netscaler
Media berichten spam aanval
Memo Besluit/Advies gebruik Tiktok binnen de organisatie (april 2023)
Meerjarenplan informatieveilgheid (v1.0, 2020)
Meerjarenplan informatieveilgheid 1.0 versie (maart 2021)
Modelprotocol-bijlage model privacy protocol binnengemeentelijke gegevensdeling
NW CERT Report Investigation Holten (v.1.0, 2022)
Ondermijnende criminaliteit (presentatie)
Overzicht kritische processen applicaties & beheer (v1.0, 06-04-2020)
Plan van aanpak ondermijning (2018)
POA Update Bedrijfsrestaurant (30-05-2023)
Presenatatie gemeenteraad 9 mei
Presentatie informatieve raadsbijeenkomst
Presentatie onboarding training v.0.9
Privacy Actieplan 2020 2021 Ede (2020)
Privacy actieplan n.a.v. AVG 0 meting Ede (2019)
Procesbeschrijving Major Incident
Procesbeschrijving major incident (versie 1.0, 2018)
Processchema Voortbrengingsproces
Project Troje Rapport Secura locatiebezoek Ede (2023)
Project Troje Rapportage Ede (2023)
Project Troje Technische scan gemeente Ede (2023)
Projectvoorstel V1.0 Smartwheels (2021)
Projectvoorstel Ondermijningsmonitor (V0.2, 02-02-2022)
Projectvoorstel Tolpoort Axxerion FASE2 (V0.1, 25-11-2021)
Projectvoorstel Tolpoort planon start (V1.0, 09-03-2021)
Projectvoorstel Tolpoort Woningbouw monitor (V0.4, 23-11-2021)
Projectvoorstel Uitvaartsuite uitbreiden V1.0 (20-03-2023)
Projectvoorstel Update bedrijfsrestaurant (V1.0, 30-05-2023)
Projectvoorstel Woningbouw monitor fase 2 (V1.0, 20220714)
PSA Leerlingenvervoer (Smartwheels)
PSA Ondermijningsmonitor

Documentatie
PSA uitvaartsuite (20-03-2023)
PvA Ondermijnings Monitor (V0.8, 03-03-2022)
PvA SmartWheels (v1.0, 20210311)
PvA Trobit (20-03-2023, V1.0)
PvA Vastgoed (v1.0, 20210714)
PvA Vastgoed Axxerion FASE2 (v.0.9, 20211006)
Raadsmemo Vragen dhr. Omlo n.a.v. beveiligingsincident Hof van Twente (16-12-2020)
Rapport Datalekken meldformulier (21 7 2022 18.28.27)
Rapport FG meting 2022 - Gemeente Ede
Rapportage penetratietest Gemeente Ede (2015)
Rapportage penetratietest Gemeente Ede (2021, v1.0)
Rekenkamerrapport onderzoek naar beleidsondersteunende IV en ICT (2017)
Resultaten risicoanalyse (powerpoint)
Risicoanalyse (powerpoint)
Riskanalyze (05-06-2023)
Screenshot intranet pagina informatiebeveiliging en privacy.PNG
Service level agreement - Iburgerzaken van PinkRoccade Generieke SLA (versie 2.7, 2020)
Service Level Agreement Shinto Labs (v1.2, 2023)
SLA NVSI MC Suite definitief (versie 1.8, 25-02-2021)
Startbijeenkomst Rekenkamer Ede informatieveiligheid
Startnotitie onderzoek informatieveiligheid RKC Ede
Statement of Applicability (v1.2, 2023)
Technische vragen over gebruik mobiele telefoons en informatiebeveiliging
Template Projectvoorstel (12052022)
Toelichting B&W voorstel Suwinet beleid (2018)
Tolpoort 4 3, presentatie
Totaal lijst risicoinventarisatie V3 Resultaten
Training I bewustzijn "Informatieveiligheid en privacy in je werk" (powerpoint)
Verslag Tolpoort (20-03-2023)
Verslag Tolpoort (04-03-2021)
Verslag Tolpoort (13-01-2022)
Verslag Tolpoort (30-05-2023)
Niet openbaar - memo reactie VNG brief van Zanen
Niet openbaar - memo stavaza informatiebeveiliging Ede voor concerndirectie
Vitale processen overzicht (19-12-2022)
Voorbeeld organisatie tolpoorten uit (2020)
voorbeeld organisatie tolpoorten uit (2023)
Voorbeeld rapportage Iburgerzaken Pink SLA Ede (01-01-2022 tm 31-12-2022)
Voorlopig Informatiebeveiligingsplan eerste helft 2019
Voorstel Applicatie Ondermijning Gemeente Ede v1.0 (28-01-2022)
Voortgangsrapportage pmo Trobit

Bijlage 3: Geïnterviewde personen

In het kader van dit onderzoek zijn in totaal 12 gesprekken gevoerd met de onderstaande betrokkenen. Daarnaast zijn twee casussen besproken en is een sessie met de geweest.

#	Datum	Rol respondent
1	22-05-2023	Portefeuillehouder
2	22-05-2023	Concern directeur
3	16-05-2023	Functionaris gegevensbescherming (FG)
4	22-05-2023	Chief Information Security Officer (CISO)
5	17-05-2023	Information Security Officer (ISO)
6	16-05-2023	Privacy officer
7	22-05-2023	Manager Basis infrastructuur en applicatie services (BIAS)
8	17-05-2023	Chief Information Officer (CIO) / Hoofd Informatie, project- en procesmanagement (IPPM)
9	16-05-2023	Concerncontroller
10	17-05-2023	Informatie adviseur generieke voorzieningen
11	17-05-2023	Informatie adviseur bedrijfsvoering
12	17-05-2023	Informatiemanager sociaal domein
13	29-06- 2023	Casusbespreking 1
14	29-06-2023	Sessie met de raad
15	03-07-2023	Casusbespreking 2

Bijlage 4: Woordenlijst

Afkorting	Betekenis
AVG	Algemene Verordening Gegevensbescherming
BAG	Basisregistratie Adressen en Gebouwen
BIG	Baseline Informatiebeveiliging Gemeenten
BIO	Baseline Informatiebeveiliging Overheid
BRP	Basis Registratie Personen
CAB	Change Advisory Board
CIO	Chief Information Officer
CISO	Chief Informatie Security Officer
DPIA	Data Protection Impact Assesment
ENSIA	Eenduidige Normatiek Single Information Audit
GeVS	Gezamenlijke Elektronische Voorzieningen Structuur
GGI	Gemeentelijke Gemeenschappelijke Infrastructuur
ICT	Informatie- en Communicatie Technologie
ISO	Information security officer
FG	Functionaris Gegevensbescherming
ISMS	Information Security Management System
PDCA	Plan-Do-Check-Act
SO	Security Officer
SOC	Security Operations Center
SUWI	Structuur uitvoeringsorganisatie werk en inkomen
VOG	Verklaring omtrent Gedrag

Begrip	Betekenis
Cybercriminaliteit	Doelbewust van binnenuit of buitenaf inbreuk maken op informatiesystemen van een organisatie met als doel financieel gewin of verstoren.
Informatiebeveiliging	Het proces van vaststellen van de vereiste beveiliging van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.
Malware	Kwaadwillende software dat informatiesystemen probeert te verstoren.
Netwerk zonering	Het segmenteren van netwerken in afzonderlijke beveiligde (logische) domeinen en het reguleren van de toegang van gebruikers tot netwerkvoorzieningen en/of het filteren van informatiestromen met beleidsregels met filters en algoritmen.
Phishing aanval	Een aanval waarbij de aanvaller zich voordoet als iemand anders (een persoon of organisatie) met als doel persoonsgegevens of inloggegevens te vergaren.
Ransomware	Ook wel gijzelsoftware genoemd. Blokkeert het gebruik van een systeem of data via versleuteling met als doel losgeld te ontvangen.