



Gemeente Eindhoven

IT Audit Management Letter 2018

12 December 2018

Introductie

Gemeente Eindhoven
Postbus 90150
5600 RB Eindhoven
Nederland

Contact

Voor vragen over deze managementletter kunt u contact opnemen met:

[Redacted contact information]

[Redacted contact information]

[Redacted contact information]



Geachte [Redacted name]

In het kader van de jaarrekeningcontrole over het boekjaar 2018 heeft Deloitte Risk Advisory B.V. werkzaamheden uitgevoerd. In deze rapportage leest u onze bevindingen ten aanzien van de in dit kader uitgevoerde werkzaamheden. Wij hebben daarbij uitsluitend die maatregelen onderzocht die relevant zijn in het kader van de jaarrekeningcontrole en wij rapporteren hierbij uitsluitend de daarbij geconstateerde bevindingen. Ons rapport is als volgt opgebouwd:

- Managementsamenvatting
 - Algemene IT Beheersmaatregelen
 - IT Governance
 - Cyber Security
- Detail observaties Algemene IT Beheersmaatregelen

Dit rapport is uitsluitend bestemd voor gebruik door de Gemeente Eindhoven en mag zonder onze uitdrukkelijke schriftelijke toestemming niet met andere / derde partijen worden gedeeld.

Mocht u naar aanleiding van deze rapportage nog vragen en/of opmerkingen hebben, neemt u dan s.v.p. contact op met ondergetekende.

Met vriendelijke groet,
Deloitte Risk Advisory B.V.

[Redacted signature]

**

Sectie 1 – Managementsamenvatting

Managementsamenvatting

Doelstelling en scope

**

Scope:

Onze IT audit werkzaamheden bestonden uit de volgende deelgebieden:

- Algemene IT Beheersmaatregelen
- IT Governance
- Cyber Security

Doelstelling

Wij hebben onze werkzaamheden uitgevoerd in de periode augustus tot oktober 2018. Onze contactpersonen gedurende de werkzaamheden waren [REDACTED] ([REDACTED]), [REDACTED] ([REDACTED]) en [REDACTED] ([REDACTED]).

Hierbij is beoordeeld of de geselecteerde controlemaatregelen in voldoende mate de risico's mitigeren die een impact hebben op de betrouwbaarheid van de financiële gegevensverwerking. Wij hebben daarbij uitsluitend die maatregelen getest die relevant zijn in het kader van de jaarrekeningcontrole en wij rapporteren hierbij uitsluitend de daarbij geconstateerde bevindingen.

De beoordeling is uitgevoerd aan de hand van interviews, beoordeling van documentatie en het beoordelen van systeeminstellingen.

In het kader van het onderzoek is gesproken met de volgende medewerkers van de Gemeente Eindhoven:

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

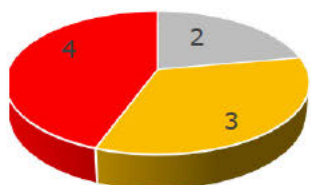
Voor Deloitte Risk Advisory hebben de volgende personen geparticipeerd:

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Managementsamenvatting

Algemene IT Beheersmaatregelen

Totaal 9 observaties welke zijn verdeeld in (impact):



■ Laag ■ Midden ■ Hoog

1. Algemene IT Beheersmaatregelen

Achtergrond

De Algemene IT Beheersmaatregelen (ook wel General IT Controls genoemd of 'GITC's') zijn de basis om te steunen op de geautomatiseerde gegevensverwerking in IT systemen. Indien GITC's effectief zijn kan –bij correcte inrichting van het IT systeem– in de audit ook gebruik worden gemaakt van de geautomatiseerde 'Business Controls' in de IT systemen, ook wel aangeduid als applicatie controles.

Uitgevoerde werkzaamheden

Wij hebben de *opzet* en het *bestaan* getoetst van de GITC's voor de applicaties Decade en Suites.

- Decade – Wordt gebruikt voor het inkoopproces en het uitvoeren van betalingen;
- Suites – Wordt gebruikt voor uitkeringen, WMO en PGB.

Aanvullend hierop is een beperkt aantal beheersmaatregelen getoetst op de Windows Active Directory, omdat dit de eerste stap is om toegang te krijgen tot de IT systemen van Gemeente Eindhoven. Gezien de aard van de opdracht ligt het beheer van de operating systemen (OS) en databases buiten de scope van de werkzaamheden.

Resultaten

Op basis van onze uitgevoerde werkzaamheden concluderen we dat de GITC's voor Decade en Suite ineffectief zijn in opzet en bestaan. Wij hebben tekortkomingen vastgesteld ten aanzien:

- De *opzet* van de IT beheersmaatregelen, omdat deze niet altijd het bijbehorende IT risico afdekken;
- De *implementatie* van de IT beheersmaatregelen (bestaan), omdat deze niet altijd overeenkomstig is met de opzet van de IT beheersmaatregel.

Op de volgende pagina noemen wij de IT observaties geprioriteerd op basis van impact en kans.

De gemeente heeft gekozen voor ITIL en BISO als uitgangspunt voor standaard processen. Wij adviseren de Gemeente Eindhoven om verdere harmonisatie toe te passen over alle applicaties heen en om de implementatie te controleren. Dergelijke standaard processen leiden tot duidelijke werkwijzen en afspraken. Een belangrijk voordeel is dat controles op alle systemen op dezelfde wijze uitgevoerd zullen worden.

Managementsamenvatting

Algemene IT Beheersmaatregelen

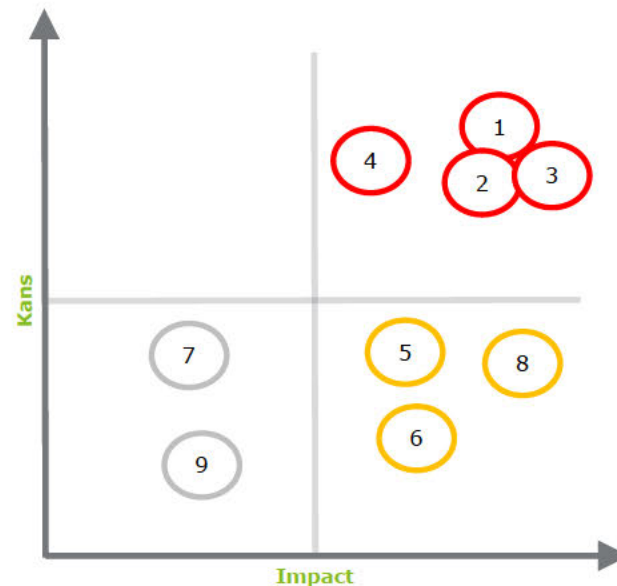
*** en

Doel:

Het management ondersteunen met een prioritering van de acties om de IT observaties op te lossen. Deze IT observaties zijn uitgezet over de assen impact en kans.

Betekenis van de symbolen

- Belangrijke bevinding met een hoog risico en potentieel grote impact op de verslaggeving, compliance en/of operationele prestaties. -> Onmiddellijke acties vereist door het management.
- Middelgrote bevinding met een gemiddeld risico en potentieel gemiddelde impact op de verslaggeving, compliance en/of operationele prestaties. -> Actie door het management vereist.
- Bevinding met een laag risico en een mogelijke lagere impact op de verslaggeving, compliance en/of operationele prestaties.



	Observaties	Applicatie
1	[Redacted]	[Redacted]
2	[Redacted]	[Redacted]
3	[Redacted]	[Redacted]
4	[Redacted]	[Redacted]
5	[Redacted]	[Redacted]
6	[Redacted]	[Redacted]
7	[Redacted]	[Redacted]
8	[Redacted]	[Redacted]
9	[Redacted]	[Redacted]

Managementsamenvatting

IT Governance

2. IT Governance

Achtergrond






Een effectief functionerende IT Governance structuur is de basis voor een optimale inzet en beheersing van IT middelen. IT Governance geeft inzicht in welke mate de interne beheersing in opzet en bestaan bijdraagt aan een betrouwbaar gegevensverwerkend proces en de effectiviteit van IT middelen. Dit vormt mede de basis voor de betrouwbaarheid van financiële informatie en verslaglegging en is daarmee een belangrijke factor voor de accountantscontrole.

Uitgevoerde werkzaamheden

Om een goed beeld te verkrijgen van de IT Governance hebben gesprekken plaatsgevonden met key functionarissen, zoals de CIO en CISO, binnen de Gemeente Eindhoven. Doel van deze gesprekken was informatie te verkrijgen en eventuele risico's te identificeren omtrent de volgende Cobit deelgebieden: Performance Measurement, Risk Management, Value Delivery, Strategic Alignment en Resource Management.

Resultaat

De slagvaardigheid van de IT functie van Gemeente Eindhoven kan verbeterd worden als taken en verantwoordelijkheden verder worden uitgewerkt en overeengekomen worden binnen de organisatie. Voor meer details zie de volgende pagina's. In onderstaande tabel hebben wij het volwassenheidsniveau per deelgebied opgenomen. Een IT Governance model in brede zin is vormgegeven in de vorm van het 9-vlakmodel, maar nog informeel doordat eigenaarschap, formele risicoanalyses en strikte tijdslijnen nog niet zijn geactualiseerd. Om door te groeien naar niveau drie adviseren wij de Gemeente Eindhoven meer te formaliseren, eigenaarschap te beleggen en tijdslijnen op te stellen en na te leven. De belangrijkste aanbeveling in dit kader betreft het opstellen van een overall IT Governance Control Framework hetgeen in lijn is met het IT Governance model en gebaseerd op een risicoanalyse. Daarnaast adviseren wij om zo snel mogelijk de IT strategie vast te stellen zodat het kan worden uitgevoerd. Wij hebben begrepen dat de IT strategie medio december 2018 zal worden bekrachtigd. Zie de appendix voor een toelichting op de Cobit Maturity levels.

Cobit deelgebied	Ad hoc	Repeatable	Defined	Managed	Optimizing
Performance Measurement					
Risk Management					
Value Delivery					
Strategic Alignment					
Resource Management					

Managementsamenvatting

IT Governance

**

2. IT Governance

Observaties	Aanbevelingen	Management Reactie + Actiehouder	Planning
<p>1. Als onderdeel van de IT strategie zijn zeven strategische thema's geformuleerd: Governance, Architectuur, Procesmanagement, Data-management, Sourcing, Informatiebeveiliging en Innovatie. In het kader van data-management heeft Gemeente Eindhoven reeds een uitgebreide data-inventarisatie en classificatie uitgevoerd. Hierbij wordt het classificatieproces als continue proces gezien dat breed gedragen moet worden en waarbij eigenaarschap wordt verwacht van eenieder. Echter, bij de meeste thema's is eerst verder inzicht in de huidige situatie en de wens van de organisatie/afnemers vereist voordat men kan beginnen aan het opstellen en uitvoeren van oplossingen. Tijdslijnen zijn nog niet vastgesteld, maar deliverables zijn omschreven en plannen zijn vastgelegd in het zogeheten i-plan. De strategische thema's zijn opgesteld met de blik "naar buiten" gericht.</p>	<p>a. Realiseer een IT Governance Control Framework voor de aansturing van ICT binnen de Gemeente Eindhoven, als overkoepelend geheel over alle betrokken organisatie onderdelen: CIO office, sector I&B maar ook de eindgebruikersorganisatie. Het IT Governance Control Framework dient de IT strategie en de geformuleerde thema's voldoende te ondersteunen.</p> <p>b. Finaliseer de IT strategie en stel de voorgestelde planning en de deliverables vast. Benoem taken en verantwoordelijkheden en een stel plan van aanpak op voor het verkrijgen van inzicht en het verder uitwerken van de IT strategie.</p> <p>c. Zorg voor voldoende alignment van de strategische thema's met de vraag vanuit de organisatie en de burgers.</p>	<p>a) Op 26 november wordt de geactualiseerde IT strategie in de Directieraad vastgesteld. Afgeleid daarvan zullen we onze huidige control maatregelen aanvullen en opnemen in een IT control framework.</p> <p><u>Actiehouder:</u> CIO in samenwerking met control</p> <p>b) Op 26 november wordt de geactualiseerde IT strategie in de Directieraad vastgesteld. Afgeleid daarvan zullen we een plan van aanpak voor de deliverables opstellen.</p> <p><u>Actiehouder:</u> CIO, in samenwerking met [REDACTED] r [REDACTED]</p> <p>c) De IT strategie is afgestemd met de behoefte van sectoren en de landelijke ontwikkelingen. We hebben 30 klantreizen gedaan (deels zelf gedaan en deels landelijke klantreizen) om de IT front-end ontwikkeling af te stemmen met onze inwoners. Bij de verdere uitwerking van de strategische thema's zal dit punt worden meegenomen.</p> <p><u>Actiehouder:</u> CIO, ondersteuning per thema</p>	<p>a) Q3 2019 b) Q1 2019 c) Q3 2019</p>

Managementsamenvatting

IT Governance

**

2. IT Governance

Observaties	Aanbevelingen	Management Reactie + Actiehouder	Planning
2. Beleidsdocumenten zoals 'aanpak strategische thema's', het informatiebeveiligingsbeleid en 'rapport visie 2020' zijn veelal opgesteld, roadmaps voor implementatie inclusief tijdslijnen, mijlpalen, eigenaren en verantwoordelijkheden binnen de gestelde kaders en tijdslijnen zijn veelal niet duidelijk gedefinieerd. Ook prioriteiten zijn vaak niet helder. De gemeente loopt hiermee het risico dat de daadkracht ten aanzien van strategische inzet van IT om haar doelen te realiseren, binnen de beschikbare budgetten, beperkt wordt.	Stel aan de hand van de gedefinieerde strategische thema's prioriteiten vast. Aan de hand hiervan kunnen actieplannen, verantwoordelijken en tijdslijnen worden gedefinieerd.	Deze aanbeveling komt overeen met die van 1b. Op 26 november wordt de geactualiseerde IT strategie in de Directieraad vastgesteld. Afgeleid daarvan zullen we een plan van aanpak voor de deliverables opstellen. <u>Actiehouder:</u> CIO, in samenwerking met [REDACTED].	Q1 2019
3. Informatiebeveiligingsbeleid wordt momenteel herschreven door de CISO.	Maak een duidelijke planning en zorg voor voldoende integratie met de gedefinieerde zeven strategische thema's, maar ook Cyber Security en AVG.	Er wordt momenteel aan gewerkt. Afhankelijkheden liggen met name t.a.v. Sourcing en Procesmanagement. AVG en Cyber security zullen nadrukkelijker worden benoemd. <u>Actiehouder:</u> CISO	Q1 2019
4. CIO office en I&B zijn bewust niet geïntegreerd in een afdeling. Het is zaak dat strategie, zoals bepaald door het CIO office, uitvoerbaar is voor de sector I&B, die verantwoordelijk zijn voor de uitvoering hiervan richting de belangrijke systemen van Gemeente Eindhoven.	<p>a) Op basis van het 9-vlakmodel zijn taken en verantwoordelijkheden uitgewerkt. Geef een specifiekere invulling en zorg dat taken en verantwoordelijkheden helder zijn gedefinieerd. Bouw voldoende organisatorische en procesmatige waarborgen in om te borgen dat strategie en uitvoering op continue basis afgestemd zijn.</p> <p>b) Maak verder inzichtelijk hoe de verhoudingen zijn tussen CIO, Sector I&B en de gebruikersorganisatie. Hierdoor wordt duidelijk wat van elkaar verwacht kan worden en hoe men elkaar kan versterken.</p>	<p>a) + b) Na 26 november werken we taken en verantwoordelijkheden verder uit o.b.v. 9-vlakmodel inclusief waarborgen van de monitoring. Dit is onderdeel van de acties n.a.v. het I-plan.</p> <p><u>Actiehouder:</u> CIO</p>	Q1 2019

Managementsamenvatting

IT Governance

2. IT Governance

Observaties	Aanbevelingen	Management Reactie + Actiehouder	Planning
5. Vanuit sector I&B is een 'Service Level Agreement' (SLA) opgesteld met de afnemers, evenals een 'Dossier Afspraken en Procedures (DAP)' waarin op operationeel niveau werkafspraken zijn vastgelegd. Afspraken zijn vaak generiek en formele goedkeuring van de stukken ontbreekt. Hierdoor zijn werkafspraken vaak onduidelijk.	<ul style="list-style-type: none"> a) Formaliseer de huidige afspraken. Kom duidelijke KPI's overeen, meet deze en rapporteer hierover. Stel deze op aan de hand van het IT Governance Control Framework. b) In het kader van operational effectiveness op termijn toewerken naar een standaard diensten en producten catalogus, binnen de kaders van de strategische doelstellingen. Hiermee wordt duidelijkheid geschapen voor de organisatie en het risico op wildgroei verminderd. Dit schept tevens duidelijkheid naar de organisatie. 	<ul style="list-style-type: none"> a) Afspraken worden momenteel geformaliseerd. b) Onderhanden <p><u>Actiehouder:</u> I&B/Diensten</p>	<ul style="list-style-type: none"> a) Q4 2019 b) Q4 2019
6. Veel applicaties vervullen eenzelfde of vergelijkbare functies zonder dat er synergie is. IT gerelateerde inkoop worden door inkoop afdeling I&B beoordeeld om aanschaf van IT te beoordelen op toegevoegde waarde voor de organisaties.	Definieer vanuit strategische kaders duidelijk beleid ten aanzien van de gewenste / toekomstige architectuur. Actualiseer het huidige landschap en stel plan van aanpak op. Vanuit deze kaders alle aanschaf van software, hardware, etc. beoordelen.	<p>Op 26 november wordt de geactualiseerde IT strategie in de Directieraad vastgesteld. Afgeleid daarvan zullen we een plan van aanpak voor de deliverables opstellen. Strategische kaders en een geactualiseerde architectuur zijn een onderdeel van de deliverables.</p> <p><u>Actiehouder:</u> CIO</p>	Q3 2019

Managementsamenvatting

IT Governance

**

2. IT Governance

Observaties	Aanbevelingen	Management Reactie + Actiehouder	Planning
<p>7. a) Belangrijkste norm voor Gemeente Eindhoven betreft de BIG die specifiek is opgesteld voor de informatiebeveiliging bij gemeenten. Hieromtrent is een gap-analyse uitgevoerd door de CISO waarbij is vastgesteld dat de Gemeente Eindhoven op een groot aantal normen (nog) niet (20) of gedeeltelijk niet (57) voldoet aan de norm. De CISO heeft inzichtelijk gemaakt hoeveel mandagen vereist zijn voor het dichtten van de 'gaps' en met welke prioriteit dit dient te gebeuren. Er is een inschatting gemaakt van het aantal mandagen voor verdere inrichting en monitoring van de SIEM-oplossing en het verder bestendigen van Microsoft systemen tegen externe bedreigingen.</p> <p>b) Het IT Governance is opgesteld vanuit het 9-vlaks model, maar een IT Governance Control Framework is niet beschikbaar. Risico's zijn niet volledig in kaart doordat een specifieke IT risicoanalyse ontbreekt. Wij hebben begrepen dat medewerkers van afdeling I&B in risico's denken en prioriteit wordt gegeven aan de juiste aspecten met de hoogste risico's en kennis hieromtrent is aanwezig, maar dat hiervan in beperkte mate vastlegging van bestaat. Wij merken op dat in het sectorplan I&B informatiebeveiliging beperkt voorkomt.</p> <p>c) Een privacy-beleid is beschikbaar waarin is opgenomen hoe men dient te voldoen aan de AVG en welke maatregelen bij de Gemeente Eindhoven geïmplementeerd zijn en dienen te worden. Recent advies vanuit de programma-manager AVG in de vorm van een raadsinformatiebrief geeft aan dat de Gemeente Eindhoven voldoet aan de minimale eis van de AVG. Wij hebben begrepen dat dit jaar geen Privacy Impact Analyse (PIA) zijn afgerond. Uit een concept advies blijkt dat een groot aantal verbeterpunten bestaan op het gebied van privacy.</p> <p>d) Wij hebben begrepen dat de AVG en privacy de aandacht heeft van de gemeentesecretaris, maar dat er nog veel activiteiten dienen te worden uitgevoerd en kennis moet worden opgebouwd, gemeente-breed, voordat men op het niveau is wat de gemeente nastreeft. Privacy Officers moeten nog worden aangesteld. Hierdoor bestaat de kans dat sectoren onvoldoende grip hebben op privacybescherming.</p>	<p>a) Actualiseer openstaande punten en risico's ten aanzien van informatiebeveiliging, Cyber Security en AVG. Ken op basis van risico inschatting prioriteiten toe, stel een actieplan op en allocer voldoende middelen.</p> <p>b) Actualiseer het overkoepelend informatiebeveiligingsbeleid.</p> <p>c) Realiseer een overall IT Governance Control Framework gebaseerd op een risicoanalyse voor het continue inventariseren van risico's. Hierdoor kan op basis van actuele risico's of dreigingen snel worden bekeken of bestaande controls voldoende zijn.</p> <p>d) Ken voldoende middelen toe om risico's ten aanzien van AVG voldoende te mitigeren. Denk hierbij aan het benoemen van Privacy Officers per sector die vervolgens PIA's kunnen uitvoeren. Uitgangspunt is de actielijst met openstaande punten.</p>	<p>a) + c) Dit loopt op dit moment de actieplannen worden op dit moment opgesteld en de middelen moeten nog worden gealloceerd.</p> <p><u>Actiehouder:</u> █████</p> <p>b) In concept gereed afstemming met organisatie loopt.</p> <p><u>Actiehouder:</u> █████</p> <p>d) In 2018 is voor de implementatie van de AVG vanuit de sector VB incidenteel budget beschikbaar gesteld. Voor 2019 e.v. dient dekking binnen bestaande gemeente-brede budgetten beschikbaar te zijn. De wijze waarop dient nog nader geconcretiseerd te worden. Vanuit de sector VB zal hiervoor een voorstel worden aangeleverd.</p> <p><u>Actiehouder:</u> Sector VB</p>	<p>a) Q2 2019 b) Q1 2019 c) Q2 2019 d) Q1 2019</p>

Managementsamenvatting

Cyber Security

3. Cyber Security

Cyber is een onlosmakelijk onderdeel geworden van onze samenleving. Dagelijks werken wij met digitale oplossingen, zowel privé als zakelijk. Door gebruik van het internet, bedrijfsnetwerken en -applicaties hebben alle organisaties, ongeacht hun omvang, te maken met aan cyber gerelateerde risico's zoals cyber aanvallen, hacks of andere vormen van cybercrime. Als cyberrisico's zich voordoen, kunnen deze een significante impact hebben op de (financiële) systemen, de interne beheersing en daarmee uiteindelijk ook op de jaarrekeningcontrole. Cyber aanvallen kunnen leiden tot een grote verscheidenheid aan risico's, variërend van ongeautoriseerde wijzigingen in de IT-systemen of in de gegevens die met deze systemen worden beheerd, tot het openbaar worden van persoonsgegevens, andere vertrouwelijke gegevens of Intellectual Property, of zelfs tot verstoring van de bedrijfsvoering (bijvoorbeeld als gevolg van ransomware).

Aangezien cyberrisico's voor iedere organisatie ernstige gevolgen kunnen hebben, attenderen wij u op het belang van een cyberrisicoanalyse als vast onderdeel van het interne controlesysteem dat:

- relevante financiële, operationele en rapportagerisico's onderkent;
- het belang en de waarschijnlijkheid daarvan adequaat inschat en
- de interne beheersing daarop toespitst.

De kernwoorden hierbij zijn veilig, waakzaam en weerbaar. Het maatschappelijk verkeer verwacht van organisaties dat cybersecurity op de bestuurlijke agenda staat en dat hiervoor passende maatregelen voorhanden zijn c.q. getroffen worden.

Voor ons als accountant is het met name relevant in hoeverre passende maatregelen zijn getroffen om de gevolgen van cyberrisico's voor de jaarrekening effectief te beheersen. Dit omvat minder risico's dan de cyber risico's die voor uw organisatie zelf relevant zijn. Onze werkzaamheden op dit vlak beperken zich daarom tot het verkrijgen van inzicht in de wijze waarop uw organisatie zelf cyber risico's identificeert en welke maatregelen uw organisatie heeft getroffen voor de risico's die wij het meest relevant achten voor de jaarrekening. Dit richt zich op de volgende gebieden:

- *Risico's rondom identificatie:* wordt cybercriminaliteit als een relevante dreiging gezien, is het duidelijk aan welke cyberrisico's uw onderneming wordt blootgesteld?
- *Risico's rondom bescherming:* heeft uw onderneming maatregelen getroffen om cyber aanvallen af te slaan (bijvoorbeeld doordat medewerkers op links in phishing-mails klikken en malware hun onvoldoende beveiligde systeem infecteert; kan zich dit dan ongebreideld binnen het netwerk verspreiden naar andere werkstations en servers)?
- *Risico's rondom detectie:* worden cyberincidenten en kwetsbaarheden tijdig opgemerkt?
- *Risico's rondom reactie:* kan uw organisatie adequaat op cyberincidenten reageren, zodat de impact hiervan beperkt wordt?
- *Risico's rondom herstel:* heeft uw organisatie voldoende voorzieningen achter de hand in de vorm van een herstelplan en back-upvoorzieningen om bij een cyberincident tijdig de bedrijfsvoering te hervatten?

Managementsamenvatting

Cyber Security

**

3. Cyber Security

Resultaten

Het belang van cyber weerbaarheid wordt binnen gemeente Eindhoven onderkend. Wij hebben vastgesteld dat verschillende maatregelen zijn getroffen. Zo beschikt de Gemeente Eindhoven bijvoorbeeld over een Security Information and Event Management systeem (SIEM). Ook is de functie van [REDACTED] ingevuld en ondersteund door een Information Security Officer per domein. Overall zien wij echter dat de beheersing van cyberrisico's nog niet het gewenste niveau heeft bereikt. Wij hebben dan ook een aantal mogelijkheden voor verbetering vastgesteld. Wij merken op dat de Gemeente Eindhoven zicht focust op compliant te zijn aan de BIG. In de BIG zijn normen opgenomen die raakvlakken hebben met betrekking tot de Cyber Security.

Bevindingen

Wij hebben de belangrijkste aandachtsgebieden hieronder opgesomd:

- Organization & Governance
- Risk Analysis
- Behavior & Culture
- Third Party Management
- Detection: Response




Conclusie

Wij concluderen dat de aanwezige cybersecurity beheersing (te) beperkt is qua aard, reikwijdte en/of diepgang met betrekking tot ongeautoriseerde wijzigingen in systemen, het openbaar worden van persoonsgegevens, vertrouwelijke gegevens of door het verstoren van de bedrijfsvoering. Wij schatten het maturity niveau in op twee hetgeen inhoudt dat controls aanwezig zijn, maar dat structurele aansturing hieromtrent ontbreekt. Zie de volgende pagina's voor onze observaties per deelgebied en zie pagina 14 voor concrete aanbevelingen.

Managementsamenvatting

Cyber Security

3. Cyber Security

Onderdeel		Ad hoc	Repeatable	Defined	Managed	Optimizing
Organization & Governance	<p>Cyber Security is niet als apart onderdeel benoemd binnen informatiebeveiliging bij de Gemeente Eindhoven. We hebben begrepen dat het verweven is in het algehele beleid omtrent informatiebeveiliging. De organisatie dient zich te confirmeren aan de BIG hetgeen de Baseline Informatiebeveiliging is voor Gemeenten in Nederland. In dit kader is er geen formeel programma of prestatie-indicatoren opgesteld omtrent Cyber Security.</p> <p>Het bewustzijn en de aandacht voor Cyber Security binnen DSO is voor verbetering vatbaar. Cyber zou een vast onderdeel moeten zijn op de bestuurlijke agenda.</p> <p>Formele rapportages over de status van Cyber Security en incidenten ontbreken nog. KPI's zijn niet gedefinieerd in dit kader.</p>					
Behavior & Culture	<p>Gemeente Eindhoven heeft activiteiten uitgevoerd om de awareness onder de medewerkers te verhogen, bijvoorbeeld in het proces omtrent classificatie van data. Desondanks hebben wij begrepen dat de awareness van de gemiddelde medewerker laag is te noemen. Er is geen specifieke campagne voor het verhogen van awareness bij de gemeente. Er zijn beperkte middelen aanwezig om de awareness te verhogen.</p>					
Risk Analysis	<p>Een risicoanalyse en risicomanagement framework omtrent Cyber Security ontbreekt. Het is de taak van de ISO's om een risicoanalyse binnen hun domein uit te voeren. Echter zijn deze ISO's recentelijk benoemd waardoor de risicoanalyses nog niet zijn uitgevoerd. Daarnaast zal hiervoor ook tijd en opleiding vereist zijn.</p>					

Managementsamenvatting

Cyber Security

3. Cyber Security

Onderdeel		Ad hoc	Repeatable	Defined	Managed	Optimizing
Third Party Management	Leveranciers dienen te voldoen aan maatregelen met betrekking tot Cyber Security. Er ontbreekt echter een actieve uitvraag en monitoring op de leveranciers. Er vindt niet op structurele wijze controle plaats van de dienstverlening van externe partijen. Sommige partijen beschikken over een TPM, maar deze worden niet of beperkt opgevraagd en beoordeeld.					
Detection	Onder andere een SIEM-oplossing is in gebruik bij de Gemeente Eindhoven voor detectie van Cyber Security bedreigingen. Echter hebben wij begrepen dat de gemeente niet over de vereiste capaciteit beschikt om de SIEM in de gewenste mate te monitoren. Penetratietesten worden uitgevoerd, echter worden deze niet volgens een vaste cyclus uitgevoerd, bijvoorbeeld inclusief procesevaluatie. Op maandelijkse basis worden alle systemen automatisch door tool Nexpose gecontroleerd op kwetsbaarheden. Op jaarlijkse basis wordt een hackathon georganiseerd waarbij elk jaar een bepaald onderdeel open staat voor ethical hackers.					
Response	Een incident respons procedure is beschikbaar en een crisisteam is benoemd. Echter is er nog nooit geoefend door het crisisteam. Er is geen disaster recovery plan, geen business continuïteit plan en er is geen business impact analyse uitgevoerd.					

Managementsamenvatting

Cyber Security

**

3. Cyber Security

Deelgebied	Aanbeveling	Management Reactie + Actiehouder	Planning
Organization & Governance	<ul style="list-style-type: none"> a) Neem in het informatiebeveiligingsbeleid ook een specifieke paragraaf op omtrent Cyber Security. b) Stel Prestatie-Indicatoren op om de beheersmaatregelen omtrent Cyber Security te monitoren (KPI's) en rapporteer hierover; c) Neem Cyber Security op als vast onderdeel van de bespreking met de DSO. d) Geef opvolging aan de gaps die zijn gesignaleerd ten op zichten van de BIG normering. 	<ul style="list-style-type: none"> a) Cyber Security zal worden opgenomen. b) Voor een groot deel is dit er al, maar zal nog verder worden uitgewerkt in structurele periodieke rapportages. c) Dit zullen we vanaf nu minimaal 2 keer per jaar agenderen. d) Onderhanden. <p><u>Actiehouder:</u> █████</p>	<ul style="list-style-type: none"> a) Q1 2019 b) Q2 2019 c) 2019 d) 2020
Behavior & Culture	<p>Om het bewustzijn omtrent Cyber Security binnen Gemeente Eindhoven te vergroten en de organisatie mee te krijgen in de cyber security ontwikkelingen bevelen wij het volgende aan:</p> <ul style="list-style-type: none"> a) Het verdient de aanbeveling om de huidige activiteiten op te nemen in een awareness beleid. Dit beleid verder aan te vullen en op periodieke basis activiteiten te organiseren waarmee de awareness wordt verhoogd. Denk hierbij aan het periodiek uitsturen van phishing mails. b) Daarnaast verdient het de aanbeveling dat management en directie actief betrokken zijn bij de cyber security activiteiten en dat samen met het management periodiek awareness campagnes worden georganiseerd waarin diversie risico's worden belicht. 	<ul style="list-style-type: none"> a) Er gebeurt al veel op het gebied awareness maar dit moet meer gestructureerd worden aangepakt en gepland. Het staat op de planning voor 2019 om dit verder uit te bouwen. b) Zie boven. <p><u>Actiehouder:</u> █████</p>	<ul style="list-style-type: none"> a) Q2 2019 en doorlopend b) Zie boven
Risk Analysis	<p>De gemeente heeft steeds meer te maken met cyber security risico's. Daarom verdient het de aanbeveling om periodiek risico analyses uit te voeren van zowel de externe omgeving als mogelijke veranderingen in de interne omgeving. Daarnaast verdient het de aanbeveling dat de gemeente de uitkomsten van deze analyses vertaalt naar de impact ervan op de gemeente en hoe zij zich beter kan verdedigen tegen deze risico's. Bij overlap met de BIG norm kan een mapping worden gemaakt.</p>	<p>Er wordt nu een begin gemaakt met het opvijzelen van het kennisniveau op dit gebied bij de ISO's per sector. Vanaf Q1 2019 zullen er periodiek (per sector) Risico analyses worden aangeleverd, waaruit maatregelen kunnen voortvloeien.</p> <p><u>Actiehouder:</u> █████</p>	<p>Q2 2019 en doorlopend</p>

Managementsamenvatting

Cyber Security

**

3. Cyber Security

Deelgebied	Aanbeveling	Management Reactie + Actiehouder	Planning
Third Party Management	Ten aanzien van de derde partijen verdient het de aanbeveling om: <ul style="list-style-type: none"> • Te inventariseren met welke derde partijen de gemeente te maken heeft; • Actief voor haar derde partijen te bekijken of een ISAE3402 beschikbaar is en/of een ISO270001. 	Wij zullen, voor zover nog niet bekend, verder inventariseren voor welke partijen deze verklaringen beschikbaar zijn. Actiehouder: [REDACTED] [REDACTED] [REDACTED]	Q2 2019
Detection	Wij adviseren om extra middelen aan te wenden om de SIEM-oplossing op een effectieve wijze te monitoren.	Dat gaan wij onderzoeken. Actiehouder: I [REDACTED] [REDACTED]	Q2 2019
Response	a) Ten aanzien van het crisis team bevelen wij aan om periodiek overleg te organiseren waarin incidenten worden geëvalueerd of de juiste handelingen zijn uitgevoerd om antwoord te geven op de incidenten. b) Hiernaast adviseren wij om een business impact analyse uit te voeren. Vervolgens kan een disaster recovery plan en business continuïteit plan worden opgesteld.	a) Er vinden al geregeld evaluaties plaats als onderdeel van het proces calamiteiten. Wij zullen beoordelen of dit verdere aanscherping benodigd m.b.t. de voorgestelde periodiciteit. b) We zijn bezig dit te analyseren. Dit zal naar verwachting grote impact hebben en als een apart project moeten worden opgepakt. Actiehouder: I&B, [REDACTED]	Q2 2019

Sectie 2 – Detail Observaties Algemene IT Beheersmaatregelen

Sectie 3 – Appendix

Appendix – Cobit Maturity Levels

Cobit Maturity level

Maturity Level	Description
0 - Non-existent	No documentation. There is no awareness or attention for certain control.
1 - Initial/ad hoc	Control is (partly) defined, but performed in an inconsistent way. The way of execution is depending on individuals.
2 – Repeatable but intuitive	Control is in place and executed in a structured and consistent, but informal way.
3 – Defined	Control is documented, executed in a structured and formalized way. Execution of the control can be proved.
4 – Managed and measurable	The effectiveness of the control is periodically assessed and improved when necessary. This assessment is documented.
5 – Optimized	An enterprise wide risk and control program provides continuous and effective control and risk issues resolution.

Cyber Security Maturity

Maturity Level	Description
1 – Ad-hoc	Cyber security activities are performed on an ad hoc basis. No mechanism to support the cyber security activities.
2 – Repeatable	Limited repeatability in cyber security activities. No structural mechanism to support the cyber security activities.
3 – Defined	Predefined cyber security activities which are consistently performed. Standardized mechanism to support the cyber security activities.
4 – Managed	Activities are part of a structured cyber security function.
5 – Optimizing	Cyber security activities are part of a structured cyber security function and are continuously improved.

Appendix - Normenkader Algemene IT Beheersmaatregelen

ID	Beschrijving Control
01	Een procedure voor het verstrekken van autorisaties dient te zijn vastgelegd en bestaat uit werkwijzen voor goedkeuring en implementatie van de autorisatie aanvraag met betrekking tot de indiensttreding en bij wijziging van rechten.
02	Toegang tot de applicatie wordt tijdig ingetrokken wanneer een medewerker de organisatie verlaat.
03	Autorisaties dienen periodiek (minimaal jaarlijks) te worden gecontroleerd (bijv. o.b.v. een autorisatiematrix). Hierbij wordt gelet op de juiste toewijzing van de rol en de inhoud van de beschikbare rollen.
04	Autorisaties in de applicatie zijn ingericht volgens een autorisatiematrix. In de autorisatiematrix is per rol inzichtelijk wat de functie zijn die door de rol zijn uit te voeren. Wanneer functiescheidingsconflicten bestaan dan is dit voorkomen of gemitigeerd door andere controls.
05	<p>De applicatie dwingt het gebruik van sterkte wachtwoordvereisten (inclusief lock-out) af.</p> <p>Toegang tot de applicatie kan alleen worden verkregen middels unieke gebruikersnamen die te herleiden zijn naar individuen. Accounts die niet te herleiden zijn naar een individu dienen een specifiek doel (bijv. batch-job of service) en worden op een juiste manier beheerd door geautoriseerde medewerkers.</p>
06	Het aantal gebruikers met "hoge bevoegdheden" (oftewel de superusers/administrators) is beperkt tot geautoriseerde medewerkers.
10	Wijzigingen worden adequaat getest en worden formeel goedgekeurd voordat deze in productie worden genomen.
13	De mogelijkheid om wijzigingen in productie aan te brengen is beperkt tot daartoe geautoriseerde personen.
17	Back-ups en de retentie worden uitgevoerd conform het beleid van de organisatie. Back-ups worden op een veilige locatie gearchiveerd om het risico op dataverlies te minimaliseren. Het back-up proces wordt gemonitord en geregistreerd. Wanneer een back-up niet succesvol is afgerond dan zal deze tijdig van opvolging worden voorzien. Alleen geautoriseerde functionarissen beschikken over toegang om de back-up schedules aan te passen. Periodiek vindt een validatie plaats van de gebacküpped data door middel van een restore.
19	Toegang tot de serverruimte en de directe omgeving van de computerapparatuur is beperkt tot personen die deze toegang nodig hebben om hun functie uit te voeren. Het IT management geeft goedkeuring voor het verlenen van deze toegang.

Appendix - Normenkader IT Governance

ID	Cobit domein	Control
ME1.2	Performance Measurement	<p><i>Definition and Collection of Monitoring Data</i></p> <p>Work with the business to define a balanced set of performance targets and have them approved by the business and other relevant stakeholders. Define benchmarks with which to compare the targets, and identify available data to be collected to measure the targets. Establish processes to collect timely and accurate data to report on progress against targets.</p>
ME1.4	Performance Measurement	<p><i>Performance Assessment</i></p> <p>Periodically review performance against targets, analyze the cause of any deviations, and initiate remedial action to address the underlying causes. At appropriate times, perform root cause analysis across deviations.</p>
ME1.5	Performance Measurement	<p><i>Board and Executive Reporting</i></p> <p>Develop senior management reports on IT's contribution to the business, specifically in terms of the performance of the enterprise's portfolio, IT-enabled investment programs, and the solution and service deliverable performance of individual programs. Include in status reports the extent to which planned objectives have been achieved, budgeted resources used, set performance targets met and identified risks mitigated. Anticipate senior management's review by suggesting remedial actions for major deviations. Provide the report to senior management, and solicit feedback from management's review.</p>
ME1.6	Performance Measurement	<p><i>Remedial Actions</i></p> <p>Identify and initiate remedial actions based on performance monitoring, assessment and reporting. This includes follow-up of all monitoring, reporting and assessments through:</p> <ul style="list-style-type: none"> • Review, negotiation and establishment of management responses • Assignment of responsibility for remediation • Tracking of the results of actions committed
ME2.1	Value Delivery	<p><i>Monitoring of Internal Control Framework</i></p> <p>Continuously monitor, benchmark and improve the IT control environment and control framework to meet organizational objectives.</p>
ME2.2	Risk Management	<p><i>Supervisory Review</i></p> <p>Monitor and evaluate the efficiency and effectiveness of internal IT managerial review controls.</p>
ME2.3	Risk Management	<p><i>Control Exceptions</i></p> <p>Identify control exceptions, and analyze and identify their underlying root causes. Escalate control exceptions and report to stakeholders appropriately. Institute necessary corrective action.</p>
ME2.6	Risk Management	<p><i>Internal Control at Third Parties</i></p> <p>Assess the status of external service providers' internal controls. Confirm that external service providers comply with legal and regulatory requirements and contractual obligations.</p>

Appendix - Normenkader IT Governance

ID	Cobit domein	Control
ME2.7	Risk Management	<i>Remedial Actions</i> Identify, initiate, track and implement remedial actions arising from control assessments and reporting.
ME3.1	Risk Management	<i>Identification of External Legal, Regulatory and Contractual Compliance Requirements</i> Identify, on a continuous basis, local and international laws, regulations, and other external requirements that must be complied with for incorporation into the organization's IT policies, standards, procedures and methodologies.
ME3.2	Strategic Alignment	<i>Optimization of Response to External Requirements</i> Review and adjust IT policies, standards, procedures and methodologies to ensure that legal, regulatory and contractual requirements are addressed and communicated.
ME4.1	Strategic Alignment	<i>Establishment of an IT Governance Framework</i> Define, establish and align the IT governance framework with the overall enterprise governance and control environment. Base the framework on a suitable IT process and control model and provide for unambiguous accountability and practices to avoid a breakdown in internal control and oversight. Confirm that the IT governance framework ensures compliance with laws and regulations and is aligned with, and confirms delivery of, the enterprise's strategies and objectives. Report IT governance status and issues.
ME4.2	Strategic Alignment	<i>Strategic Alignment</i> Enable board and executive understanding of strategic IT issues, such as the role of IT, technology insights and capabilities. Ensure that there is a shared understanding between the business and IT regarding the potential contribution of IT to the business strategy. Work with the board and the established governance bodies, such as an IT strategy committee, to provide strategic direction to management relative to IT, ensuring that the strategy and objectives are cascaded into business units and IT functions, and that confidence and trust are developed between the business and IT. Enable the alignment of IT to the business in strategy and operations, encouraging co-responsibility between the business and IT for making strategic decisions and obtaining benefits from IT-enabled investments.
ME4.3	Value Delivery	<i>Value Delivery</i> Manage IT-enabled investment programs and other IT assets and services to ensure that they deliver the greatest possible value in supporting the enterprise's strategy and objectives. Ensure that the expected business outcomes of IT-enabled investments and the full scope of effort required to achieve those outcomes are understood; that comprehensive and consistent business cases are created and approved by stakeholders; that assets and investments are managed throughout their economic life cycle; and that there is active management of the realization of benefits, such as contribution to new services, efficiency gains and improved responsiveness to customer demands. Enforce a disciplined approach to portfolio, program and project management, insisting that the business takes ownership of all IT-enabled investments and IT ensures optimization of the costs of delivering IT capabilities and services.
ME4.4	Resource Management	<i>Resource Management</i> Oversee the investment, use and allocation of IT resources through regular assessments of IT initiatives and operations to ensure appropriate resourcing and alignment with current and future strategic objectives and business imperatives.

Appendix - Normenkader IT Governance

ID	Cobit domein	Control
ME4.5	Risk Management	<p><i>Risk Management</i></p> <p>Work with the board to define the enterprise's appetite for IT risk, and obtain reasonable assurance that IT risk management practices are appropriate to ensure that the actual IT risk does not exceed the board's risk appetite. Embed risk management responsibilities into the organization, ensuring that the business and IT regularly assess and report IT-related risks and their impact and that the enterprise's IT risk position is transparent to all stakeholders.</p>
ME4.6	Performance Measurement	<p><i>Performance Management</i></p> <p>Confirm that agreed-upon IT objectives have been met or exceeded, or that progress toward IT goals meets expectations. Where agreed-upon objectives have been missed or progress is not as expected, review management's remedial action. Report to the board relevant portfolios, program and IT performance, supported by reports to enable senior management to review the enterprise's progress toward identified goals.</p>
ME4.7	Risk Management	<p><i>Independent Assurance</i></p> <p>Obtain independent assurance (internal or external) about the conformance of IT with relevant laws and regulations; the organization's policies, standards and procedures; generally accepted practices; and the effective and efficient performance of IT.</p>

Appendix - Normenkader Cyber Security

Phase	Beschrijving Control
Organization & Governance	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
Behaviour & Culture	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
Risk Analysis	The entity specifies objectives with sufficient clarity and identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
	The entity identifies and assesses changes that could significantly impact the system of internal control.
Third Party Management	The entity assesses and manages risks associated with vendors and business partners and communicates with these external parties regarding matters affecting the functioning of internal control.
Detection	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
Response	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, mitigate and communicate security incidents, as appropriate.



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.nl/about for a more detailed description of DTTL and its member firms.

Deloitte provides audit, consulting, financial advisory, risk management, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries bringing world-class capabilities, insights, and high-quality service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 225,000 professionals make an impact that matters, please connect with us on Facebook, LinkedIn, or Twitter.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.