Informatiebeveiliging binnen Nederlandse gemeenten: de basis op orde?

Mitchell van den Bogaart
Radboud Universiteit, Nijmegen
Faculteit der Managementwetenschappen

Master thesis 11-2022
Opleiding Bestuurskunde
Begeleidend docent: Prof. dr. I. Helsloot

Abstract

In december 2020 werd de gemeente Hof van Twente getroffen door een ransomware-aanval, waardoor nagenoeg de volledige gemeentelijke dienstverlenings- en bedrijfsvoeringsprocessen stil kwamen te liggen (IBD, 2021). Om gemeenten te doordringen van het belang van informatieveiligheid en de digitale weerbaarheid bij overheidsorganisaties te verhogen, is in 2019 door het Rijk de Baseline Informatiebeveiliging Overheid (BIO) geïntroduceerd. De BIO beschrijft verschillende beheersmaatregelen en aanvullende beveiligingsmaatregelen waar minimaal aan moet worden voldaan om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie(systemen) te kunnen waarborgen (CIP, 2021). Hoewel het belang hiervan regelmatig door gemeenten wordt erkend, blijkt uit diverse onderzoeken dat er nog maar weinig bekend is over wat de naleving met dit soort richtlijnen stimuleert. Op basis van literatuuronderzoek is er daarom binnen deze verkennende studie op zoek gegaan naar factoren die een positieve invloed uitoefenen op de naleving van de Baseline Informatiebeveiliging Overheid binnen Nederlandse gemeenten. Geïnspireerd door rationalistische- en normatieve compliance theorieën, wordt binnen dit onderzoek verondersteld dat de factoren bestuurlijke toewijding, interne controle en informatiebeveiligingsbewustzijn de mate van compliance met de BIO binnen gemeenten positief beïnvloeden. Uit de resultaten van dit onderzoek werd duidelijk dat alleen de factor informatiebeveiligingsbewustzijn een significante invloed uitoefent op de naleving van de BIO binnen gemeenten. Vanwege het relatief sterke effect dat bij deze relatie werd gevonden, kon worden verondersteld dat gemeentelijke inspanningen om het informatiebeveiligingsbewustzijn te verhogen de naleving van de BIO positief beïnvloedt. Bij de overige twee factoren werd daarentegen geen significant verband gevonden.

Introductie

Sinds de komst van het internet spelen informatie- en communicatiesystemen een steeds belangrijkere rol in ons dagelijks leven (Amiri & Woodside, 2017). We shoppen online, communiceren met elkaar via WhatsApp en ook werken we steeds vaker vanuit huis. Digitalisering bevindt zich tegenwoordig dan ook binnen alle aspecten van ons leven en verandert de interactie tussen mens en leefomgeving aanzienlijk (Jardas Antonić & Segota, 2012).

Ook binnen Nederlandse gemeenten is digitalisering geen nieuw fenomeen: waarbij in de jaren negentig technische innovaties bijvoorbeeld al werden ingezet om de administratieve controle te vergroten, innoveert de gemeentelijke dienstverlening zich tegenwoordig in een snel tempo (Meijer & Bekkers, 2015; Digitale overheid, 2020). Informatie- en communicatiesystemen (ICT) zijn in sterke mate verweven met de dienstverleningsprocessen van gemeenten en maken daarnaast steevast onderdeel uit van de gemeentelijke ambitie om de dienstverlening de komende jaren nog gebruiksvriendelijker, toegankelijker en efficiënter aan burgers te verlenen (VNG, 2022; Lindgren et al., 2019). Burgers hoeven bijvoorbeeld al lang niet meer fysiek naar een stadskantoor, maar regelen hun zaken met gemeenten gemakkelijk en overzichtelijk digitaal.

Hoewel deze technologische vooruitgang duidelijk verschillende maatschappelijke voordelen creëert, leidt de toegenomen afhankelijkheid van deze systemen ook tot de blootstelling aan enkele serieuze nieuwe risico's (NCSC, 2018). In december 2020 werd de gemeente Hof van Twente bijvoorbeeld nog getroffen door een ransomware-aanval, waardoor nagenoeg de volledige gemeentelijke dienstverlenings- en bedrijfsvoeringsprocessen stil kwamen te liggen (IBD, 2021). Hierdoor konden burgers tijdelijk geen paspoorten en identiteitskaarten aanvragen en liep de uitbetaling van uitkeringen in de essentiële decembermaand vertraging op.

Om de stabiliteit en continuïteit van de digitale dienstverlening te kunnen blijven garanderen, is het voor gemeenten van belang om zorgvuldig met data om te gaan en daarnaast op een adequate wijze te beveiligen (Hingh & Lodder, 2017, p. 27). Dit gaat volgens internationale standaarden over het vaststellen van de vereiste beveiliging van informatiesystemen in termen van beschikbaarheid, integriteit en vertrouwelijkheid alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen (ISO, 2013). Informatiebeveiliging is volgens deze beschrijving geen product of technologie, maar een proces waarbij het van belang is dat de volledige organisatie zich bewust is van de potentiële digitale risico's (Von Solms et al., 2013). Een informatiebeveiligingsincident, zoals bij de gemeente Hof van Twente, raakt namelijk de volledige bedrijfsvoering en is daarom niet enkel een technische uitdaging, maar vraagt ook om bestuurlijke visie, focus en draagvlak (VNG, 2013). Om bestuurders te doordringen van het belang van informatieveiligheid en de digitale weerbaarheid bij

overheidsorganisaties te verhogen, is in 2019 door het Rijk de Baseline Informatiebeveiliging Overheid (BIO) geïntroduceerd. Dit vernieuwde uniforme normenkader, gebaseerd op de internationaal erkende standaarden NEN-ISO/IEC 27001: 2017 bijlage A en NEN-ISO/IEC 27002:2017, beoogt de beveiliging van informatie(systemen) bij alle bestuursorganen van de overheid te bevorderen, zodat erop kan worden vertrouwd dat onderling uitgewisselde gegevens, in lijn met wet- en regelgeving, passend beveiligd zijn (CIP, 2021)

Concreet beschrijft de BIO verschillende beheers- (controls) en aanvullende beveiligingsmaatregelen waar minimaal aan moet worden voldaan om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie(systemen) te kunnen waarborgen (CIP, 2021). Vanwege de snelle ontwikkeling van techniek en bijbehorende dreigingen, wordt bij de implementatie van deze maatregelen ook benadrukt dat dit geen eenmalige taak, maar een continu verbeterproces is waarin de actualiteit en volledigheid van beveiligingsmaatregelen regelmatig moet worden vergeleken met de actuele dreigingen. Risicoafwegingen door bestuurders en een cyclische benadering (Plan-Do-Check-Act) van informatiebeveiliging, spelen daarom een belangrijke rol binnen de BIO en zijn bepalend om als gemeente volwassen met informatiebeveiliging om te gaan (CIP, 2021).

Het op orde krijgen van deze 'basis' door te voldoen aan de BIO, is een opgave die voor veel gemeenten echter niet van de ene op de andere dag is geregeld. De BIO bevat namelijk een breed aantal technische, fysieke en organisatorische maatregelen die niet enkel op strategisch niveau, maar door de volledige organisatie dienen te worden geïmplementeerd en nageleefd (CIP, 2021) Hoewel gemeenten zich bewust zijn van deze opgave, blijkt uit diverse onafhankelijke onderzoeken geïnitieerd door gemeentelijke Rekenkamers dat essentiële basismaatregelen- en processen bij een groot aantal gemeenten nog onvoldoende aanwezig zijn of ontbreken (Deben, 2021; IB&P, 2021). Ook de Informatiebeveiligingsdienst (IBD) die gemeenten ondersteunt bij de implementatie van de BIO, geeft op basis van incidentenanalyses aan dat een groot aantal gemeenten nog doorlopend stappen te zetten hebben om deze 'basishygiëne' te waarborgen (IBD, 2021). Zij signaleert grote verschillen in de volwassenheid waarmee gemeenten aan de slag gaan met informatiebeveiliging en waarschuwt dat deze basis snel 'op orde' dient te worden gebracht om basale dreigingen tegen processen te kunnen detecteren en pareren (IBD, 2021; NCSC, 2018).

Diverse onderzoeken op het gebied van informatiebeveiliging benadrukken het belang van baselines en (inter)nationale beveiligingsstandaarden voor een effectieve bescherming van informatiesystemen (Saint-Germain, 2005; Von Solms, 2001). Naast dat zij organisaties van een structuur voorzien om technische en socio-organisatorische beheersmaatregelen binnen een organisatie te configureren (Killmeyer, 2006), is het voldoen aan richtlijnen ook een belangrijk middel om legitimiteit te verwerven (Crowther et al., 2010). Door te voldoen aan baselines en beveiligingsstandaarden kunnen organisaties aantonen dat beveiligingsinspanningen op een consistente en herhaalbare wijze worden uitgevoerd, waaruit blijkt dat zij informatiebeveiliging serieus nemen (Silva et al., 2016). Dit draagt bij aan het vertrouwen van burgers en controlerende instanties in de wijze waarop een organisatie rechtmatig en veilig gegevens verwerkt.

Hoewel het voldoen aan baselines en beveiligingsstandaarden volgens de literatuur dan ook verschillende belangrijke voordelen bieden, zijn er weinig onderzoeken bekend die factoren identificeren die eraan bijdragen aan dit soort richtlijnen te voldoen. Aanvullend op deze lacune, is het doel van dit onderzoek om kennis te vergaren over factoren die van invloed zijn op BIO-compliance, teneinde de digitale weerbaarheid van gemeenten te verhogen. Hiervoor is de volgende onderzoeksvraag opgesteld: *Welke factoren zijn van invloed op de naleving van de Baseline Informatiebeveiliging Overheid door Nederlandse gemeenten?*

Voor de beantwoording van deze onderzoeksvraag is dit artikel als volgt ingedeeld. Allereerst zal er theoretisch worden verkend wat het begrip compliance nu eigenlijk inhoudt en welke factoren compliance bevorderen of ontmoedigen. Vervolgens zal op basis van deze inzichten het conceptueel model van dit onderzoek worden gepresenteerd, met aansluitend de wijze waarop er data is verzameld- en geanalyseerd. Afsluitend zullen de resultaten van dit onderzoek alsmede de conclusies worden beschreven waarmee de onderzoeksvraag kan worden beantwoord.

Theoretisch kader

Het begrip compliance

Naar aanleiding van de voortdurende- en snel ontwikkelende dreiging van cyberaanvallen, worden inspanningen om informatie te beveiligen in toenemende mate gemandateerd door overheidsregulering en aanvullende beveiligingsstandaarden (Alkabani et al., 2017). Richtlijnen zoals wettelijke eisen, baselines en IT-managementstandaarden vormen namelijk een belangrijk kader voor het configureren en managen van beveiligingssystemen (Peltier, 2016). Zij voorzien organisaties van inzichten waarop zij een effectieve beveiligingsstrategie kunnen vaststellen en bieden daarnaast referenties om organisationele processen en procedures te herhalen en evalueren. Aan de hand van dit soort 'controls' kunnen organisaties tevens vaststellen in hoeverre zij voldoen aan (minimale) beveiligingsvereisten, die voortkomen uit wettelijke verplichtingen of sectorspecifieke best practices (Kluge & Sambasivlam, 2008).

Wanneer er wordt gesproken over de mate waarin organisaties voldoen aan dit soort voorgeschreven beveiligingsvereisten, komt het begrip compliance bij veel mensen al snel ter gedachte. Hoewel er geen algemeen geaccepteerde definitie van dit begrip bekend is, wordt compliance in de meeste onderzoeken gedefinieerd als de mate waarin er wordt voldaan- en gehandeld naar- wet- en

regelgeving (Checkel, 2001; MacLean & Behnam, 2010) of andere voorgeschreven normen zoals (inter)nationale standaarden en intern beleid (Étienne, 2010). In brede zin heeft compliance dan ook betrekking op de mate waarin een organisatie of individu zich conform een expliciet of impliciet verzoek van anderen gedraagt (ten Have, 2014; Cialdini & Trost, 1998). Dit maakt compliance volgens enkele onderzoeken een kwestie van gedragsmotivatie en is om deze reden ook regelmatig terug te vinden binnen zowel de sociologische als de psychologische literatuur. Enkele auteurs uit deze disciplines merken op dat compliance niet enkel een status is die kan worden bereikt, maar ook kan worden gezien als een doorlopend proces (Doganata, 2012) dat samenhangt met een onderliggend doel, zoals het creëren van transparantie of het opdoen van legitimiteit (Tyler & Jackson, 2014). Compliance betreft vanuit het perspectief van deze verschillende vakgebieden dan ook een breed en relatief complex begrip, waarvan de feitelijke betekenis sterk afhankelijk is van de context waarin het wordt gebruikt.

Binnen dit onderzoek is in navolging op de studie van Foorthuis (2012) compliance gedefinieerd als de mate waarin een actor zich overeenkomstig gedraagt- en aantoonbaar handelt naar- vooraf gedefinieerde en tevens expliciete normen die aan hen zijn opgelegd. Uit deze definitie kan allereerst worden ontleend dat compliance verder gaat dan enkel de implementatie van voorgeschreven normen. Het aantoonbaar handelen hiernaar vraagt namelijk om inspanningen die ertoe doen geloven dat normen ook daadwerkelijk door een organisatie zijn geadopteerd (Weitzner, 2008; Foorthuis, 2012). Om deze reden bevat compliance een belangrijk verantwoordingsaspect, waarbij de activiteiten die in lijn met normen worden uitgevoerd moeten worden gedocumenteerd en vervolgens worden gecontroleerd aan de hand van audits (Saleh, 2011). Deze onafhankelijke blik helpt organisaties een inzicht te verkrijgen in lacunes binnen de bestaande beveiligingssystemen en toont daarnaast de voortgang aan waarin beveiligingsmaatregelen worden geïmplementeerd (Diéguez et al., 2012). Bij gemeenten wordt hiervoor de laatste jaren gebruik gemaakt van ENSIA (Eenduidige Normatiek Single Information Audit), die de verantwoording richting de gemeenteraad en toezichthouders structureert en zo de staat van informatieveiligheid op basis van de BIO, op een effectieve wijze helpt over te brengen. Hoewel deze methode zeer bruikbaar is voor een inzicht in de handelingen die worden verricht om compliance te bereiken, kan worden opgemerkt dat op deze wijze echter niet gelijk duidelijk wordt in hoeverre organisaties zich ook overeenkomstig een richtlijn gedragen. Om deze reden wordt er binnen enkele gemeenten ook gebruik gemaakt van het NBA- volwassenheidsmodel, die de conformiteit met BIO- en ISO-normen uitdrukt in vijf opeenvolgende volwassenheidsniveaus (NBA, 2019). Deze niveaus variëren van initieel (niveau 1) tot continu verbeterend (niveau 5) en geven een belangrijk inzicht in het groeiproces van de compliancefuncties binnen gemeenten. Pas vanaf niveau 3 (gedefinieerd) kan volgens dit volwassenheidsmodel worden gesteld dat informatiebeveiliging binnen de bedrijfsprocessen zijn geborgd en digitale risico's gestructureerd en gedocumenteerd worden beheerst (Ibid.). In auditermen kan de opzet, bestaan én werking van beveiligingsmaatregelen vanaf dit niveau worden aangetoond en is dan ook het minimale niveau dat dient te worden bereikt om compliance met de BIO aan te kunnen tonen (NBA, 2019; CIP, 2021).

Een fundamentele blik op compliance

Binnen diverse wetenschappelijke vakgebieden is er al eerder stilgestaan bij de vraag wat (non)-compliance met voorgeschreven normen en richtlijnen bij organisaties nu eigenlijk verklaart. Uit deze literatuur is een breed aantal theorieën te onderscheiden die elk unieke inzichten bieden in het onderliggend gedrag en bijbehorende motivaties gerelateerd aan compliance. Hathaway (2002) classificeert deze theorieën en maakt een onderscheid tussen een rationalistische- en normatieve stroming compliance theorieën. Hoewel er verschillende aanvullingen op deze twee stromingen bestaan (denk aan het realisme, institutionalisme en constructivisme), zal in navolging op de onderzoeken van Foorthuis (2012) en Wolman (2015) deze oorspronkelijke tweedeling worden gebruikt om een beter inzicht te verkrijgen in causale mechanismen en onderliggende verklaringen van (non)-compliance.

Rationalistische theorieën

De eerste fundamentele stroming aan compliance-theorieën kenmerkt zich volgens Hathaway (2002) als rationalistisch en is gebaseerd op de overtuiging dat actoren uit verschillende alternatieven altijd de afgewogen keuze maken die hun eigen belangen het beste behartigen (Shiffman, 2005; Hathaway, 2002). Bij deze theorieën wordt in de meeste gevallen een 'logic of consequences' gebruikt om te beargumenteren dat actoren vaste gedragspreferenties bezitten en er bewust voor kiezen wel of niet te voldoen aan voorgeschreven normen, door de gepercipieerde consequenties hiervan nauwkeurig af te wegen (Foorthuis, 2012; Wolman, 2015). Sommige onderzoekers beschrijven deze afweging daarom ook wel als een kosten-batenanalyse, gezien voor elk alternatief de verwachte kosten en baten worden gecalculeerd en hier vervolgens de optie uit wordt gekozen die voor hen het meest gunstig uitvalt (Johnston, 2002). Vanuit dit rationele perspectief vindt compliance dan ook vooral plaats in de gevallen waarin de baten van compliance de kosten overstijgen. Dit maakt compliance volgens enkele onderzoeken beïnvloedbaar, gezien de kosten of baten van de afweging met intentie kunnen worden gemanipuleerd. Zo kunnen sancties volgens het afschrikkingsmodel van Becker (1968) worden ingezet om non-compliance onaantrekkelijker te maken, maar kunnen beloningen organisaties ook juist motiveren zich te committeren aan voorgeschreven normen (Shiffman, 2005). Het is duidelijk dat actoren vanuit het rationele perspectief vooral uitgaan van nutsmaximalisatie en compliance om deze reden uitsluitend een strategische keuze betreft.

Normatieve theorieën
Naar aanleiding van kritiek op rationalistische theorieën is er volgens Hathaway (2002) vanaf de jaren 90 een alternatieve stroming aan compliance theorieën zichtbaar. Deze normatieve stroming veronderstelt dat het gedrag van organisaties niet enkel verklaard kan worden op basis van eigen belang of kosten-baten analyses, maar stelt dat werknemers binnen organisaties door morele- en ethische waarden over het algemeen al de voorkeur of neiging bezitten te voldoen aan voorgeschreven normen (Koops, 2014). Non-compliance betreft vanuit dit perspectief dan ook geen bewuste of strategische beslissing, maar komt voort uit een capaciteitsprobleem dat zich volgens Mitchell (1996) vormt door een tekort aan middelen, kennis of commitment. In lijn met deze gedachte, stellen Chayes & Chayes (1993) dat compliance daarom ook niet gesanctioneerd, maar gemanaged dient te worden. Zo zijn het creëren van awareness, het beschikbaar stellen van budget en het evalueren van prestaties volgens hen belangrijke strategieën om organisaties gemakkelijker aan voorgeschreven normen te laten voldoen en ze deze bovendien ook beter leren te begrijpen (Chayes & Chayes, 1993).

Compliance bij gemeenten
Hoewel rationele- en normatieve theorieën elk een unieke blik op verklaringen van compliance bieden, is er binnen dit onderzoek voor gekozen een hoofdzakelijk normatief uitgangspunt te hanteren. Hier is voor gekozen op basis van inzichten uit de stewardship theorie van Davis et al. (1997), die stellen dat publieke managers niet enkel vanuit hun eigen belang handelen, maar ook een sterke intrinsieke motivatie bezitten om het 'goede' te doen. Andere onderzoeken spreken binnen deze context ook wel over een 'professionaliteit' die gepaard gaat met een plichtsgevoel om collectieve doelen na te streven (Schillemans, 2013). Deze houding legt een belangrijke vertrouwensbasis bij het delegeren van taken en leidt in de meeste gevallen ook tot een minder dwingende sturingsrelatie (Contrafatto, 2014). Wanneer er met deze blik wordt gekeken naar de wijze waarop de BIO is opgelegd aan gemeenten, valt op dat er geen sancties of beloningen zijn verbonden aan het navolgen van dit normenkader. Gemeenten hebben zich daarentegen zelf de verplichting opgelegd aan de BIO te voldoen, vanwege het maatschappelijk belang dat deze richtlijn dient (CIP, 2021). Dit maakt dat er kan worden verondersteld dat er een vertrouwen bestaat dat gemeenten, zonder de aanwezigheid van extrinsieke motivatoren, de normen uit de BIO toch in acht zullen nemen. Vanuit deze assumptie lijkt een normatieve oorzaak voor (non)-compliance hier dan ook meer voor de hand liggend, wat de onderzoeker ertoe heeft laten besluiten dit uitgangspunt primair te gebruiken bij het identificeren van verklarende variabelen voor compliance. Omdat een rationele oorzaak van (non)-compliance echter niet volledig kan worden uitgesloten, is ervoor gekozen tevens één rationele variabele mee te nemen in de analyse van het onderzoek. Deze criteria hebben uiteindelijk geleid tot de selectie van de variabelen bestuurlijke toewijding, interne controle en organisationele awareness, die binnen de volgende paragrafen van dit hoofdstuk individueel zullen worden toegelicht.

Hypothesen en onderzoeksmodel

Bestuurlijke toewijding
Binnen de managementliteratuur zijn er verschillende onderzoeken bekend die zich richten op factoren die van invloed zijn op het succesvol managen van (informatie)beveiliging binnen organisaties (Boss et al., 2009; Bulcurgu et al., 2010; Knapp et al., 2006). Het overgrote deel van deze onderzoeken benadrukt dat de toewijding van het topmanagement of bestuur van een organisatie een cruciale voorwaarde is voor het succes van elke inspanning die wordt genomen om beveiligingsprestaties te behalen (Knapp et al., 2006) en te voldoen aan voorgeschreven normen en standaarden (Alkalbani et al., 2015; Hu et al., 2012; Alkalbani et al., 2016). Als de top informatiebeveiliging immers niet belangrijk acht, is de kans ook erg klein dat dit daadwerkelijk binnen een organisatie gaat leven (Straub, 1989). De term bestuurlijke toewijding wordt binnen dit onderzoek gedefinieerd als de beslissingen, investeringen en acties die door een bestuur worden ondernomen om een informatiebeveiligingsstrategie binnen een organisatie af te dwingen (Knapp et al., 2006). Toewijding van het bestuur gaat dan ook vooral om de inspanningen die ertoe leiden dat de beoogde resultaten van het strategische informatiebeveiligingsbeleid worden behaald. Hierbij kan allereerst worden gedacht aan het beschikbaar stellen van voldoende middelen voor een effectieve implementatie. Dit is essentieel gezien het voldoen aan normen in de meeste gevallen vraagt om de nodige aanpassingen van bedrijfsprocessen en de verzorging van extra trainingen, die bij de afwezigheid van voldoende middelen onwaarschijnlijk tot stand komen (Amoako-Gyampah et al., 2018). Hiernaast verbindt de zichtbare steun en betrokkenheid van bestuurders de werknemers in een belangrijke zin met de veranderingen die plaatsvinden om beveiligingsmaatregelen te implementeren **(**Merhi & Ahluwalia, 2015**).** Hierdoor kan eventuele weerstand tegen deze merkbare veranderingen worden weggenomen, waardoor informatiebeveiliging gemakkelijker kan worden opgenomen in de cultuur van een organisatie (Ma et al., 2009). Op basis van deze inzichten wordt verwacht dat:

H1: Bestuurlijke toewijding oefent een positieve invloed uit op de naleving van de BIO binnen Nederlandse gemeenten

Informatiebeveiligingsbewustzijn
Waar informatiebeveiliging voor een lange tijd vooral werd gezien als een technische opgave, wordt er tegenwoordig duidelijk meer aandacht besteedt aan (socio)organisatorische aspecten van informatiebeveiliging (Dhillon & Backhouse, 2001; Chang & Ho, 2006). Ingezien wordt dat louter het nemen van technische maatregelen onvoldoende is om de veiligheid van informatiesystemen te waarborgen. Ondanks dat empirisch en anekdotisch bewijs laat zien dat organisaties meer investeren in technische oplossingen, blijft het aantal beveiligingsincidenten

toenemen (Bulgurcu et al., 2010; Sohrabi Safa, von Solms, Furnell, 2016). Dit komt doordat (on)bewust menselijk gedrag van werknemers een significante invloed uitoefent op de effectiviteit van aanwezige beveiligingsmaatregelen (Sindhuja & Kunnathur, 2015; Dhillon & Backhouse, 2001; Alotaibi et al., 2016). Onachtzaamheid of onbegrip van werknemers creëert inherente kwetsbaarheden waar kwaadwillenden slim gebruik van maken om alsnog toegang te verkrijgen tot beveiligde informatiesystemen. Niet voor niets is het grootste deel van de beveiligingsincidenten te herleiden naar (on)bewust menselijk gedrag en staan werknemers alom bekend als een zwakke schakel op het gebied van informatiebeveiliging (Von Solms, 2001; Broderick, 2006).

Tegen deze achtergrond wordt al geruime tijd beargumenteerd dat Information Security Awareness (ISA) ofwel het informatiebeveiligingsbewustzijn binnen organisaties een van de belangrijkste componenten is om organisationele doelstellingen op het gebied van informatiebeveiliging te bereiken en te voldoen aan voorgeschreven richtlijnen (D'arcy et al., 2009; Thompson & von Solms, 1998). Het informatiebeveiligingsbewustzijn, dat in navolging op Siponen (2000) is gedefinieerd als een staat waarin werknemers zich bewust zijn van- en idealiter gecommitteerd zijn- aan de opgestelde beveiligingsstrategie, weerspiegelt namelijk in belangrijke mate de kennis die werknemers bezitten over risico's die gepaard gaan met het gebruik van digitale systemen. Deze kennis is van essentieel belang, gezien het werknemers beter in staat stelt bedreigingen op het gebied van informatiebeveiliging te identificeren (Haeussinger & Kranz, 2013) en daardoor ook het belang van beveiligingsmaatregelen beter inzien (D'arcy et al., 2009).

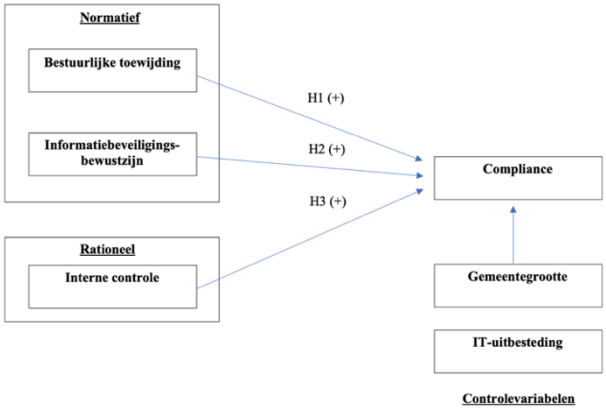
Volgens Bulgurcu et al. (2010) wordt dit veiligheidsbewustzijn vooral opgebouwd door directe levenservaringen, zoals het meemaken van een cyberaanval of het ontvangen van een sanctie voor het niet naleven van beveiligingsvoorschriften. Verschillende onderzoeken vullen hier echter op aan dat trainingen en bewustzijnsprogramma's voor dit doel onmisbaar zijn, gezien op deze wijze het gedrag van werknemers in positieve zin kan worden beïnvloed (Ma et al., 2009; D'Arcy, 2009). Door werknemers de goede kant op te sturen, kunnen (on)bewuste handelingen van werknemers worden tegengegaan en helpt dit organisaties volwassener om te gaan met het beschermen van informatie. Op basis van deze inzichten wordt verwacht dat:

H2: Informatiebeveiligingsbewustzijn oefent een positieve invloed uit op de naleving van de BIO binnen Nederlandse gemeenten

Interne controle

Doordat organisaties en werknemers doorgaans uiteenlopende doelen bezitten, is het volgens diverse onderzoeken van essentieel belang dat organisaties in staat zijn een redelijke mate van zekerheid te verkrijgen dat strategische doelstellingen worden bereikt en er daadwerkelijk wordt voldaan aan relevante wet- en regelgeving (Liang et al., 2013). Tegen deze achtergrond vormt het begrip (interne) controle al geruime tijd een centraal concept binnen de managementliteratuur (Ouchi, 1979; Kirsch, 1996) en krijgt het de afgelopen jaren ook significant meer aandacht bij onderzoeken op het gebied van informatiebeveiliging (Hong et al., 2003; Boss et al., 2009). In navolging op de onderzoeken van Ouchi (1979) en Flamholtz (1985) is het begrip controle hier gedefinieerd als de pogingen van een organisatie om de acties en het gedrag van werknemers zo te beïnvloeden dat dit ertoe leidt dat organisatiedoelstellingen worden bereikt. In brede zin beoogt controle dan ook uiteenlopende belangen of verwachtingen op elkaar af te stemmen, door kenbaar te maken welk gedrag er van werknemers wordt verwacht. Hierbij is het volgens Boss et al. (2009) allereerst van kritisch belang het gewenste gedrag te specificeren in formeel gedocumenteerde procedures zoals een informatiebeveiligingsbeleid. Dit helpt bestuurders het gewenste gedrag af te stemmen op de compliancedoelstellingen, waardoor het voor werknemers duidelijk wordt wat er van hen wordt verwacht (ten Have, 2014). Wanneer deze richting is gespecificeerd, is het vervolgens aan bestuurders of managers om het gedrag te monitoren of evalueren. Op deze wijze wordt inzichtelijk of het gedrag van werknemers niet verslapt en helpt dit garanderen dat een organisatie daadwerkelijk aan de voorgeschreven normen voldoet (Boss et al., 2009). Dit maakt dat er wordt verwacht dat:

H3: Interne controle oefent een positieve invloed uit op de naleving van de BIO binnen Nederlandse gemeenten



Figuur 1: Onderzoeksmodel

Controlevariabelen

Het theoretisch model dat de geformuleerde hypothesen en hun onderlinge relaties weergeeft wordt getoond in figuur 1. Binnen dit model is zichtbaar dat gemeentegrootte en IT-uitbesteding als controlevariabelen zijn opgenomen binnen dit onderzoek. In de bestudeerde literatuur wordt namelijk regelmatig verondersteld dat organisatiegrootte significant is verbonden met het behaalde complianceniveau binnen verschillende sectoren (Straub, 1989; Chang & Ho, 2006). In deze onderzoeken wordt beargumenteerd dat grotere organisaties meer budget bezitten voor kosten op het gebied

van informatiebeveiliging en er hierdoor beter in slagen beveiligingsmaatregelen en procesveranderingen te implementeren. Ook vonden Solomon & Brown (2019) dat grotere organisaties vaker een bestaande cultuur bezitten waarin individuen intuïtief de voorgeschreven regels begrijpen en om deze reden ook actiever naleven. Aanvullend wordt bij deze onderzoeken de mate van IT-uitbesteding juist negatief in verband gebracht met het complianceniveau van organisaties. In het onderzoek van Bachlechner et al. (2014) wordt bijvoorbeeld aangehaald dat een sterke aanwezigheid van IT-uitbesteding kan leiden tot een verlies van controle op beveiligingsprocessen en zo ook tot de inventarisatie van compliancefuncties.

Methode

Het algemene doel van dit verkennend onderzoek is om factoren te identificeren die bijdragen aan de naleving van de BIO, teneinde de digitale weerbaarheid van gemeenten te verhogen. Binnen dit hoofdstuk zal worden toegelicht welke onderzoeksmethode is gehanteerd om de hypothesen gerelateerd aan deze doelstelling te toetsen.

Meetinstrument

De empirische data voor dit onderzoek is primair verzameld aan de hand van online surveys. Dit zijn schriftelijke enquêtes die met behulp van het internet worden verspreid onder een gekozen onderzoekspopulatie (Baarda et al., 2007). Er is voor deze methode gekozen, omdat op deze wijze in korte tijd een grote hoeveelheid personen kon worden bevraagd en respondenten daarnaast op hun eigen tempo vragen konden invullen, wat veelal positief uitpakt voor het responspercentage van een survey (Wright & Schwager, 2008). Het ontwerp van de survey is grotendeels gebaseerd op een mix van reeds gevalideerde onderzoeken op het gebied van compliance en informatiebeveiliging. Hieronder wordt toegelicht hoe deze survey is vormgegeven en op welke methode de variabelen van dit onderzoek zijn geoperationaliseerd. Dit helpt de lezer te begrijpen hoe de vragenlijst tot stand is gekomen en op welke wijze de betrokken variabelen zijn gemeten.

Compliance

Compliance met de BIO is gemeten aan de hand van een zelf-geconstrueerde compliance index van 4 items, die is gebaseerd op BIO-volwassenheidsindicatoren (NBA, 2019) en inzichten uit vergelijkbare onderzoeken (Checkel, 2001; Foorthuis, 2012). Op deze wijze is geprobeerd een beter inzicht te verkrijgen in de wijze waarop gemeenten omgaan met informatiebeveiliging en hoe volwassen zij daarnaast omgaan met het naleven van de BIO als overheidsbrede informatiebeveiligingsrichtlijn. Doordat compliance vanuit dit perspectief wordt gezien als een gradueel proces, is ervoor gekozen compliance niet als een dichotome variabele (wel of niet compliant) te meten, maar op een continue schaal. Elk item is om deze reden gemeten aan de hand van een stelling die is gecodeerd op basis van een 5-punts Likertschaal, met scores variërend van (1) volledig mee oneens tot (5) volledig mee eens.

Bestuurlijke-toewijding

Het overgrote deel van de literatuur beschrijft het begrip bestuurlijke toewijding als een heterogeen construct, waardoor er een breed aantal interpretaties over bestaan. Zo zijn leiderschap, ondersteuning, participatie en zichtbaarheid verschillende manifestaties van toewijding die worden benoemd binnen de aanwezige literatuur (Merhi & Ahluwalia, 2015; Knapp et al., 2006). In een poging deze uiteenlopende beschrijvingen samen te voegen tot een meetbaar construct, is gebruik gemaakt van de empirische analyse uitgevoerd door Boonstra (2013), die vijf essentiële gedragingen van bestuurlijke toewijding identificeert:

- Het bestuur stelt voldoende middelen beschikbaar om strategische projecten te ondersteunen en effectieve implementatie hiervan te garanderen.
- Het bestuur stelt een adequate structuur op om organisationele doelen te bereiken.
- Bestuurders ondersteunen strategische projecten door hier met zichtbare enthousiasme over te communiceren.
- Bestuurders doen voldoende kennis en expertise op van het beoogde strategische project.
- Bestuurders gebruiken hun autoriteit om strategische projecten te ondersteunen.

Doordat informatiebeveiliging een vakgebied is dat specifieke- en vooral technische kennis vereist, delegeren bestuurders veelal een groot aantal taken naar Chief Information Security Officers (CISO's) (Merhi & Ahluwalia, 2015). Zij worden in de meeste gevallen verantwoordelijk gesteld voor het opstellen van het informatiebeveiligingsbeleid en voor de verdere implementatie hiervan. Doordat bestuurders vanwege deze gedelegeerde verantwoordelijkheid niet per definitie inhoudelijke kennis over informatiebeveiliging nodig hebben en hun autoriteit daarnaast minder benodigd is dan bij andere strategische projecten, zijn tevens in navolging op het onderzoek van Merhi & Ahluwalia (2015) de eerste 3 van de 5 gedragingen als meetbare indicatoren voor bestuurlijke toewijding gebruikt. Dit heeft geleid tot het opstellen van vijf items voor dit construct, die elk aan de hand van stellingen zijn gemeten.

Interne-controle

Binnen dit onderzoek wordt aan de hand van het begrip interne controle geprobeerd te meten in hoeverre gemeenten pogingen ondernemen de acties en het gedrag van werknemers te beïnvloeden zodat beveiligingsdoelstellingen worden bereikt (Kirsch, 2004). Bij het meten van dit construct wordt in vergelijkbare onderzoeken een onderscheid gemaakt tussen een formele- en informele controlestrategie (Ouchi, 1979; Rustagi et al., 2008). Waarbij formele controlestrategieën vooral voortbouwen op mechanismen die het gedrag van werknemers trachten te beïnvloeden aan de hand van prestatiemetingen en evaluaties, wordt bij een informele controlestrategie vooral gebruik gemaakt van sociale beïnvloedingsmechanismen zoals groepsdruk. Doordat beide strategieën kunnen worden toegepast om de acties en het gedrag richting beveiligingsdoelstellingen te

bevorderen, is ervoor gekozen items voor elk van deze controlevormen op te stellen. Dit heeft uiteindelijk geleid tot drie items voor de dimensie formele controle en twee items voor het begrip informele controle die zijn ontleend uit de gevalideerde onderzoeken van Kirsch (1996) en Boss et al. (2009). Deze items zijn elk in lichte mate aangepast om ze bij de context van dit onderzoek te laten passen.

Informatiebeveiligingsbewustzijn
Het begrip informatiebeveiligingsbewustzijn meet de mate waarin gemeenten zich inspannen om kennis over informatiebeveiliging bij te brengen, met als doel dat het leden van de organisatie overtuigt hun gedrag ten aanzien van het gebruik van informatiesystemen te veranderen (Wolf et al., 2011). Drie items voor dit construct zijn afgeleid van de survey over informatiebeveiligingsbewustzijn die wordt gebruikt binnen de onderzoeken van D'Arcy (2009) en Bulgurcu et al. (2011). Deze items hebben betrekking op de mate waarin organisaties zich inzetten het belang van informatiebeveiliging over te brengen en de gepercipieerde kennis die werknemers bezitten over de informatiebeveiligingsstrategie van een organisatie.

Controlevariabelen
Doordat verschillende onderzoekers opmerken dat organisatiegrootte en de mate van IT-uitbesteding invloed uitoefenen op het managen van compliance (Solomon & Brown, 2019; Bachlechner et al. 2014), zijn de controlevariabelen gemeentegrootte en IT-uitbesteding aan de analyse van dit onderzoek toegevoegd. De controlevariabele gemeentegrootte is op basis van inwoneraantal ingedeeld in vijf klassen, die zijn ontleend van vergelijkbaar gemeentelijk onderzoek uitgevoerd door het Centraal Bureau voor de Statistiek (CBS). De controlevariabele IT-uitbesteding tracht te meten in hoeverre een gemeente zijn of haar systeembeheer en beveiligingsinspanningen uitbesteedt aan marktpartijen. Beiden zijn aan de hand van een 4-punts Likertschaal met scores variërend van (1) dit wordt niet uitbesteed tot (4) dit wordt volledig uitbesteedt uitgevraagd.

De operationalisatie van de latente variabelen heeft uiteindelijk geleid tot een vragenlijst van 17 items, die in zijn volledigheid is opgenomen in bijlage 1 van dit onderzoek. Deze survey is in testvorm voorgelegd aan een IT-auditor en een CISO met ervaring binnen het gemeentelijk domein, voordat deze onder de onderzoekspopulatie is verspreid. Naar aanleiding van enkele contextuele opmerkingen is de vragenlijst licht aangepast en vervolgens in definitieve vorm onder de onderzoekspopulatie verspreid middels het online surveyprogramma Qualtrics.com. Het verzamelen van de data heeft in totaal circa acht weken geduurd, waarbij er aan het einde van de achtste week nog een herinneringsbericht is gestuurd aan alle benaderde respondenten. Dit helpt volgens Van Mol (2017) namelijk bij het verhogen van het responspercentage van een survey en draagt zo ook indirect bij aan de generaliseerbaarheid van de onderzoeksresultaten.

Dataverzameling
Om meer te weten te komen over oorzaken van (non)-compliance ten aanzien van de BIO, is op zoek gegaan naar respondenten die technische en integrale kennis bezitten over informatiebeveiligingsprocessen binnen gemeenten. Op basis van deze criteria zijn in handreikingen van de Vereniging Nederlandse Gemeenten (VNG) en de Informatiebeveiligingsdienst (IBD) CISO's geïdentificeerd als primaire onderzoekspopulatie voor dit onderzoek. CISO's zijn er volgens deze documenten namelijk formeel mee belast informatiebeveiligingsbeleid van gemeenten te implementeren en dragen daarnaast de verantwoordelijkheid ervoor te zorgen dat gemeenten voldoen aan de BIO (VNG & IBD, 2020).

Doordat er echter niet direct in contact kon worden getreden met personen binnen deze specifieke onderzoekspopulatie, is het netwerk van de IT-organisatie waarvoor het onderzoek is uitgevoerd gebruikt om de respondenten te benaderen. Zo hebben leden van de IT-organisatie gemeentelijke CISO's binnen hun netwerk opgeroepen deel te nemen aan het onderzoek en hebben zij de onderzoeker daarnaast doorverwezen naar CISO's zodat er via sociale media met hen in contact kon worden gekomen. Het risico van deze aanpak is dat de IT-organisatie op deze wijze een 'gatekeeper' wordt en tussen de onderzoeker en potentiële respondenten in komt te staan (Lavrakas, 2008). Dit kan een significante impact uitoefenen op zowel de steekproef als de resultaten van het onderzoek, doordat een gatekeeper ervoor kan kiezen bepaalde respondenten niet te benaderen (Crowhurst & Kennedy-Macfoy, 2013). Bewust van deze invloed is hier echter toch voor gekozen, gezien de geselecteerde onderzoekspopulatie anders minder effectief kon worden bereikt en de generaliseerbaarheid van het onderzoek hierdoor mogelijk te sterk werd aangetast. Uit de 112 respondenten die hierdoor uiteindelijk zijn benaderd, zijn 51 volledig ingevulde vragenlijsten ontvangen, waarmee een responspercentage van 46% is bereikt. Hierbij dient echter te worden opgemerkt dat niet de volledige onderzoekspopulatie van 344 gemeenten en zo ook CISO's kon worden bereikt, waardoor het werkelijke responspercentage op zo'n 16% ligt. Hoewel dit responspercentage als laag kan worden bestempeld, is een responspercentage van tussen de 15- en 20% niet ongebruikelijk bij surveys op het gebied van informatiebeveiliging (Kotulic & Clark, 2004). Het bereikte responspercentage van 16% kan op basis van deze kennis als acceptabel worden beschouwd.

Data-analyse en Resultaten

Analysemethode

Door het gebruik van statistische onderzoeksmethoden is het mogelijk om empirische relaties tussen een afhankelijke en (meerdere) onafhankelijke variabelen vast te stellen (Verbeek, 2017). Hierbij is het echter van cruciaal belang dat er kijkend naar het verband dat wordt verondersteld, de juiste analysemethode wordt geselecteerd (Field, 2017). Een foute keuze kan namelijk leiden tot problemen bij de interpretatie van bevindingen, waardoor de conclusie van het onderzoek mogelijk negatief wordt beïnvloed (Ibid.). Met dit in gedachten is ervoor gekozen de hypothesen binnen dit onderzoek te analyseren aan de hand van een Ordinary Least Square (OLS) regressieanalyse. Dit is een bekende multipele regressieanalyse die wordt gebruikt voor het voorspellen van waarden in lineaire regressiemodellen met data op schaalniveau (Field, 2017). Er is voor deze analysemethode gekozen doordat deze aansluit op het doel van dit onderzoek om de effecten van verschillende theoretisch afgeleide voorspellers van compliance als afhankelijke variabele te evalueren en vergelijken. Bij het gebruik van deze methode is het echter van belang dat de geanalyseerde data aan enkele statistische assumpties voldoet. Zo moet iedere relatie daadwerkelijk lineair van aard zijn, moet er worden voldaan aan de assumptie van multicollineariteit en homoscedasticiteit en dienen de residuen ten slotte normaal verdeeld te zijn (Field, 2017, p. 387-388). Uit het toetsen van deze assumpties werd met behulp van het statistisch programma SPSS v.20 allereerst duidelijk dat multicollineariteit geen probleem was, gezien de variantie- inflatiefactor (VIF) van de data laag was (<1.59). De geplotte histogrammen lieten daarnaast zien dat de data normaal verdeeld- en homoscedastisch was, waarmee aan de assumpties voor een lineaire regressieanalyse werd voldaan.

Deelnemende gemeente	Valid *N*	Percentage
Minder dan 5000 inwoners	2	3.9%
5000 tot 20.000 inwoners	9	17.6%
20.000 tot 100.000 inwoners	27	52.9%
100.000 tot 250.000 inwoners	9	17.6%
Meer dan 250.000 inwoners	4	7.8%
Totaal	51	100%

Tabel 1: Verdeling steekproef

Hiernaast werd uit de beschrijvende statistiek van de verzamelde data duidelijk dat de steekproef van dit onderzoek vooral bestond uit CISO's afkomstig uit middelgrote gemeenten van tussen de 20- en 100.000 inwoners (52.9%), wat de populatie van gemeenten in Nederland voldoende reflecteert. Een weergave van de verdere verdeling van deze steekproef is opgenomen in tabel 1. Uit de beschrijvende statistieken van de onderzoeksvariabelen zoals weergegeven in tabel 2, werd daarnaast duidelijk dat het gemiddelde van alle constructen boven- of net iets onder- de waarde 3 als het middelpunt van de 5-punts Likertschaal lag. Het algemeen resultaat liet verder zien dat bestuurlijke toewijding het meest belangrijke construct is van de gemeten variabelen. Dit is niet verrassend gezien bestuurders een enorm belangrijke rol spelen binnen de besluitvorming van een gemeente, vooral ten aanzien van het budget en de richting van het informatiebeveiligingsbeleid.

	Valid *N*	Minimum	Maximum	Gemiddelde	Standaard Deviatie
Compliance	51	2.00	4.25	3.12	0.53
Bestuurlijke Toewijding	51	1.33	4.67	2.99	0.75
Formele Controle	51	1.00	4.00	2.72	0.80
Informele Controle	51	1.50	4.50	2.81	0.89
Informatiebeveiligings-bewustzijn	51	1.00	4.00	2.68	0.75
Omvang Gemeenten	51	1.00	5.00	3.08	0.91
Uitbesteding systeembeheer	51	1.00	5.00	2.83	0.82
Uitbesteding beveiliging IT	51	1.00	5.00	2.80	0.92

Tabel 2: Beschrijvende statistiek onderzoeksvariabelen

Betrouwbaarheid en validiteit meetinstrument

Voordat de hypothesen van dit onderzoek zijn getoetst, is de betrouwbaarheid van het opgestelde meetinstrument vastgesteld door de schalen van de latente variabelen met behulp van Cronbach's Alpha (Cronbach's α) te controleren op interne consistentie. Uit deze analyse bleek allereerst dat de vijf items gerelateerd aan de variabele bestuurlijke toewijding gezamenlijk een Cronbach's Alpha van 0.46 produceerden, wat significant lager ligt dan de traditionele grenswaarde van 0.7. Uit de resultaten werd echter duidelijk dat de Cronbach's alpha kon worden verbeterd naar een waarde van 0.62 indien items 2.3 en 2.5 uit de schaal werden verwijderd. Hoewel hiermee de traditionele grenswaarde van 0.7 nog steeds niet werd bereikt, is er vanwege deze significante verbetering voor gekozen beide items uit de schaal te verwijderen en de schaal zo te accepteren. De Cronbach's alpha onderschat volgens Hinton et al. (2014) namelijk de interne consistentie van een latente variabele indien deze minder dan tien items bevat en/of de steekproefgrootte kleiner is dan 100. In dit geval is een grenswaarde van 0.55 volgens Hair et al (2006) acceptabel. Doordat er binnen dit onderzoek sprake is van een vrij unieke populatie die vanwege hun functie lastig te bereiken zijn, is deze aangepaste grenswaarde voor alle schalen binnen dit onderzoek gehanteerd.

Zoals is te zien in tabel 3 bereikten de overige variabelen formele- en informele controle een acceptabele Cronbach's alpha van boven de 0.55, maar eindigde deze waarde bij de latente variabele informatiebeveiligingsbewustzijn duidelijk lager (0.42). Hoewel de verwijdering van item 4.2 tot een significante verbetering van deze schaal leidde, werd de aangepaste basiswaarde van 0.55 alsnog niet behaald. Hoewel de schaal van deze latente variabele hierdoor minder betrouwbaar is dan die van de andere variabelen, is gezien het theoretisch belang van deze variabele besloten deze toch in deze vorm binnen het onderzoek te behouden.

Aspect	Cronbach's Alpha
Bestuurlijke toewijding	0.62
Formele controle	0.56
Informele controle	0.57
Informatiebeveiligings-bewustzijn	0.42

Tabel 3: Cronbach's alpha schalen

Toetsing van hypothesen

Zoals reeds is benoemd zijn de hypothesen van dit onderzoek getoetst met behulp van een OLS regressieanalyse. De onafhankelijke variabelen inclusief de controlevariabelen zijn hierbij gelijktijdig aan de regressieanalyse toegevoegd (enter methode), gezien er binnen dit onderzoek geen verwachting bestond dat voorspellers elkaar zouden beïnvloeden (Field, 2017). De resultaten van de regressieanalyse met hierin de (on)gestandaardiseerde coëfficiënten, standaardfouten en significantieniveaus worden weergegeven in tabel 4. Uit deze resultaten werd hiernaast duidelijk dat het gezamenlijke model ongeveer 25,6% van de variantie verklaart (R^2), wat gezien kan worden als een gemiddelde waarde bij regressieanalyses (Field, 2017).

	β (std. E.)	Beta
Compliance	2.12*** (0.63)	
Bestuurlijke toewijding	0.02 (0.11)	0.03
Formele Controle	0.24** (0.11)	0.18
Informele Controle	-0.08 (0.11)	-0.14
Informatiebeveiligings-bewustzijn	0.43* (0.11)	0.50
Omvang Gemeenten	0.07 (0.08)	0.12
Uitbesteding systeembeheer	0.00 (0.10)	0.00
Uitbesteding beveiliging ICT	-0.01 (0.09)	-0.02

$p < 0.001$*** $p < 0.01$ ** $p < 0.05$*

Tabel 4: Resultaten hypothesen

Rol van bestuurlijke toewijding

Uit de onderzoeksresultaten is allereerst gebleken dat bestuurlijke toewijding geen significante invloed uitoefent op de afhankelijke variabele compliance (H1: $\beta = 0.02$, $p > 0.5$). Op basis van deze bevinding kan de nulhypothese niet worden verworpen, waardoor binnen dit onderzoek moet worden aangenomen dat er geen verband bestaat tussen bestuurlijke toewijding en compliance met de BIO binnen gemeenten.

Effect van interne controle

Zoals aangegeven in de operationalisatie is het begrip interne controle onderverdeeld in twee meetbare variabelen. De variabele formele controle bleek allereerst op basis van de resultaten van dit onderzoek een significante invloed uit te oefenen op compliance met de BIO bij gemeenten ($\beta = 0.24$, $p < 0.1$). De variabele informele controle bleek daarentegen geen significante invloed uit te oefenen op de afhankelijke variabele ($\beta = -0.08$, $p > 0.05$). Omdat interne controle uit twee niet uitsluitbare variabelen bestaat, dienen beide verbanden significant te zijn om de nulhypothese te kunnen verwerpen. Omdat dit niet het geval is, kan er binnen dit onderzoek niet worden aangenomen dat er een significant relatie bestaat tussen interne controle en compliance met de BIO binnen gemeenten.

Effect van informatiebeveiligingsbewustzijn

De resultaten van dit onderzoek laten ten slotte zien dat de relatie tussen het gepercipieerde informatiebeveiligingsbewustzijn en compliance met de BIO significant kan worden bevonden (H3: $\beta = 0.43$, $p < 0.01$). Opvallend aan dit verband is het relatief sterke effect dat wordt gevonden, waarmee kan worden gesuggereerd dat de aandacht voor informatiebeveiligingsbewustzijn binnen een gemeente van essentieel belang is voor de mate waarin compliance met de BIO wordt bereikt. Concluderend kan de nulhypothese behorend bij deze variabele dan ook worden verworpen, waarmee hypothese 3 kan worden aangenomen.

Effect van de controlevariabelen

Gemeentegrootte bleek allereerst geen significante invloed uit te oefenen op het complianceniveau van gemeenten ($\beta = 0.07$, $p = > 0.05$), waardoor er kan worden gesuggereerd dat ondanks een gemeente bijvoorbeeld een kleiner inwonersaantal heeft, dit niet direct tot een lager complianceniveau leidt. Een andere mogelijke verklaring hiervoor is echter dat vanwege het relatief lage aantal deelnemende kleine gemeenten (< 20.000 inwoners), er onvoldoende variantie was in de steekproef om deze controlevariabele significant te maken (Field, 2017).
Naast gemeentegrootte werden beide vormen van IT-uitbesteding op basis van de onderzoeksresultaten als insignificant bevonden ($\beta = 0.00$, $p = > 0.05$ en $\beta = -0.01$, $p = > 0.05$). De toevoeging van de controlevariabelen leidde dan ook niet tot een significante bijdrage aan de gevonden onderzoeksresultaten.

Samengevat kon op basis van de resultaten worden vastgesteld dat hypothese 3 werd ondersteund, maar dat hypothesen 1 en 2 moesten worden verworpen. In de conclusie van dit onderzoek zal verder stil worden gestaan bij de betekenis van deze resultaten en zullen mogelijke verklaringen van de gevonden verbanden worden gepresenteerd.

Conclusie

Binnen deze verkennende studie is onderzocht welke factoren van invloed zijn op de naleving van de Baseline Informatiebeveiliging Overheid (BIO) door Nederlandse gemeenten. Op basis van rationalistische- en normatieve compliance theorieën is een onderzoeksmodel opgesteld waarin de factoren bestuurlijke toewijding, interne controle en informatiebeveiligingsbewustzijn zijn geïdentificeerd als positieve voorspellers van compliance volgens gemeentelijke CISO's. De verwachtingen uit dit onderzoeksmodel zijn vervolgens getoetst met behulp van een OLS-regressieanalyse. Uit de resultaten van deze analyse is gebleken dat er enkel een significante relatie bestond tussen het informatiebeveiligingsbewustzijn en de mate van compliance binnen gemeenten. Opvallend aan deze relatie is het relatief sterke effect dat hierbij is gevonden (0.43), waardoor er kan worden verondersteld dat compliance met de BIO wordt beïnvloed door de aandacht voor informatiebeveiligingsbewustzijn binnen een gemeente. Bij de overige twee factoren werd daarentegen geen significant verband gevonden.

Discussie

De insignificante relatie die werd gevonden tussen de andere twee factoren en compliance is in sterk contrast met de resultaten uit de onderzoeken van Hu et al. (2012) en Alkalbani et al (2015), waarbij de invloed van bestuurlijke toewijding en interne controle op compliance juist als sterk significant werd bevonden ($p < 0.01$). Een eerste mogelijke verklaring voor dit verschil is dat de steekproef van dit onderzoek relatief klein is, waarmee er potentieel onvoldoende variantie werd bereikt om de variabelen significant te maken (Field, 2017). In beide vergelijkbare onderzoeken is de steekproef namelijk groter dan 100 en zijn er minimaal 9 variabelen opgenomen in het onderzoeksmodel, waarmee een grotere dataset werd gevormd. Beide aspecten kunnen de effectsterkten van de veronderstelde relaties beïnvloeden en leiden dan ook mogelijk tot meer significante resultaten (Field, 2017). Een tweede mogelijke verklaring voor het insignificante verband tussen de variabele bestuurlijke toewijding en compliance is dat deze variabele mogelijk in te brede zin is geoperationaliseerd binnen dit onderzoek. Om dit uit te sluiten is de beschikbaarheid van middelen voor de CISO nog individueel met compliance in een regressiemodel opgenomen. Hierbij werd een significant verband gevonden ($\beta = 0.25$, $p < 0.05$), waardoor inderdaad kan worden gesuggereerd dat de variabele bestuurlijke toewijding in te brede zin is gemeten. De beschikbaarheid van middelen dient daarom in toekomstig onderzoek op een andere wijze geoperationaliseerd te worden.

Daarnaast is er binnen dit onderzoek hoofdzakelijk gekeken naar positieve voorspellers van compliance, terwijl negatieve factoren mogelijk nog meer aspecten van dit begrip hadden kunnen verklaren. Voor eventueel vervolgonderzoek wordt dan ook geadviseerd zowel positieve als negatieve voorspellers van compliance in het onderzoeksmodel op te nemen. Hiernaast is dit onderzoek enkel gebaseerd op de kennis die CISO's bezitten over de naleving van de BIO bij gemeenten. Om het onderzoek uit te breiden zou bij vervolgonderzoek afsluitend worden geadviseerd diverse functies waarbij kennis over complianceprocessen wordt verwacht, in de onderzoekspopulatie op te nemen. Op deze wijze kunnen mogelijk nieuwe perspectieven op compliance worden gevonden en kunnen deze daarnaast met elkaar worden afgewogen.

Literatuurlijst

AlKalbani, A., Deng, H., & Kam, B. (2015). Organisational security culture and information security compliance for e-government development: the moderating effect of social pressure.

AlKalbani, A., Deng, H., Kam, B., & Zhang, X. (2016). Investigating the impact of institutional pressures on information security compliance in organizations. *ACIS 2016 Proceedings*, *26*.

Alotaibi, M., Furnell, S., & Clarke, N. (2016). Information security policies: A review of challenges and influencing factors. 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST),

Amiri, S., & Woodside, J. M. (2017). Emerging markets: the impact of ICT on the economy and society. *Digital Policy, Regulation and Governance*, *19*(5), 383-396. https://doi.org/10.1108/DPRG-04-2017-0013

Amoako-Gyampah, K., Meredith, J., & Loyd, K. W. (2018). Using a social capital lens to identify the mechanisms of top management commitment: a case study of a technology project. *Project Management Journal*, *49*(1), 79-95.

Baarda, D. B., Goede, M. P. M., & Kalmijn, M. (2007). *Basisboek enquêteren: handleiding voor het maken van een vragenlijst en het voorbereiden en afnemen van enquêtes*. Wolters-Noordhoff.

Bachlechner, D., Thalmann, S., & Maier, R. (2014). Security and compliance challenges in complex IT outsourcing arrangements: A multi-stakeholder perspective. *Computers & Security*, *40*, 38-59. https://doi.org/https://doi.org/10.1016/j.cose.2013.11.002

Becker, G. S. (1968). Crime and Punishment: An Economic Approach. *Journal of Political Economy*, *76*(2), 169-217. http://www.jstor.org/stable/1830482

Boonstra, A. (2013). How do top managers support strategic information system projects and why do they sometimes withhold this support? *International Journal of Project Management*, *31*(4), 498-512.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems*, *18*(2), 151-164.

Broderick, J. S. (2006). ISMS, security standards and security regulations. *information security technical report*, *11*(1), 26-31.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 523-548.

Centrum Informatiebeveiliging en Privacybescherming (CIP). (2021). Criteria BIO-SA Uitleg van de 16 BIO-criteria en de volwassenheidsniveaus. https://cip-overheid.nl/media/1670/de-16-criteria-van-de-bio-sa-v10.pdf

Chang, S. E., & Ho, C. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management and Data Systems*, *106*, 345-361. https://doi.org/10.1108/02635570610653498

Chayes, A., & Chayes, A. H. (1993). On Compliance. *International Organization*, *47*(2), 175-205. http://www.jstor.org/stable/2706888

Checkel, J. T. (2001). Why Comply? Social Learning and European Identity Change. *International Organization*, *55*(3), 553-588. http://www.jstor.org/stable/3078657

Cialdini, R. B., & Trost, M. R. (1998). Social influence: Social norms, conformity and compliance. In *The handbook of social psychology, Vols. 1-2, 4th ed.* (pp. 151-192). McGraw-Hill.

Contrafatto, M. (2014). Stewardship Theory: Approaches and Perspectives. *Advances in Public Interest Accounting*, *17*, 177-196. https://doi.org/10.1108/S1041-706020140000017007

Crowhurst, I., & Kennedy-Macfoy, M. (2013). Troubling gatekeepers: methodological considerations for social research. In (Vol. 16, pp. 457-462): Taylor & Francis.

Crowther, K. G., Haimes, Y. Y., & Johnson, M. E. (2010). Principles for better information security through more accurate, transparent risk scoring. *Journal of Homeland Security and Emergency Management*, *7*(1).

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79-98.

Davis, J. H., Schoorman, F. D., & Donaldson, L. (1997). Toward a Stewardship Theory of Management. *The Academy of Management Review*, *22*(1), 20-47. https://doi.org/10.2307/259223

Deben, M. (2021). Volwassenheidsonderzoek informatiebeveiliging gemeente Overbetuwe.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*, *11*(2), 127-153. https://doi.org/https://doi.org/10.1046/j.1365-2575.2001.00099.x

Diéguez, M., Sepúlveda, S., & Cares, C. (2012). On optimizing the path to information security compliance. 2012 Eighth International Conference on the Quality of Information and Communications Technology,

Digitale Overheid. (2020). *Gemeentelijke dienstverlening Gemeentelijke dienstverlening aan ondernemers* Retrieved August 02 from https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/dienstverlening-aan-burgers-en-ondernemers/gemeentelijke-dienstverlening/

Doganata, Y. (2012). Detecting Compliance Failures in Un-managed Processes. In *Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions* (pp. 385-404). IGI Global. https://doi.org/10.4018/978-1-4666-0197-0.ch022

Etienne, J. (2010). Compliance Theories: A Literature Review. *Revue française de science politique*, *60*, 493-517. https://doi.org/10.3917/rfspe.602.0139

Field, A. (2013). *Discovering statistics using IBM SPSS statistics*. Sage.

Flamholtz, E. G., Das, T. K., & Tsui, A. S. (1985). Toward an integrative framework of organizational control. *Accounting, Organizations and Society*, *10*(1), 35-50. https://doi.org/https://doi.org/10.1016/0361-3682(85)90030-3

Foorthuis, R. (2020). Tactics for Internal Compliance: A Literature Review. arXiv:2008.03775. Retrieved August 01, 2020, from https://ui.adsabs.harvard.edu/abs/2020arXiv200803775F

Haeussinger, F., & Kranz, J. (2013). Understanding the antecedents of information security awareness - An empirical study. *19th Americas Conference on Information Systems, AMCIS 2013 - Hyperconnected World: Anything, Anywhere, Anytime*, *5*, 3762-3770.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2006). Multivariate data analysis (Vol. 6): Pearson Prentice Hall Upper Saddle River. In: NJ.

Hathaway, O. A. (2002). Do Human Rights Treaties Make a Difference? *The Yale Law Journal*, *111*(8), 1935-2042. https://doi.org/10.2307/797642

Hingh, A., & Lodder, A. R. (2017). Informatieveiligheid: de digitale veerkracht van Nederlandse overheden. *Bestuurskunde*, *1*, 27-34.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615-660.

IB&P. (2021). Rekenkameronderzoek informatiebeveiliging van gemeenten en verbonden partijen. https://www.rekenkamerwvolv.nl/wp-content/uploads/2021/02/2021-02-08-IBP-Rekenkameronderzoek-Informatiebeveiliging-WVOLV.pdf

Informatiebeveiligingsdienst. (2021). *Lessen uit de hack bij Hof van Twente*. https://vng.nl/sites/default/files/2021-03/20210315-lessen-hvt-tlp_wit-v1.0.pdf

ISO. (2017). *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements*. https://www.iso.org/standard/54534.html

Jardas Antonić, J., & Segota, A. (2012). Measuring the performance of local e-government in the Republic of Croatia using data envelopment analysis. *Problems and Perspectives in Management*, *10*, 35-44.

Johnston, J. S. (2002). A Game Theoretic Analysis of Alternative Institutions for Regulatory Cost-Benefit Analysis. *University of Pennsylvania Law Review*, *150*(5), 1343-1428. https://doi.org/10.2307/3312942

Killmeyer, J. (2006). *Information security architecture: an integrated approach to security in the organization*. Auerbach Publications.

Kirsch, L. J. (1996). The management of complex tasks in organizations: Controlling the systems development process. *Organization science*, *7*(1), 1-21.

Kluge, D., & Sambasivam, S. (2008). Formal information security standards in German medium enterprises. CONISAR: The Conference on Information Systems Applied Research,

Knapp, K., Marshall, T., Jr, R., & Ford, F. (2006). Information security: Management's effect on culture and policy. *Inf. Manag. Comput. Security*, *14*, 24-36. https://doi.org/10.1108/09685220610648355

Koops, C. E. (2014). *Contemplating compliance: European compliance mechanisms in international perspective*. Universiteit van Amsterdam.

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management*, *41*(5), 597-607.

Kuiper, M. E. H. (2022). *Regulation and compliance: Conflicts of interest, disclosure, and compliance culture*

Lavrakas, P. J. (2008). *Encyclopedia of survey research methods*. Sage publications.

Liang, H., Xue, Y., & Wu, L. (2013). Ensuring employees' IT compliance: carrot or stick? *Information Systems Research*, *24*(2), 279-294.

Lindgren, I., Madsen, C. Ø., Hofmann, S., & Melin, U. (2019). Close encounters of the digital kind: A research agenda for the digitalization of public services. *Government Information Quarterly*, *36*(3), 427-436.

https://doi.org/https://doi.org/10.1016/j.giq.2019.03.002
Ma, Q., Schmidt, M. B., & Pearson, J. M. (2009). An Integrated Framework for Information Security Management. *Review of Business*, *30*(1).
MacLean, T. L., & Behnam, M. (2010). The Dangers of Decoupling: The Relationship Between Compliance Programs, Legitimacy Perceptions, and Institutionalized Misconduct. *Academy of Management Journal*, *53*(6), 1499-1520. https://doi.org/10.5465/amj.2010.57319198
Meijer, A., & Bekkers, V. (2015). A metatheory of e-government: Creating some order in a fragmented research field. *Government Information Quarterly*, *32*. https://doi.org/10.1016/j.giq.2015.04.006
Merhi, M., & Ahluwalia, P. (2015). Top management can lower resistance toward information security compliance. *ICIS 2015 3*.
Mitchell, R. B. (1996). *Compliance Theory: An Overview* (Vol. 1). Routledge.
Nationaal Cybersecurity Centrum (NCSC). (2018). *Nationale Cybersecurity Agenda*. https://www.ncsc.nl/onderwerpen/nederlandse-cyber-security-agenda/documenten/publicaties/2019/mei/01/nederlandse-cybersecurity-agenda
Nederlandse Beroepsorganisatie voor Accountants (NBA). (2019). *Handreiking bij Volwassenheidsmodel Informatiebeveiliging*. https://www.nba.nl/globalassets/over-de-nba/ledengroepen/lio/lio-new/nba-lio-norea-handreiking-bij-volwassenheidsmodel-informatiebeveiliging-januari-2019.pdf
Ouchi, W. G. (1979). A conceptual framework for the design of organizational control mechanisms. *Management science*, *25*(9), 833-848.
Queirós, A., Faria, D., & Almeida, F. (2017). Strengths and limitations of qualitative and quantitative research methods. *European journal of education studies*.
Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. CRC Press.
Safa, N., Solms, R., & Furnell, S. (2016). Information security policy compliance model in organisations. *Computers & Security*, *56*, 70-82.
Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *Information Management Journal-Prairie Village-*, *39*(4), 60.
Schillemans, T. (2013). Moving beyond the clash of interests: On stewardship theory and the relationships between central government departments and public agencies. *Public management review*, *15*(4), 541-562.
Shiffman, C. (2010). Making Law Work: Environmental Compliance & Sustainable Development by Durwood Zaelke, Donald Kaniaru, and Eva Kružíková Cameron May Ltd., 2005. *Sustainable Development Law & Policy*, *6*(1), 21.
Silva, L., Hsu, C., Backhouse, J., & McDonnell, A. (2016). Resistance and power in a security certification scheme: The case of c:cure. *Decision Support Systems*, *92*, 68-78. https://doi.org/https://doi.org/10.1016/j.dss.2016.09.014
Sindhuja, P., & Kunnathur, A. (2015). Information security in supply chains: A management control perspective. *Information and Computer Security*, *23*, 476-496. https://doi.org/10.1108/ICS-07-2014-0050
Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31-41. https://doi.org/10.1108/09685220010371394
Straub, D. W. (1989). Validating instruments in MIS research. *MIS Q.*, *13*(2), 147–169. https://doi.org/10.2307/248922
ten Have, W. (2014). Systematisch en in samenhang werken aan compliance, cultuur en controls. *Privacy & Compliance Tijdschrift voor de Praktijk*(4), 4-11.
Thomas, R. M. (2003). *Blending qualitative and quantitative research methods in theses and dissertations*. Corwin Press.
Tyler, T. R., & Jackson, J. (2014). Popular legitimacy and the exercise of legal authority: Motivating compliance, cooperation, and engagement. *Psychology, public policy, and law*, *20*(1), 78.
Rustagi, S., King, W. R., & Kirsch, L. J. (2008). Predictors of Formal Control Usage in IT Outsourcing Partnerships. *Information Systems Research*, *19*(2), 126-143. https://doi.org/10.1287/isre.1080.0169
Vereniging Nederlandse Gemeenten (VNG). (2013). *Informatieveiligheid, randvoorwaarde voor de professionele gemeente*. https://vng.nl/files/vng/brieven/2013/attachments/20131031_resolutie-informatieveiligheid.pdf
Vereniging Nederlandse Gemeenten (VNG). (2022). *Aan de slag met de omnichannel aanpak*. https://vng.nl/nieuws/omnichannelstrategie-voor-naadloze-klantinteractie
Von Solms, B. (2001). Corporate governance and information security. *Computers & Security*, *20*(3), 215-218.
Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102.

Verbeek, M. (2017). Using linear regression to establish empirical relationships. *IZA World of Labor*. https://doi.org/10.15185/izawol.336

Weitzner, D. J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., & Sussman, G. J. (2008). Information accountability. *Communications of the ACM*, *51*(6), 82-87.

Wolman, A. (2015). Japan and international refugee protection norms: Explaining non-compliance. *Asian and Pacific Migration Journal*, *24*(4), 409-431. https://doi.org/10.1177/0117196815606852

Wright, B., & Schwager, P. H. (2008). Online survey research: can response factors be improved? *Journal of Internet Commerce*, *7*(2), 253-269.

Bijlage 1: Vragenlijst online survey

Construct	Definitie	Bron	Vragen
Compliance	De mate waarin een actor zich overeenkomstig gedraagt- en aantoonbaar handelt naar- vooraf gedefinieerde en tevens expliciete normen die aan hen zijn opgelegd.	Gebaseerd op Foorthuis (2012), Checkel (2001), Étienne (2010)	1. Mijn gemeente heeft zicht op de belangrijkste risico's op het gebied van informatiebeveiliging.
			2. Binnen mijn gemeente worden de belangrijkste risico's op het gebied van informatiebeveiliging beheerst.
			3. Mijn gemeente heeft de beheersmaatregelen uit de BIO aantoonbaar geïmplementeerd.
			4. Zowel op afdelings- als organisatieniveau wordt bewaakt dat men zich aan de vastgestelde processen op het gebied van informatiebeveiliging houdt.
Bestuurlijke toewijding	De beslissingen, investeringen en acties die door het bestuur worden ondernomen om een informatiebeveiligingsstrategie binnen een organisatie af te dwingen.	Gebaseerd op Boonstra (2013), Mehri & Ahluwalia (2015), Knapp et al. (2006)	1. De gemeentesecretaris draagt het belang van informatiebeveiliging zichtbaar uit.
			2. Bestuurders binnen mijn gemeente houden zich enkel actief met informatiebeveiliging indien er iets mis gaat.
			3. Er worden voldoende middelen beschikbaar gesteld om benodigde maatregelen op het gebied van informatiebeveiliging te implementeren.
			4. De portefeuillehouder ICT van mijn gemeente draagt het belang van informatiebeveiliging zichtbaar uit.
			5. Ik ervaar voldoende ondersteuning vanuit het bestuur van mijn gemeente bij

			het uitvoeren van mijn werkzaamheden.
Interne controle	De pogingen van een organisatie om de acties en het gedrag van anderen zo te beïnvloeden dat dit ertoe leidt dat beveiligingsdoelstellingen worden bereikt.	Gebaseerd op Ouchi (1979), Kirsch (1996), Boss et al. (2009)	1. De gemeenteraad neemt een actieve controlerende rol op zich ten aanzien van informatiebeveiliging binnen mijn gemeente
			2. Er wordt actief op toegezien dat organisationele doelstellingen op het gebied van informatiebeveiliging worden behaald
			3. Ik ervaar druk om jaarlijks verbetering te laten zien op het gebied van informatiebeveiliging
			4. De doelstellingen van mijn gemeente op het gebied van informatiebeveiliging zijn volledig gebaseerd op kwantitatieve cijfers (budget, productiviteit, aantallen, compliance)
			5. Binnen mijn gemeente heerst er een cultuur waarin fouten kunnen worden besproken en waar feedback kan worden gegeven
Organisationele awareness	Een staat waarin werknemers zich bewust zijn van- en idealiter gecommitteerd zijn aan- de opgestelde beveiligingsstrategie van een organisatie	Gebaseerd op Tschou et al. (2008), Wolf et al. (2011), D'Arcy (2009), Bulgurcu et al. (2011)	1. Alle werknemers binnen mijn gemeente zijn op de hoogte van het informatiebeveiligingsbeleid en aansluitende procedures
			2. Binnen mijn gemeente wordt er actief ingezet op awareness-campagnes (denk aan presentaties en voorlichtingen) om werknemers bewust te maken over het belang van informatiebeveiliging
			3. Informatiebeveiliging wordt binnen mijn gemeente ervaren als een collectieve opgave