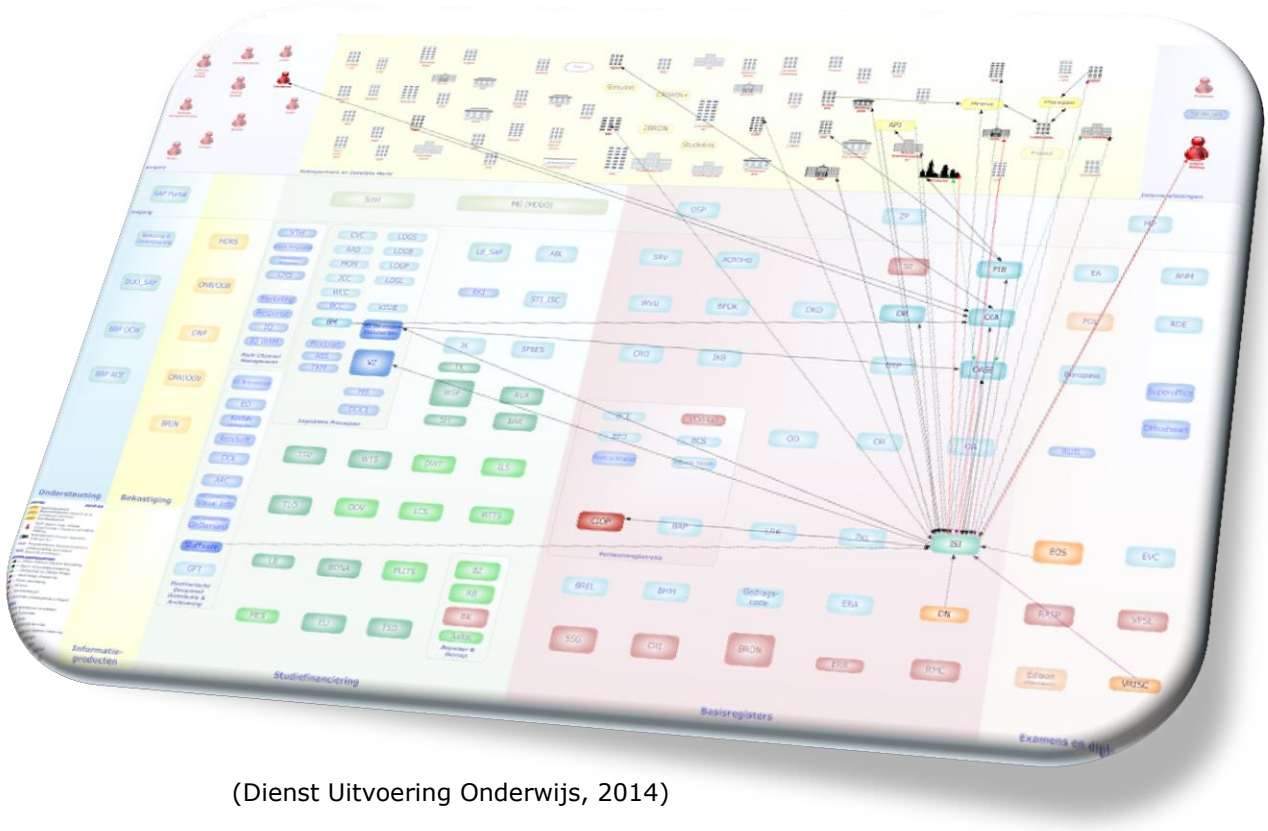
HEDENDAAGSE INFORMATIEBEVEILIGING;

Een analyse naar de *State of the Art* in informatiebeveiliging en de uiting daarvan bij de Dienst Uitvoering Onderwijs in de periode 2010-2015.



(Dienst Uitvoering Onderwijs, 2014)

Universiteit Leiden

Naam	D.H.C. Dijkstra
Studentennummer	S1191624
Opleiding	Msc. Crisis and Security Management
Plaats	Universiteit Leiden te Den Haag
Datum van inlevering	Augustus 2016
Eerste lezer	Dr. J. Matthys
Tweede lezer	Dr. R.S. Prins

"In some ways, security is the most potent and dangerous of all policy goals, because leaders can use it to trump all others" (Stone, 2012, p. 152).

Voorwoord

Het afronden van de masterscriptie betrof voor mij een onverwacht en lang proces. In dit proces heb ik niet stilgestaan; ik heb zo'n vier verschillende werkplekken gezien en ik heb nieuwe drijfveren leren kennen waar mijn passies liggen. Tijdens het afronden van deze masterscriptie, start voor mij een nieuwe uitdaging bij het Ministerie van Defensie waar ik als functioneel beheerder aan de slag ga. Hiermee sluit ik mijn werkperiode af bij BECIS BV. Waar ik als junior adviseur informatiemanagement meer kennis heb mogen maken met het vakgebied waar mijn passies liggen. Op het moment dat ik het onderwerp, van deze masterscriptie, koos was van deze twee functies geen sprake. Mijn keuze voor het onderwerp is onbewust een uiting van mijn destijdse interesse. Ik had nooit verwacht dat ik zoveel met het managen van informatie te maken zou gaan krijgen. Door mijn gevoel te volgen heb ik met veel plezier nieuwe deuren geopend. Ik verwonder mij over personen die onbewust onjuist met persoonsgegevens omgaan én over de omvang van maatregelen, die door organisaties worden ingezet, om de beveiliging van informatie te verbeteren. Ik vroeg mijzelf waar de keuzes voor die maatregelen op zijn gebaseerd. Dit soort verwonderingen maak ik nog dagelijks mee.

Eveneens is de fysieke (on)veiligheid aanwezig en zichtbaar in de hedendaagse samenleving; het kost moeite om deze onder controle te krijgen en houden. Onveiligheid van bijvoorbeeld (identiteits)diefstal van vertrouwelijke gegevens is vaak onzichtbaar; het gevolg is niet direct zichtbaar en meetbaar. Deze twee voorbeelden van onveiligheden zijn vandaag de dag steeds meer met elkaar verweven. Ik pleit voor meer onderzoek naar informatiebeveiliging én de implicaties die dit met zich meebrengen. Doordat het schrijven van mijn scriptie een, relatief, lang proces is geweest, heb ik mogen ervaren hoe de aandacht voor het onderwerp in de loop van de jaren steeds meer in de dagelijkse praktijk terugkomt. Ik hoop vooral dat als neveneffect kleinere organisaties met publieke diensten de beschreven factoren als een praktisch handvat zien om aan de slag te gaan met de verbetering van de organisatie van informatiebeveiliging.

Ondanks alle professionele overwegingen is het schrijven van de scriptie vooral een persoonlijke aangelegenheid. Ik ben aan de universiteit Leiden gaan studeren om als persoon verder te groeien en mijn intellect uit te dagen. Blijven leren en ontwikkelen is een belangrijke waarde voor mij. Tijdens het scriptieproces ben ik meerdere malen in twijfel gebracht over mij intellect. , Hier heb ik veel ondersteuning en vertrouwen gehad van mijn vrienden, oud-collega's en familie. Het is fijn om te kunnen beseffen dat ik zulke lieve mensen om me heen heb; dit is mij veel waard. Mede dankzij hen heb ik de handoek niet in de ring gegooid en heb ik vele avonden besteed in de universiteitsbibliotheek te Delft.

Ik kan lang niet iedereen bedanken in mijn voorwoord. Ik wil mijn vrienden, familie en voormalig collega's bedanken voor het vertrouwen dat zij in mij hebben. Bij dezen wil ik diegene die mij in de laatste fase erdoorheen hebben gesleept benoemen; Thanim van Dokkum, Bram Groeneveld en Koen Vermeulen. Tenslotte wil ik Joery Matthys bedanken voor zijn proffesionaliteit, flexibiliteit en moderne 'plaats- en tijd onafhankelijke' manier van begeleiden. Merci.

Desiree Helena Corina Dijkstra
Augustus, 2016

Inhoud

1.Inleiding

Over het jaar 2012 luidt de Algemene Rekenkamer de noodklok; van vijf ministeries en vijf baten-lastenagentschappen is de informatiebeveiliging als onvolkomen beschouwd. Voor twee ministeries en een baten-lastenagentschap is informatiebeveiliging als aandachtspunt aangemerkt. (Algemene Rekenkamer, 2012a). Twee jaar daarvoor, in 2010, werd de Nederlandse overheid geconfronteerd door de 'Diginotar-affaire'. Diginotar verleende PKIoverheidcertificaten voor onder andere het gebruik van DigiD en voor de RDW. Echter, de beveiliging hiervan was niet goed op orde, waardoor het mogelijk werd om valse SSL-certificaten te genereren. Als gevolg hiervan konden hackers willekeurige certificaten genereren, terwijl het in de webbrowser leek of de pagina te vertrouwen was. Tegelijkertijd konden er persoonsgegevens gestolen worden. Vervolgens werd er in 2011 tijdens 'Lektober' opgeroepen om datalekken te melden bij de website www.Webwereld.nl. In oktober 2011 werd er elke werkdag van de week een privacylek gepubliceerd, het leek in die maand een wassen neus om informatie en persoonsgegevens van de overheid los te peuteren.

(Door)ontwikkelingen binnen de informatie- en communicatietechnologie (ICT) zijn aan de orde van de dag. De komst van ICT heeft eveneens gezorgd voor de komst van opzettelijk misbruik van ICT. Daarnaast is de samenleving steeds meer afhankelijk van ICT. E-dienstverlening binnen de publieke sector is hiervan een voorbeeld. Daarbij zijn vitale infrastructuren en banken afhankelijk van de technologie. Een voorbeeld van misbruik van ICT is de digitale inbraak waar (persoons)gegevens worden gestolen. Gevolgen van dit misbruik voor de desbetreffende organisatie kan leiden tot financiële schade en imagoschade; het vertrouwen in de organisatie wordt geschaad. Het aantal daadwerkelijke inbreuken op computersystemen, bedrijfsgegevens en persoonsgegevens is onbekend. Over het jaar 2013 zijn er 431 gevallen bekend waar fraude is gepleegd met Nederlandse identiteitsdocumenten (Panteia, 2014, p. chap 4.3). Daarnaast zijn er in 2013 617 meldingen gedaan bij het Centraal Meld- en Informatiepunt Identiteitsfraude en -fouten (CMI). In 2012 betroffen dit 291 meldingen bij het CMI. Deze cijfers zeggen onvoldoende over de daadwerkelijke omvang van identiteitsfraude. Eveneens dient vermeld te worden dat het CMI in 2012 is opgestart, waar onder andere uit blijkt dat het meten van deze gegevens nog in ontwikkeling is. De omvang van het misbruik van vertrouwelijke gegevens is onbekend.

Over het jaar 2015 stelt de Algemene Rekenkamer dat veel van de onvolkomenheden in informatiebeveiliging, zoals gesteld in 2012, als opgelost zijn beschouwd.

> "In 2014 waren er rijksbreed 13 onvolkomenheden op het gebied van informatiebeveiliging, wat er 7 meer waren dan in 2013. In 2015 zijn wij van oordeel dat er nog maar 1 onvolkomenheid over is. …Op basis van de ICV's hebben wij in 2015 nog wel 11 aandachtspunten bij diverse departementen."(Algemene Rekenkamer, 2015, pp. 32-33)

Uit de conclusie van de Algemene Rekenkamer is te herleiden dat de Rijksoverheid aan de slag is gegaan met het verbeteren van de informatiebeveiliging. De vraag of de maatregelen ervoor zorgen dat informatie veiliger is, is niet beantwoord.

Door de snelheid van de ontwikkeling van ICT en de positie van ICT in de Nederlandse samenleving is er behoefte aan standaarden en richtlijnen. Deze standaarden en richtlijnen dienen flexibel aanpasbaar te zijn op vernieuwingen binnen de ICT. In het publieke domein zijn, vanwege het belang van een transparante en open overheid, de terugvindbaarheid en reproduceerbaarheid van overheidsinformatie belangrijke pijlers. Binnen de wetenschap is summier onderzoek verricht op het gebied van informatiebeveiliging binnen de ICT, specifiek binnen het publieke domein. Tevens is er nog weinig wetenschappelijk verklaard op het gebied van de veiligheid van diezelfde IT. Recentelijke academische literatuur is voornamelijk gericht op effectieve inrichting van informatiebeveiliging middels de analyse van theorieën en overheidsrichtlijnen. Er is geen wetenschappelijk onderzoek verricht op het verklaren van de effectiviteit van beveiligingsmaatregelen en of deze maatregelen tot veiligere informatie leiden (Flores, Sommestad, Holm, & Ekstedt, 2011; Salini & Kanmani, 2015; Veiga & Eloff, 2007). In de academische literatuur wordt er aandacht besteed aan een conventionele scheiding tussen een organisatorische en een technische benadering van informatiebeveiliging. Er is onderscheid gemaakt tussen de fysieke, sociale en systeemtechnische aspecten van de informatiebeveiliging. Academici en professionals richten zich op modellen die deze scheiding overbruggen (Houngbo & Hounsou, 2015; Mishra & Powel, 2011; Veiga & Eloff, 2007). Het integraal aanpakken van informatiebeveiliging en de informatiebeveiligingscultuur zijn onderwerpen die minimaal de laatste tien jaar steeds meer aandacht krijgen (Dhillon, 2007; Spruit, 2010). In de literatuur is geen set van aspecten, ofwel factoren, ofwel variabelen, beschikbaar die bruikbaar zijn voor wetenschappelijk onderzoek naar een integrale aanpak voor informatiebeveiliging. Hiertoe ontbreekt het aan handvatten voor de wetenschappelijke discipline om meer inzicht, begrip en kennis aangaande informatiebeveiliging te vergaren. Daarnaast is het nog de vraag of informatiebeveiliging in de praktijk al dan niet integraal wordt benaderd.

Voor een aantal departementen binnen de Rijksoverheid blijft informatiebeveiliging een aandachtspunt voor de Algemene Rekenkamer. Eén daarvan is de Dienst Uitvoering Onderwijs (DUO). De DUO heeft een van de grootste aantallen van persoonsgegevens in beheer binnen de Rijksoverheid, doordat zij onder andere belast is met de registratie en verwerking van gegevens van studenten, kinderen die kinderopvang behoeven en de ouders hiervan. Als baten-lastenagentschap is de DUO gemoeid met het beheer van de gegevens van studenten, het uitbetalen van de studiefinanciering en de bekostiging van de desbetreffende onderwijsinstellingen. Bij de DUO liggen de risico's voornamelijk in het gebruik van de websites. Via de websites kunnen studenten en instellingen hun gegevens inzien en wijzigen. Hierdoor is de DUO een interessante organisatie voor hackers; het gaat om een grote hoeveelheid persoonsgegevens die van grotere waarde is voor de desbetreffende doelgroep. In 2010 kwam de DUO in het nieuws met het bericht dat studenten in hun eigen omgeving gegevens konden zien van andere studenten (Schellevis, 2010). DUO is een van de grootgebruikers van DigiD, waartoe ook de Diginotar-affaire de DUO heeft geraakt. Vanuit die invalshoek is de DUO een interessante organisatie om te bestuderen; in hoeverre heeft de DUO informatiebeveiliging integraal aangepakt en hoe beoogt de DUO vertrouwelijke informatie veilig te stellen?

1.1 Centrale onderzoeksvraag

Het doel van dit onderzoek is het aanvullen van de academische literatuur over overheidsborging van digitaal opgeslagen vertrouwelijke informatie. Dit is beoogd door de ontwikkeling van zeven factoren die zijn gebaseerd op kritische aspecten conform *State of the Art* op het gebied van informatiebeveiliging. Vervolgens zijn deze factoren gebruikt om te onderzoeken in hoeverre de DUO, na een informatiebeveiligingsincident in 2010, deze factoren tot uiting brengt. Om dit doel te bereiken, is de volgende onderzoeksvraag geformuleerd:

'Welke factoren zijn conform State of the Art van belang voor het organiseren van informatiebeveiliging in de publieke sector en in hoeverre komt dit tot uiting bij de Dienst Uitvoering Onderwijs (DUO) in de periode van 2010-2015?'

1.2 Beveiliging van vertrouwelijke informatie

In deze masterscriptie betreft het digitaal opslaan van vertrouwelijke informatie, informatie die bij wet niet openbaar gesteld mag worden[1]. Voorbeelden hiervan zijn persoonsgegevens en informatie waarbij sprake is van geheimhoudingsplicht. Informatiebeveiliging is onderdeel van het gehele pakket aan ontwikkeling, inrichting, beheer en *governance* aangaande informatievoorzieningen. Het gaat hier niet alleen om de technische en de databeveiliging, maar ook om de beveiliging van procedures en personeel (Salini & Kanmani, 2015). Zoals eerder gesteld is ICT onderhevig aan vernieuwing en is daarmee vluchtig beleid. In de praktijk blijft de wet- en regelgeving achter op de snelle ontwikkeling van ICT (zoals de Archiefwet uit 1994). Dit brengt uitdagingen met zich mee voor de borging van vertrouwelijke informatie binnen het publieke domein. In dit onderzoek is uitgegaan van *State of the Art* op het gebied van informatiebeveiliging binnen het domein van de ICT.

1.3 Leeswijzer

De masterscriptie is opgebouwd uit vijf hoofdstukken: hoofdstuk 1 inleiding, hoofdstuk 2 theoretisch kader, hoofdstuk 3 methodologie, hoofdstuk 4 resultaten en hoofdstuk 5 conclusie. In het theoretisch kader zijn de academische literatuur en de richtlijnen met betrekking tot informatiebeveiliging van de laatste vijftien jaar beschreven. Dit heeft als doel om een antwoord te kunnen geven wat de *State of the Art*-literatuur is. Hoofdstuk 3 bevat een beschrijving van welke onderzoeksmethode is gehanteerd om te komen tot de beantwoording van de centrale onderzoeksvraag. Het vierde hoofdstuk bevat een korte beschrijving van de casus en de resultaten van de analyse van in hoeverre de factoren, die conform de *State of the Art* van belang zijn voor de organisatie van informatiebeveiliging, tot uiting komen bij de DUO in de periode 2010-2015. Ten slotte wordt in hoofdstuk 5 de centrale vraagstelling van dit onderzoek beantwoord. Verder zijn er bijlagen aan dit onderzoek toegevoegd, waarin het onderzoeksmateriaal dat uit de analyse is voortgekomen is opgenomen.

1 Betreft Wet bescherming persoongegevens, Archiefwet 1994 en Algemene Verordening Gegevensbescherming

2. Theoretisch kader

In het theoretisch kader van deze masterscriptoe zijn literatuur en richtlijnen met betrekking tot informatiebeveiliging van de laatste 15 jaar bestudeert om te komen tot de '*State of the Art'* op het gebied van informatiebeveiliging. Er is gekozen voor de laatste 15 jaar omdat de ontwikkelingen in de ICT elkaar snel opvolgen. Eveneens is er wetenschappelijk weinig verklaard op het gebied van informatiebeveiliging. Het theoretisch kader vormt de basis voor het bepalen van de factoren welke, conform '*State of the Art',* van belang zijn voor het organiseren van informatiebeveiliging in de publieke sector. Dit hoofdstuk start (paragraaf 2.1) met het definiëren van het begrip informatiebeveiliging alsmede de afbakening van het onderwerp. Vervolgens zijn de verschillende benaderingen voor het organiseren van informatiebeveiliging vanuit de literatuur beschreven (paragraaf 2.2). In paragraaf 2.3 is een selectie aan richtlijnen voor informatiebeveiliging beschreven. In zowel de academische literatuur als de richtlijnen ligt de nadruk op een informatiebeveiligingssysteem. Om die reden is in paragraaf 2.4 een beschrijving opgenomen van informatiebeveiligingssystemen en de voor- en nadelen hiervan. De uitkomst van dit hoofdstuk resulteert in zeven factoren die conform *'State of the Art'* van belang zijn voor het organiseren van informatiebeveiliging in de publieke sector (paragraaf 2.5). Deze zeven factoren zijn uiteengezet in paragraaf 2.6. In hoofdstuk 4 (resultaten) is beschreven in hoeverre deze factoren tot uiting komen bij de DUO.

2.1 Definiëring informatiebeveiliging

Nog geen 10 jaar geleden werd in de academische literatuur onder andere het beeld geschetst dat vooral gericht werd op de technische aspecten in de organisatie van informatiebeveiliging en dat de socio-organisatorische aspecten niet voldoende zijn opgenomen in deze sturing (Dhillon, 2007). Conventioneel gezien is informatiebeveiliging opgedeeld in socio-organisatorisch, fysieke en technische beveiliging van informatie (van Lieshout et al., 2012). Bij socio-organisatorische aspecten gaat het om factoren op het gebied van organisatiemanagement en informatiebeveiligingscultuur. Vanaf 2001 is in de academische literatuur zichtbaar meer aandacht voor sociale aspecten, zoals het handelen door gebruikers van informatievoorzieningen (Dhillon & Backhouse, 2001). Een van de risico's voor beveiliging van informatie is het menselijk falen (Spruit 2010). Wanneer alle technische aspecten op orde zijn, kunnen alsnog menselijke handelingen lekken van data al dan niet opzettelijk veroorzaken. Oorspronkelijk probeerden organisaties dit op te vangen door checklists, handleidingen en logische beveiligingsmaatregelen (Dhillon & Backhouse, 2001). Enkel het voldoen aan de beveiligingschecklist sluiten menselijke fouten niet uit. Menselijke fouten treden vooral op door onbewust gedrag of doordat handelingen op de automatische piloot worden uitgevoerd (Spruit 2010). D'Arcy en Hovav (2008) stellen dat het begrijpen van de factoren die invloed hebben op de effectiviteit van beveiligingsmaatregelen een consistent thema is in de literatuur over informatiebeveiliging. Daarbij kaarten Dhillon en Backhouse (2001) de noodzaak aan voor meer empirisch onderzoek op dit gebied; met als doel het ontwikkelen van effectieve principes rondom informatiebeveiliging. De effectiviteit van de informatiebeveiliging wordt door Staub (1990, p. 4) gedefinieerd als; "het vermogen om

bescherming te bieden tegen ongeautoriseerd en opzettelijk misbruik van middelen van de lokale informatiesystemen door individuen, inclusief de overtredingen met betrekking tot hardware, programma's, data en computerdiensten" (Idem).

Kortweg wordt informatiebeveiliging conventioneel beschreven als het beschermen van informatievoorzieningen tegen kwaadwillige gebruikers (Pieters, 2011, p. 326). In 2003 heeft het National Institute of Standards and Technology (US NIST), het meetinstrument *'security metrics'* waarmee beleid op informatieveiligheid kan worden getoetst in gebruik genomen (Wulp, 2004, p. 15).

> "Het primaire doel van Security Metrics is het kwantificeren van de mate van effectiviteit van security-maatregelen en -procedures. Afhankelijk van de volledigheid en de kwaliteit van het beveiligingsbeleid levert een goed Security Metrics-systeem in tweede instantie informatie op over de kwaliteit van de geïmplementeerde beveiliging". (Wulp, 2004, p. 16)

Security Metrics richt zich op de kwaliteit van de beveiligingsmaatregel op zichzelf en daarmee niet op de effectiviteit van de maatregel. Dhillon en Torkzedeh (2006) stellen dat beveiligingsbeleid fundamenteel is voor het verbeteren van informatiebeveiliging en dat afschrikking een fundamenteel middel is om de effectiviteit van beveiligingsmanagement te verbeteren. Hiertoe zijn de talloze standaarden, en handvatten gecreëerd om organisaties hierin te ondersteunen. Het aannemen van standaarden voor informatiebeveiliging biedt, volgens Janczewski (1999) , handvaten om tot snellere beleidsontwikkeling aangaande informatiebeveiliging te komen. Dit onderkennen Baskerville en Siponen (2002) eveneens. Zij hebben echter hun kanttekeningen op het gebruik van standaarden. Deze kanttekeningen hebben zij samengevat in de volgende vier punten:

1. *Algemene informativebeveiligingmanagement standaarden en handleidingen bieden te weinig handvaten om, om te gaan met de verscheidenheid van organisaties en dat deze om die reden anderemaatregelen behoeven dan welke zijn opegenomen in de standaarden (Baskerville, 1993);*
2. *Standaarden zijn niet gericht op de sociale aspecten van de problematiek (Baskerville & Siponen, 2002);*
3. *Generieke standaarden houden geen rekening met de geldende algemene vereisten voor de organisatie. Hierdoor kan er een mogelijk conflict optreden tussen normale organisatie vereisten en de gestandaardiseerde informatibeveiligingsvereisten (Baskerville & Siponen, 2002);*
4. *Generieke standaarden zijn grotendeels uitgeschreven. Informatibeveiliging bevat tevens noodzakelijke, ad hoc besluitvorming en/of oordelen (Ferris, 1994). Echter, de standaarden bieden geen ondersteuning bij problemen die optreden om tot besluitvorming te komen (Baskerville & Siponen, 2002).*

Verder wordt gesteld dat een informatiebeveiligingscultuur noodzakelijk is en dat de beveiligingsmaatregelen procesmatig opgepakt dienen te worden (informatiebeveiligingssysteem) (Beynon-Davies, 2002; Dhillon, 2007; Dhillon & Torkzadeh, 2006; Jensen & van der Aalst, 2009; Mishra & Powel, 2011; Veiga & Eloff, 2007). Op basis van de verschillende geanalyseerde definities voor dit onderzoek de volgende definitie van informatiebeveiliging gehanteerd:

Informatiebeveiliging betreft het totaalpakket aan preventieve maatregelen welke eraan bijdragen dat vertrouwelijke informatie niet openbaar beschikbaar is door bescherming te bieden tegen ongeautoriseerd- en opzettelijk misbruik van informatiesystemen.

2.2 Academische invalshoeken op het gebied van informatiebeveiliging

Op het gebied van informatiebeveiliging zijn binnen de sociale- en (computer-)technische wetenschappen een aantal kenmerken en lacunes benoemd ter verbetering van de organisatie van informatiebeveiliging. In de literatuur wordt vooral over het inrichten van een informatiebeveiligingssysteem geschreven, waarbij het uitgangspunt een integrale aanpak bevat (Houngbo & Hounsou, 2015; Mishra & Powel, 2011; Veiga & Eloff, 2007). Vanuit de academische literatuur zijn de volgende benaderingen en aspecten te onderkennen;

- Organisatorisch;
    - Strategie;
    - Management;
    - Operatie.
- Technisch;
- Informatiebeveiligingssysteem.

Het organisatorische aspect van informatiebeveiliging betreft in dit kader de strategische-, management- en operationele aspecten van informatiebeveiliging. De keuze voor de noemer organisatorisch is ontstaan door het, ten opzichte van technisch, veel voorkomend gebruik van de term *'Socio-Organizational'* (Dhillon & Backhouse, 2001; Houngbo & Hounsou, 2015; Mishra & Powel, 2011; Pieters, 2011; Veiga & Eloff, 2007). *'Socio-Organizational'* duidt op; organisatie voor en door menselijk handelen. Dit betreft de richting, inrichting en verrichting binnen de organisatie. Onder de 'technisch' vallen systeemtechnische beveiligingseisen waar vertrouwelijkheid, integriteit en beschikbaarheid van informatie ofwel data een rol spelen. Beide noemers zijn geenszins absoluut en hebben overlappen elkaar. De scheiding van definities geven een scheiding tussen de sociale- en de (computer)technische wetenschappen weer. Tenslotte is er sprake van informatiebeveiligingssystemen, die alle (bekende) deelaspecten van zowel organisatorische- als technische aspecten integreren (Houngbo & Hounsou, 2015; Mishra & Powel, 2011; Veiga & Eloff, 2007).

In de literatuur is er overeenstemming dat informatiebeveiligingsbeleid de basis is voor goede informatiebeveiliging binnen een organisatorische context (Baskerville & Siponen, 2002; David, 2002; Doherty & Fulford, 2006; Lindup, 1995). Higgings (1999) stelt dat de belangrijkste reden hiervoor is dat, bij het ontbreken van beleid, beveiligingsmaatregelen ontwikkelt worden zonder een duidelijke afbakening van doelen en verantwoordelijkheden. De hoeveelheid mogelijkheden en onvoorziene consequenties zorgen ervoor dat afbakening en kaders nodig zijn om wildgroei te voorkomen alsmede toegevoegde waarde voor de organisatie te creëren. Doherty & Fulford (2006) stellen dat er te weinig overeenstemming is tussen een informatiebeveiligingsstrategie en –beleid én dat er meer aandacht dient te komen voor het strategische aspect. Vanuit het technische

perspectief bestaat informatieveiligheid conventioneel gezien uit: (1) checklists met eisen waar het systeem aan moet voldoen, (2) een probabilistische risicoanalyse en (3) evaluaties waarbij bijvoorbeeld wordt geteld hoevaak bepaalde aanvallen voorkomen (Dhillon & Backhouse, 2001). Kritiek op deze vorm richt zich met name op de onderliggende vraag; wat is mogelijk?. De hoeveelheid aan mogelijkheden kunnen hierdoor leiden tot een uitdijing en verhoogde complexiteit van checklists. Daarbij richt het zich met name op de middelen ten opzichte van doelen. In plaats van de vraag 'wat is allemaal mogelijk?' beschrijven critici dat de vraag 'wat is er nodig?' belangrijker is (Baskerville, 1993; Beck, 1992; Hirschheim & Klein, 1989). Pieters (2011) beschrijft dit contrast als volgt:

> *"For the computer scientist it does not matter what kind of information needs to be . However, for the policymaker, it does. Therefore, the technical solutions never speak of privacy as it is used at policy level, and policymakers never speak of information security as it is used in the technical domain".* (Pieters, 2011, p. 2)

In deze paragraaf is een set factoren gedestilleerd vanuit de analyses en beschrijvingen van de in deze masterscriptie bestudeerde literatuur. Deze factoren zijn weergegeven in
Tabel **1**. De selectie van de literatuur is voornamelijk gericht op *governance* en informatiebeveiliging alsmede een integrale benadering van informatiebeveiliging. Deze invalshoeken zijn geformuleerd door academici die pleiten voor een benadering waarbij diverse invalshoeken samen worden genomen om tot een integrale benadering te komen. Vanwege het gebrek aan wetenschappelijke aandacht is het lastig om verschillende stromingen te identificeren.

Tabel 1 Factoren erkend door academici op het gebied van informatieveiligheid

Factoren	Beschrijving
Strategie	De factor strategie bestaat uit de missie, visie en bestuurlijke doelstellingen van de organisatie. Het verschil tussen strategie en management betreft dat strategie zich richt op wat nodig is en management gericht is op hoe dit te doen.
Management	Het aspect management richt zich op hoe informatiebeveiliging uit te voeren. Onder dit aspect vallen informatiebeveiligingsbeleid en informatiebeveiligingsrichtlijnen. In de literatuur is er overeenstemming dat informatiebeveiligingsbeleid de basis is voor goede informatiebeveiliging binnen een organisatorische context. (Baskerville & Siponen, 2002; David, 2002; Doherty & Fulford, 2006; Lindup, 1995)
Operationeel	Beveiligingsmaatregelen op het operationele aspect zijn voornamelijk gericht op het begrijpen en verbeteren van activiteiten binnen de bedrijfsvoering. Deze gaan onder andere over procesoptimalisatie en activiteitenoptimalisatie zoals training geven aan gebruikers over systemen en het verbeteren van de kwaliteit van de gegevens die de basis vormen voor informatie.
Technisch	Het technische aspect bevat de systeemtechnische beveiligingseisen, richtlijnen en handelingen die nodig zijn voor informatieveiligheid. Mishra & Powel (2011) onderscheiden hierin vertrouwelijkheid, integriteit en de beschikbaarheid van data. Het is van belang welke personen, welk niveau van data kunnen zien/gebruik maken. Daarbij wordt onderscheid gemaakt tussen een persoon die alles ziet/gebruikt en een persoon die slechts een noodzakelijk deel ziet/gebruikt (autorisaties).
Informatiebeveiligings systeem	In de literatuur wordt voornamelijk aandacht besteed aan de noodzaak om de scheiding tussen organisatorisch en technisch te overbruggen (Houngbo & Hounsou, 2015; Mishra & Powel, 2011; Veiga & Eloff, 2007). Er is een opkomst van informatiebeveiligingssystemen en het herkennen van gebruikerbewustwordingskaders.. Hier wordt de factor cultuur en bewustwording specifiek benadrukt, met als voorbeeld de stelling dat onveiligheid ontstaat door menselijk falen (Spruit, 2010).

2.3 Richtlijnen voor informatiebeveiliging in de publieke sector

Ter bevordering van de beveiliging van informatie zijn er voor zowel de publieke als private sector een groot aantal richtlijnen ontwikkeld. De volgende richtlijnen zijn benoemd in de geraadpleegde artikelen van academici; *'Control Objectives for Information Technology'* (COBIT), *'ISO 27000 series of standards, specifically designed for information security matters'* en de *'Information Technology Infrastructure Library'* (ITIL) (Dhillon & Backhouse, 2001; Houngbo & Hounsou, 2015; Mataracioglu & Ozkan, 2011; Mishra & Powel, 2011; Veiga & Eloff, 2007). In deze paragraaf zijn de meest bekende richtlijnen die van invloed zijn op de publieke sector geanalyseerd. De selectie richtlijnen is gebaseerd op de genoemde modellen in de gebruikte literatuur en de door de Nederlandse overheid gestelde verplichte standaarden als onderdeel van de 'pas toe of leg uit' lijst (College en Forum Standaardisatie, 2016). Deze verplichte standaarden zijn allen gebaseerd op de NEN-ISO/IEC 27001 en 27002. De ITIL en de COBIT zijn buiten beschouwing gelaten. ITIL is specifiek opgenomen in de Baseline Informatiebeveiliging Gemeenten. Daarnaast zijn zowel ITIL als COBIT in meerdere mate managementmodellen rondom informatietechnologie in het algemeen dan dat deze gericht zijn op informatiebeveiliging specifiek. Hierdoor zijn ITIL en COBIT minder geschikt voor dit onderzoek.

Tabel 2 'State of the Art' Richtlijnen voor informatiebeveiliging

Jaar	Model	Refereert naar
2014	NIST Special Publication 800-27 Rev A Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	▪ SP 800-14 (1996) ▪ The Common Criteria (ISO/IEC 15408) (2009) ▪ Defense-in-Depth (onbekend)
2010	SURF Startkit informatiebeveiliging voor het hoger onderwijs en wetenschappelijk onderzoek	▪ *'De Code voor Informatiebeveiliging'(NEN-ISO/IEC 27002) (2007)* ▪ *het IABB-procesmodel voor een gestructureerde aanpak' (van Stichting SURF)(1998)*
2015	SA-MBO ICT programma Informatiebeveiliging en Privacy,Normenkader en toetsingskader informatiebeveiliging mbo	▪ *ISO 27002:2013;* ▪ *Richtsnoer Beveiliging Persoonsgegevens van het College Bescherming Persoonsgegevens (CBP);* ▪ *ISO 27018;* ▪ *Capability Maturity Model.*
2012	Baseline Informatiebeveiliging Rijksdienst	▪ Wet Bescherming Persoonsgegevens (WBP); ▪ Wet Particuliere Beveiligingsorganisaties en Recherchebureaus (WBPR); ▪ Wet Veiligheidsonderzoeken (WVO); ▪ Wet Politiegegevens (WPG); ▪ Ambtenarenwet; ▪ Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007); ▪ Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie (VIRBI2012) ▪ Beveiligingsvoorschrift 2005 (BVR); ▪ Algemeen Rijksambtenarenreglement (ARAR); ▪ Ambtseed/belofte; ▪ Algemene Rijksvoorwaarden bij IT-overeenkomsten (ARBIT2010); ▪ Kader Rijkstoegangsbeleid; ▪ Uitgangspunten online communicatie rijksambtenaren. ▪ Programma van Eisen PKI Overheid; ▪ Code voor Informatiebeveiliging (ISO 27001:2005 en ISO 27002:2007); ▪ Telecommunication Infrastructure Standard for Data Centers (TIA-942).
2012	Baseline Informatiebeveiliging Gemeenten	▪ *NEN-ISO/IEC-27001/27002 (2005/2007)* ▪ *Wet Bescherming Persoonsgegevens (WBP)* ▪ *SUWI-wet en aansluitvoorwaarden* ▪ *BIR*

		▪ *Gemeentelijke Basis Administratie (GBA)* ▪ *Bussiness Impact Analyse (BIA) (2007)* ▪ *Gemeentelijke Model Architectuur (GEMMA)* ▪ *De Nederlandse Overheid Referentie Architectuur (NORA) (2007)* ▪ *ITIL security management (2003) www.marcelspruit.nl/papers/itilsecman.pdf* ▪ *RASCI, www.kwaliteitshandvesten.nl* ▪ *Best Practice Normen Informatiebeveiliging ICT-Voorzieningen, Jaap van der Veen (2009)* ▪ *Diverse documenten Govcert, www.govcert.nl* ▪ *Basiskennis informatiebeveiliging volgens NEN-ISO 2700x J. Hintzbergen en anderen (2011)* ▪ *Provinciale Baseline Informatiebeveiliging (2010)* ▪ *Diverse informatiebeveiligingsplannen gemeenten* ▪ *White paper Raamwek beveiliging webapplicaties, Govcert (2010)* ▪ *Het inrichten van een beveiligingsorganisatie. Welke factoren zijn van invloed, PvIB (2006) http://www.pvib.nl/download/?id=6259853*
2013	Baseline Informatiebeveiliging Waterschappen	▪ *BIG;* ▪ *BIR;* ▪ NEN-ISO/IEC 27001 en 27002 (2007)

2.3.1. Voorgangers van de huidige, binnen de overheid gehanteerde, richtlijnen

De richtlijnen die in dit hoofdstuk zijn toegelicht zijn ontstaan vanuit verschillende voorgaande '*best practices*,' voorgaande richtlijnen en samenvoegingen van een aantal losstaande richtlijnen. Dit is terug te zien in

Tabel 2. De BIR is bijvoorbeeld een vervanging van vijf voormalige richtlijnen (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2012). In de academische literatuur wordt veelal benoemt dat er een conventionele scheiding tussen sociale en technische wetenschappen aanwezig is. Opvallend isdat de achtergrond van de op dit moment meest gebruikte modellen, zoals het US-NIST sp800-14 model, uit 1996, een integrale benadering betreft. Dit was destijds niet de enige richtlijn die deze insteek had, zo wordt er in het document verwezen naar de Organization for Economic Co-operation and Development's (OECD) Guidelines for the Security of Information Systems te 1992 en de Britse standard (BSI) 7799 'A Code of Practice for Information Security Management' als basis. BSI is later overgegaan in de ISO/IEC.

2.3.2 US NIST

Het *'National Institute of Standards and Technology'* (US NIST) is opgericht in 1901 als een *'non-regulatory federal agency'* binnen het *'U.S. Department of Commerce'*. De missie van deze overheidsorganisatie is de promotie van innovatie en het industriële concurrentievermogen van de Verenigde Staten, door het bevorderen van wetenschappelijke metrieken, standaarden en technologie op manieren die economische veiligheid en de welvaart verbeterd. Het instituut heeft een organisatieonderdeel dat zich specifiek richt op *'Computer Security'* (US NIST, 2015). Yang, Ku, & Liu (2016), Wulp (2004) en Houngbo & Hounsou (2015) halen het model van de US NIST SP800-26 aan als set integrale standaarden. Dit specifieke model is niet meer beschikbaar. Hiervoor zijn nieuwere versies in de plaats gekomen. Een groot deel van de documenten die door dit departement zijn gepubliceerd betreft richtlijnen die per specifiek onderdeel zijn uitgewerkt voor de publieke sector. De betreffende richtlijn is een integrale uitwerking van al dat wat nodig is voor

een goede organisatie van informatiebeveiliging. In 2014 is de 'NIST Special Publication 800-27 Rev A Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A' gepubliceerd. Deze bevat een set van 16 principes, en lijkt een vervanging voor de 800-26 te zijn. In Tabel 3 is beschreven welke categorieën US NIST adresseert in haar integrale modellen.

Tabel 3 NIST Special Publication 800-27 Rev A Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A 2014

NIST Special Publication 800-27 Rev A Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A 2014	
Categorieën	**Beschrijving**
Security Foundation	Voorbereiding waarbij de basis op orde moet zijn voor de start van de ontwerpfase.
Risk based	Risico management van zowel het interne system als externe systemen en -invloeden. Waarbij tevens rekening met kosten en baten wordt gehouden.
Ease of Use	Inrichting welke rekening houd met (eind)gebruikersgemak, overdraagbaarheid en aanpassingsvermogen.
Increase Resilience	Vergroten van de weerbaarheid met betrekking tot gelaagde beveiliging, schadebeperking en borgen van continuïteit.
Reduce Vulnerabilities	Verminderen van kwetsbaarheden door het verlagen van de complexiteit en een gecontroleerde toegang.
Design with Network in Mind	Ontwerp met in acht name van het netwerk, dit betreft zowel andere beleidsstukken, systemen en identificatie van unieke gebruikers.

2.3.3 NEN-ISO/IEC 27001 en 27002

NEN-ISO/IEC staat voor het beheer van- en voor de Nederlandse normalisatie van de standaarden van de International Standards Organization (ISO). Deze is samengevoegd met de International Electrotechnical Commission (IEC). Vanwege de plaatsing op de 'pas toe of leg uit lijst' zijn in Nederland de NEN-ISO/IEC 27001:2013 en 27002:2013 modellen aangeduid als verplicht voor (semi-)overheidsorganisaties. Deze 'pas toe of leg uit lijst' is een lijst van standaarden die toegepast moeten worden bij de aanschaf van nieuwe IT-middelen, indien dit niet toegepast wordt dient dit uitgelegd te worden (College en Forum Standaardisatie, 2016). Op de 'pas toe of leg uit lijst' zijn de modellen als volgt gedefinieerd:

NEN-ISO/IEC 27001:2013

Specificeren van eisen voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System (ISMS) in het kader van de algemene bedrijfsrisico's voor de organisatie.

NEN-ISO/IEC 27002:2013

De standaard omvat "best practices" op het gebied van het organiseren van informatiebeveiliging voor een organisatie, bestaande uit het beheer van bedrijfsmiddelen, veilig personeel, toegangsbeveiliging, cryptografie, fysieke beveiliging en beveiliging van de omgeving, beveiliging in de bedrijfsvoering, communicatiebeveiliging, leveranciersrelaties, beheer van informatiebeveiligingsincidenten, informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer, naleving en de acquisitie, ontwikkeling en het onderhoud van informatiesystemen.

Op basis van de NEN-ISO/IEC 27001 en 27002 gelden er in Nederland voor de publieke sector vijf bedrijfsspecifieke modellen. Deze modellen zijn aangevuld met eigen inzichten, dit is achter de specifieke eisen gemarkeerd. In elk van deze modellen is er een onderscheid gemaakt tussen tactische kaders en normen kaders. Het tactische deel verwijst naar de '*best practices*' en het

normen deel naar een Information Security Management System. In het vervolg van deze paragraaf is per model het doel beschreven en zijn de hoofdcategorieën omschreven. Het betreft de volgende modellen:

- SURF Startkit informatiebeveiliging voor het hoger onderwijs en wetenschappelijk onderzoek (2010);
- SA-MBO ICT programma Informatiebeveiliging en Privacy, Normenkader en toetsingskader informatiebeveiliging mbo (2015);
- Baseline Informatiebeveiliging Rijksdienst (BIR 2012);
- Tactische Baseline Informatiebeveiliging Gemeenten(BIG 2013);
- Strategische Baseline Informatiebeveiliging Gemeenten(BIG 2013);
- Baseline Informatiebeveiliging Waterschappen (BIW 2013);

2.3.4 SURF Startkit informatiebeveiliging voor het hoger onderwijs en wetenschappelijk onderzoek

De SURF Startkit informatiebeveiliging (2010) is een handleiding om op een projectmatige wijze te komen tot gestructureerde informatiebeveiliging. Startkit, verwijst naar de beginfase van het ontwikkelen van het informatiebeveiligingsbeleid. Dit document is voornamelijk als advies opgesteld en bevat tips en kleine overzichten van waar informatiebeveiliging aan zou moeten voldoen. In de Startkit wordt verwezen naar:

- *'De Code voor Informatiebeveiliging'(NEN-ISO/IEC 27002) (2007)*
- *het IABB-procesmodel voor een gestructureerde aanpak' (van Stichting SURF)(1998)*

Binnen het Startkit worden geen (nieuwe) eisen gesteld en wordt er vooral een manier beschreven over hoe met deze eisen om te gaan. Surf Startkit betreft een normenkader in de vorm van stappenplan voor een plan van aanpak met een IST-SOLL situatieschets. Het bevat geen factoren en voornamelijk een stappenplan:

- *Fase 1: inventarisatie huidige situatie;*
- *Fase 2: korte termijn verbeteringen en opstellen Plan van Aanpak;*
- *Fase 3: de dialoog met bestuurders;*
- *Fase 4: projectmatige uitvoering Plan van Aanpak;*
- *Fase 5: beheer.*

2.3.5 en Privacy, Normenkader en toetsingskader informatiebeveiliging mbo

SA-MBO ICT is een overkoepelende organisatie voor al het MBO onderwijs. De organisatie is onder andere gelieerd aan de MBO Raad, Kennisnet en SURF. De organisatie heeft drie pijlers:

- *belangenbehartiging; SA-MBO ICT programma Informatiebeveiliging*
- *kennisdeling;*
- *gezamenlijke projecten.*

Het programma informatiebeveiliging heeft de veelvoorkomende opdeling tussen de normenkader en het toetsingskader (vaker bekend als tactisch kader). Beide kaders verwijzen naar dezelfde clusters, en het verschil lijkt hier enkel te zitten in de doelgroep. Het is de enige uit de rij

Nederlandse richtlijnen welke naast de benoemde ISO-standaard ook de richtlijn van het CPB in acht neemt. Het gebruik van de kaders is als volgt gedefinieerd:

> "Het Normenkader Informatiebeveiliging MBO wordt in de MBO-sector gebruikt als referentie voor informatie-beveiliging. Het wordt voor ditzelfde doel ook gebruikt in de HO sector. Op basis van dit normenkader kan een instelling bepalen of zij voldoet aan de eisen die gesteld worden. Bij het Normenkader Informatiebeveiliging MBO hoort een toetsingskader. In dit toetsingskader staat in detail beschreven wat een instelling geregeld moet hebben om aan de normen te voldoen. Dat toetsingskader is een separaat document, is opgesteld door interne auditors van de instellingen en afgestemd met informatiebeveiligers van de instellingen en externe auditpartijen, onder meer met de auditors van de grootste accountsbureaus. Het Normenkader Informatiebeveiliging MBO is de basis voor audits, self-assessments en peer-reviews in het kader van MBOaudit." (SA-MBO ICT, 2015, p. 4)

Tabel 4 SA-MBO ICT programma Informatiebeveiliging en Privacy,Normenkader en toetsingskader informatiebeveiliging mbo (2015)

SA-MBO ICT- Toetsingskader Informatiebeveiliging cluster 1 t/m 6 (2015)	
Categorieën	**Beschrijving**
Beleid en organisatie	Betreft: ☐ Beleidsregels voor informatiebeveiliging ☐ Beoordeling van het Informatiebeveiligingsbeleid ☐ Taken en verantwoordelijkheden informatiebeveiliging ☐ Informatiebeveiliging in projectbeheer ☐ Beleid voor mobiele apparatuur ☐ Classificatie van informatie ☐ Informatie labelen ☐ Beleid inzake het gebruik van cryptografische beheersmaatregelen ☐ Beleid inzake het gebruik van cryptografische beheersmaatregelen ☐ Verwijdering van bedrijfsmiddelen ☐ Beleid en procedures voor informatietransport ☐ Overeenkomsten over informatietransport: ☐ Analyse en specificatie van informatiebeveiligingseisen ☐ Opnemen van beveiligingsaspecten in leveranciersovereenkomsten ☐ Toeleveringsketen van informatie- en communicatietechnologie ☐ Verantwoordelijkheden en procedures ☐ Rapportage van informatiebeveiligingsgebeurtenissen ☐ Beschermen van registraties ☐ Privacy en bescherming van persoonsgegevens ☐ Scheiding van taken
Personeel, studenten en gasten	Betreft: ☐ Arbeidsvoorwaarden ☐ Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging ☐ Toegangsrechten intrekken of aanpassen ☐ 'Clear desk'- en 'clear screen'-beleid ☐ Vertrouwelijkheids- of geheimhoudingsovereenkomst ☐ Rapportage van zwakke plekken in de informatiebeveiliging ☐ Screening
Ruimten en apparatuur	Betreft: ☐ Beleid voor mobiele apparatuur ☐ Verwijderen van media ☐ Fysieke beveiligingszone ☐ Fysieke toegangsbeveiliging ☐ Kantoren, ruimten en faciliteiten beveiligen ☐ Beschermen tegen bedreigingen van buitenaf ☐ Werken in beveiligde gebieden ☐ Laad- en loslocatie: ☐ Plaatsing en bescherming van apparatuur ☐ Nutsvoorzieningen ☐ Beveiliging van bekabeling ☐ Onderhoud van apparatuur: ☐ Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein ☐ Veilig verwijderen of hergebruiken van apparatuur ☐ Kloksynchronisatie

Continuïteit	Betreft: ☐ Wijzigingsbeheer ☐ Scheiding van ontwikkel-, test- en productieomgevingen ☐ Beheersmaatregelen tegen malware ☐ Back-up van informatie ☐ Software installeren op operationele systemen ☐ Beheer van technische kwetsbaarheden ☐ Beperkingen voor het installeren van software ☐ Beveiligde ontwikkelomgeving ☐ Beheer van veranderingen in dienstverlening van leveranciers ☐ Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen ☐ Respons op informatiebeveiligingsincidenten ☐ Informatiebeveiligingscontinuïteit implementeren ☐ Beschikbaarheid van informatie verwerkende faciliteiten
Toegangsbeveiliging /Vertrouwelijkheid en integriteit	Betreft: ☐ Beleid voor toegangsbeveiliging ☐ Toegang tot netwerken en netwerkdiensten ☐ Registratie en afmelden van gebruikers ☐ Gebruikers toegang verlenen ☐ Beheren van speciale toegangsrechten ☐ Beheer van geheime authenticatie-informatie van gebruikers ☐ Geheime authenticatie-informatie gebruiken ☐ Beperking toegang tot informatie ☐ Beveiligde inlogprocedures ☐ Sleutelbeheer ☐ Beschermen van informatie in logbestanden ☐ Beheersmaatregelen voor netwerken ☐ Beveiliging van netwerkdiensten ☐ Scheiding in netwerken ☐ Elektronische berichten ☐ Transacties van toepassingen beschermen
Controle en logging	Betreft: ☐ Beoordeling van toegangsrechten van gebruikers ☐ Gebeurtenissen registreren ☐ Logbestanden van beheerders en operators ☐ Uitbestede softwareontwikkeling ☐ Testen van systeembeveiliging ☐ Systeemacceptatietests ☐ Monitoring en beoordeling van dienstverlening van leveranciers ☐ Verzamelen van bewijsmateriaal ☐ Naleving van beveiligingsbeleid en –normen ☐ Beoordeling van technische naleving

2.3.6 Baseline Informatiebeveiliging Rijksdienst (BIR)

De BIR betreft een richtlijn dat geldt voor de gehele Rijksdienst. Voordat de BIR in werking trad was er sprake van vijf richtlijnen, waardoor er tal van verschillende aanpakken binnen de Rijksoverheid optraden. Het betreft de vervanging van de Haagse Ring, Rijksweb, mobiele datadragers, Departementaal Vertrouwelijke webapplicaties en Digitale Werkomgeving Rijksdienst. Al deze verschillen zorgde voor een wildgroei aan verschillende voorzieningen met dezelfde functies en moeilijkheden als het gaat om centraal beheer en centrale implementatie.

> "De BIR:2012 bestaat uit een tactisch normenkader (TNK) en een operationele baseline (OB). Het tactische normenkader is verplicht (comply or explain). De operationele baseline is niet verplicht, het is een best practice. De patronen uit de OB voldoen aan het TNK maar het toepassen van een patroon uit de operationele baseline ontslaat de organisatie niet van de verplichting om aan te tonen dat zij voldoet aan het gehele TNK."(Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2012, p. 4)

Tabel 5 Baseline Informatiebeveiliging Rijksdienst (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2012)

Baseline Informatiebeveiliging Rijksdienst (2012)	
Categorieën	**Beschrijving**
Beveiligingsbeleid	Directie richting en ondersteuning bieden voor Informatiebeveiliging overeenkomstig de bedrijfsmatige eisen en relevante wetten en voorschriften.
Organisatie van de Informatiebeveiliging	Beheren van de informatiebeveiliging binnen de organisatie. Beveiligen van de informatie en ICT-voorzieningen van de organisatie handhaven waartoe externe partijen toegang hebben of die door externe partijen worden verwerkt of beheerd, of die naar externe partijen wordt gecommuniceerd.
Beheer van bedrijfsmiddelen	Bereiken en handhaven van een adequate bescherming van bedrijfsmiddelen van de organisatie. Bewerkstelligen dat informatie een geschikt niveau van bescherming krijgt.
Personele beveiliging	Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers hun verantwoordelijkheden begrijpen, en geschikt zijn voor de rollen waarvoor zij worden overwogen, en om het risico van diefstal, fraude of misbruik van faciliteiten te verminderen. Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers ordelijk de organisatie verlaten of hun dienstverband wijzigen. Bewerkstelligen dat alle werknemers, ingehuurd personeel en externe gebruikers zich bewust zijn van bedreigingen en gevaren voor informatiebeveiliging, van hun verantwoordelijkheid en aansprakelijkheid, en dat ze zijn toegerust om het beveiligingsbeleid van de organisatie in hun dagelijkse werkzaamheden te ondersteunen, en het risico van een menselijke fout te verminderen.
Fysieke beveiliging en beveiliging van de omgeving	Het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatie van de organisatie. Het voorkomen van verlies, schade, diefstal of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten. Plaatsing en bescherming van apparatuur
Beheer van Communicatie- en Bedieningsprocessen	Waarborgen van een correcte en veilige bediening van IT voorzieningen. Een geschikt niveau van informatiebeveiliging en dienstverlening implementeren en bijhouden in overeenstemming met de overeenkomsten voor dienstverlening door een derde partij. Het risico van systeemstoringen tot een minimum beperken. Beschermen van de integriteit van programmatuur en informatie. Handhaven van de integriteit en beschikbaarheid van informatie en IT voorzieningen. Bewerkstelligen van de bescherming van informatie in netwerken en bescherming van de ondersteunende infrastructuur. Voorkomen van onbevoegde openbaarmaking, modificatie, verwijdering of vernietiging van bedrijfsmiddelen en onderbreking van bedrijfsactiviteiten. Handhaven van beveiliging van informatie en programmatuur die wordt uitgewisseld binnen een organisatie en met enige externe entiteit. Bewerkstelligen van de beveiliging van diensten voor e-commerce en het veilig gebruik van de diensten. Ontdekken van onbevoegde informatieverwerkingsactiviteiten.
Toegangsbeveiliging	Beheersen van de toegang tot informatie. Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot informatiesystemen voorkomen. Voorkomen van onbevoegde toegang door gebruikers, en van beschadiging of diefstal van informatie en ICT-voorzieningen. Het voorkomen van onbevoegde toegang tot netwerkdiensten. Voorkomen van onbevoegde toegang tot besturingssystemen. Voorkomen van onbevoegde toegang tot informatie in toepassingssystemen. Waarborgen van informatiebeveiliging bij het gebruik van draagbare computers en faciliteiten voor telewerken.
Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Bewerkstelligen dat beveiliging integraal deel uitmaakt van informatiesystemen. Voorkomen van fouten, verlies, onbevoegde modificatie of misbruik van informatie in toepassingen. Beschermen van de vertrouwelijkheid, authenticiteit of integriteit van informatie met behulp van cryptografische middelen. Beveiliging van systeembestanden bewerkstelligen. Beveiliging van toepassingsprogrammatuur en -informatie handhaven. Risico's verminderen als gevolg van benutting van gepubliceerde technische kwetsbaarheden.
Beheer van Informatiebeveiligingsincidenten	Bewerkstelligen dat informatiebeveiligingsgebeurtenissen en zwakheden die verband houden met informatiesystemen zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen. Bewerkstelligen dat een consistente en doeltreffende benadering wordt

	toegepast voor het beheer van informatiebeveiligingsincidenten.
Bedrijfscontinuïteitsbeheer	Tegengaan van onderbreking van bedrijfsactiviteiten en bescherming van kritische bedrijfsprocessen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.
Naleving	Voorkomen van schending van enige wetgeving, wettelijke en regelgevende of contractuele verplichtingen, en van enige beveiligingseisen. Bewerkstelligen dat systemen voldoen aan het beveiligingsbeleid en de beveiligingsnormen van de organisatie. Doeltreffendheid van audits van het informatiesysteem maximaliseren en verstoring als gevolg van systeemaudits minimaliseren.

2.3.7 Baseline Informatiebeveiliging Gemeenten

De Baseline Informatiebeveiliging Gemeenten (BIG) is opgesteld door het Kwaliteit Instituut Nederlandse Gemeenten (KING). Het KING is onderdeel van de Verenigde Nederlandse Gemeenten (VNG) welke een koepel organisatie is voor dienstverlening en belangenbehartiging ten behoeve van de gemeenten. Om de BIG te borgen en inzet vast te leggen is er ingestemd met de resolutie informatie beveiliging (Jorritsma-Lebbink, 2013). In de BIG is de volgende doelstelling geformuleerd:

> *"Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties heeft opdracht gegeven voor het ontwikkelen van een Baseline Informatiebeveiliging Nederlandse Gemeenten. De Baseline Informatiebeveiliging Nederlandse Gemeenten is bedoeld om:*
> *1. Gemeenten op een vergelijkbare manier efficiënt te laten werken met informatiebeveiliging.*
> *2. Gemeenten een hulpmiddel te geven om aan alle eisen op het gebied van Informatiebeveiliging te kunnen voldoen.*
> *3. De auditlast bij gemeenten te verminderen.*
> *4. Gemeenten een aantoonbaar betrouwbare partner te laten zijn."*(Kwaliteitsinstituut Nederlandse Gemeenten, 2013, p. VI)

Tabel 6 Tactische Baseline Informatiebeveiliging Gemeenten (IBD, 2013)

Tactische Baseline Informatiebeveiliging Gemeenten (2013)	
Categorieën	**Beschrijving**
Beveiligingsbeleid	Borgen van betrouwbare dienstverlening en een aantoonbaar niveau van informatiebeveiliging dat voldoet aan de relevante wetgeving, algemeen wordt geaccepteerd door haar (keten-)partners en er mede voor zorgt dat de kritische bedrijfsprocessen bij een calamiteit en incident voortgezet kunnen worden.
Organisatie van de Informatiebeveiliging	Voorkomen van schending van enige wetgeving, wettelijke en regelgevende of contractuele verplichtingen, en van enige beveiligingseisen.
Beheer van bedrijfsmiddelen	Bereiken en handhaven van een adequate bescherming van bedrijfsmiddelen van de organisatie. Bewerkstelligen dat informatie een geschikt niveau van bescherming krijgt. Informatie behoort te worden geclassificeerd om bij het verwerken van de informatie de noodzaak, prioriteiten en verwachte graad van bescherming te kunnen aangeven.
Personele beveiliging	Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers hun verantwoordelijkheden begrijpen, en geschikt zijn voor de rollen waarvoor zij worden overwogen, en om het risico van diefstal, fraude of misbruik van faciliteiten te verminderen. Bewerkstelligen dat alle werknemers, ingehuurd personeel en externe gebruikers zich bewust zijn van bedreigingen en gevaren voor informatiebeveiliging, van hun verantwoordelijkheid en aansprakelijkheid, en dat ze zijn toegerust om het beveiligingsbeleid van de organisatie in hun dagelijkse werkzaamheden te ondersteunen en het risico van een menselijke fout te verminderen. Bewerkstelligen dat werknemers, ingehuurd personeel en

	externe gebruikers ordelijk de organisatie verlaten of hun dienstverband wijzigen.
Fysieke beveiliging en beveiliging van de omgeving	Het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatie van de organisatie. Het voorkomen van verlies, schade, diefstal of compromitteren van bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten. Plaatsing en bescherming van apparatuur
Beheer van Communicatie- en Bedieningsprocessen	Waarborgen van een correcte en veilige bediening van ICT-voorzieningen. Een geschikt niveau van informatiebeveiliging en dienstverlening implementeren en bijhouden in overeenstemming met de overeenkomsten voor dienstverlening door een derde partij. Het risico van systeemstoringen tot een minimum beperken. Beschermen van de integriteit van programmatuur en informatie. Handhaven van de integriteit en beschikbaarheid van informatie en IT-voorzieningen. Bewerkstelligen van de bescherming van informatie in netwerken en bescherming van de ondersteunende infrastructuur. Voorkomen van onbevoegde openbaarmaking, modificatie, verwijdering of vernietiging van bedrijfsmiddelen en onderbreking van bedrijfsactiviteiten. Handhaven van beveiliging van informatie en programmatuur die wordt uitgewisseld binnen een organisatie en met enige externe entiteit. Bewerkstelligen van de beveiliging van diensten voor e-commerce, en veilig gebruik ervan. Ontdekken van onbevoegde informatieverwerkingsactiviteiten.
Toegangsbeveiliging	Beheersen van de toegang tot informatie. Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot informatiesystemen voorkomen. Voorkomen van onbevoegde toegang door gebruikers, en van beschadiging of diefstal van informatie en ICT-voorzieningen. Het voorkomen van onbevoegde toegang tot netwerkdiensten. Voorkomen van onbevoegde toegang tot besturingssystemen.Voorkomen van onbevoegde toegang tot informatie in toepassingssystemen. Waarborgen van informatiebeveiliging bij het gebruik van draagbare computers en faciliteiten voor telewerken.
Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Bewerkstelligen dat beveiliging integraal deel uitmaakt van informatiesystemen. Voorkomen van fouten, verlies, onbevoegde modificatie of misbruik van informatie in toepassingen. Beschermen van de vertrouwelijkheid, authenticiteit of integriteit van informatie met behulp van cryptografische middelen. Beveiliging van systeembestanden bewerkstelligen. Beveiliging van toepassingsprogrammatuur en -informatie handhaven. Risico's verminderen als gevolg van benutting van gepubliceerde technische kwetsbaarheden.
Beheer van Informatiebeveiligingsincidenten	Bewerkstelligen dat informatiebeveiligingsgebeurtenissen en zwakheden die verband houden met informatiesystemen zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen. Bewerkstelligen dat een consistente en doeltreffende benadering wordt toegepast voor het beheer van informatiebeveiligingsincidenten.
Bedrijfscontinuïteitsbeheer	Tegengaan van onderbreking van bedrijfsactiviteiten en bescherming van kritische bedrijfsprocessen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.
Naleving	Beheren van de informatiebeveiliging binnen de organisatie. Het beveiligen van de informatie en ICT-voorzieningen van de organisatie handhaven waartoe externe partijen toegang hebben of die door externe partijen worden verwerkt of beheerd, of die naar externe partijen wordt gecommuniceerd. Bewerkstelligen dat systemen voldoen aan het beveiligingsbeleid en de beveiligingsnormen van de organisatie. Doeltreffendheid van audits van het informatiesysteem maximaliseren en verstoring als gevolg van systeemaudits minimaliseren.

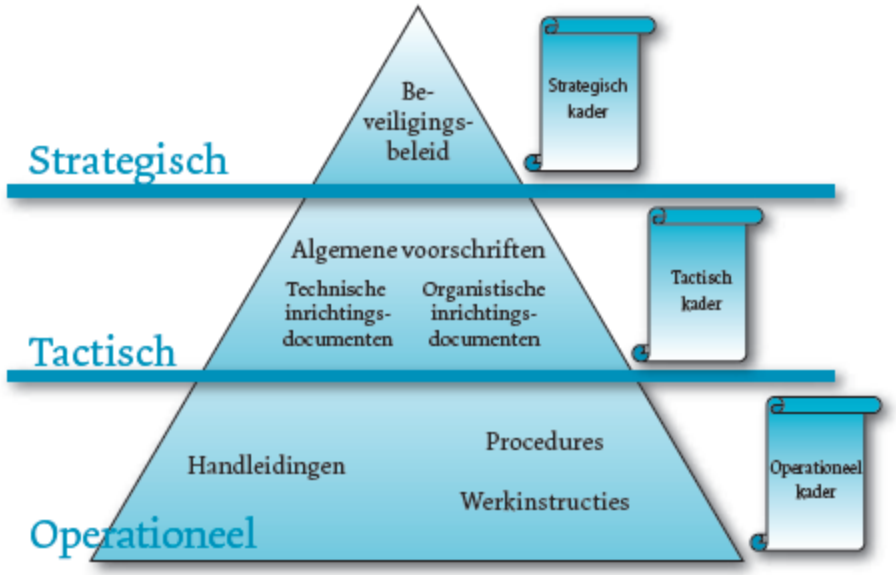
2.3.8 Baseline Informatiebeveiliging Waterschappen

De Baseline Informatiebeveiliging Waterschappen (BIWA) is in 2013 gepubliceerd door de Unie van Waterschappen. Deze Unie betreft een vereniging van alle Nederlandse Waterschappen en behartigt de belangen, deelt kennis zowel nationaal als internationaal en stimuleert samenwerking. De BIWA heeft als doel om te bewerkstelligen dat:

1. "Waterschappen op een vergelijkbare- en efficiëntere manier werken met informatiebeveiliging;

2. Waterschappen van een leidraad worden voorzien om aan alle relevante eisen op het gebied van Informatiebeveiliging te kunnen voldoen;
3. Er een eenduidig toetsingskader geboden wordt voor informatieveiligheid over alle waterschappen;
4. Waterschappen een aantoonbaar betrouwbare partner kunnen aantonen te zijn.” (Unie van Waterschappen, 2013, p. 12)

Wat opvalt, is dat de waterschappen naast een normen- en tactisch kader ook het operationeel kader uitlicht. Hiervoor is de volgende piramide opgesteld:



Figuur 1 BIWA Piramide (Waterschappen, 2013, p. 13)

Tabel 7 Baseline Informatiebeveiliging Waterschappen ‘Tactisch Normenkader’ (Waterschappen, 2013)

Baseline Informatiebeveiliging Waterschappen ‘Tactisch Normenkader’ (2013)	
Categorieën	**Beschrijving**
Beveiligingsbeleid	Borgen van betrouwbare dienstverlening en een aantoonbaar niveau van informatiebeveiliging dat voldoet aan de relevante wetgeving, algemeen wordt geaccepteerd door haar (keten-)partners en er mede voor zorgt dat de kritieke bedrijfsprocessen bij een calamiteit en incident voortgezet kunnen worden.
Organisatie van de Informatiebeveiliging	Beheren van de informatiebeveiliging binnen de organisatie. Beveiligen van de informatie en ICT-voorzieningen van de organisatie handhaven waartoe externe partijen toegang hebben of die door externe partijen worden verwerkt of beheerd, of die naar externe partijen wordt gecommuniceerd.
Beheer van bedrijfsmiddelen	Bereiken en handhaven van een adequate bescherming van bedrijfsmiddelen van de organisatie. Bewerkstelligen dat informatie een geschikt niveau van bescherming krijgt. Informatie behoort te worden geclassificeerd om bij het verwerken van de informatie de noodzaak, prioriteiten en verwachte graad van bescherming te kunnen aangeven.
Personele beveiliging	Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers hun verantwoordelijkheden begrijpen, en geschikt zijn voor de rollen waarvoor zij worden overwogen, en om het risico van diefstal, fraude of misbruik van faciliteiten te verminderen. Bewerkstelligen dat alle werknemers, ingehuurd personeel en externe gebruikers zich bewust zijn van bedreigingen en gevaren voor informatiebeveiliging, van hun verantwoordelijkheid en aansprakelijkheid, en dat ze zijn toegerust om het beveiligingsbeleid van de organisatie in hun dagelijkse werkzaamheden te ondersteunen en het risico van een menselijke fout te verminderen. Bewerkstelligen dat werknemers, ingehuurd personeel en

	externe gebruikers ordelijk de organisatie verlaten of hun dienstverband wijzigen.
Fysieke beveiliging en beveiliging van de omgeving	Het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatie van de organisatie. Het voorkomen van verlies, schade, diefstal of compromitteren van bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten.
Beheer van Communicatie- en Bedieningsprocessen	Waarborgen van een correcte en veilige bediening van ICT-voorzieningen. Een geschikt niveau van informatiebeveiliging en dienstverlening implementeren en bijhouden in overeenstemming met de overeenkomsten voor dienstverlening door een derde partij. Het risico van systeemstoringen tot een minimum beperken. Beschermen van de integriteit van programmatuur en informatie. Handhaven van de integriteit en beschikbaarheid van informatie en IT voorzieningen. Bewerkstelligen van de bescherming van informatie in netwerken en bescherming van de ondersteunende infrastructuur. Voorkomen van onbevoegde openbaarmaking, modificatie, verwijdering of vernietiging van bedrijfsmiddelen en onderbreking van bedrijfsactiviteiten. Handhaven van beveiliging van informatie en programmatuur die wordt uitgewisseld binnen een organisatie en met enige externe entiteit. Bewerkstelligen van de beveiliging van diensten voor e-commerce, en veilig gebruik ervan. Ontdekken van onbevoegde informatieverwerkingsactiviteiten.
Toegangsbeveiliging	Beheersen van de toegang tot informatie. Er behoort toegangsbeleid te worden vastgesteld, gedocumenteerd en beoordeeld op basis van organisatie-eisen en beveiligingseisen voor toegang. Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot informatiesystemen voorkomen. Voorkomen van onbevoegde toegang door gebruikers, en van beschadiging of diefstal van informatie en ICT-voorzieningen. Gebruik van wachtwoorden. Het voorkomen van onbevoegde toegang tot netwerkdiensten. Voorkomen van onbevoegde toegang tot besturingssystemen. Voorkomen van onbevoegde toegang tot informatie in toepassingssystemen. Waarborgen van informatiebeveiliging bij het gebruik van alle vormen van draagbare computers en faciliteiten voor telewerken.
Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Bewerkstelligen dat beveiliging integraal deel uitmaakt van informatiesystemen. Voorkomen van fouten, verlies, onbevoegde modificatie of misbruik van informatie in toepassingen. Beschermen van de vertrouwelijkheid, authenticiteit of integriteit van informatie met behulp van cryptografische middelen. Beveiliging van systeembestanden bewerkstelligen. Beveiliging van toepassingsprogrammatuur en -informatie handhaven. Risico's verminderen als gevolg van benutting van gepubliceerde technische kwetsbaarheden.
Beheer van Informatiebeveiligingsincidenten	Bewerkstelligen dat informatiebeveiligingsgebeurtenissen en zwakheden die verband houden met informatiesystemen zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen. toegepast voor het beheer van informatiebeveiligingsincidenten.
Bedrijfscontinuïteitsbeheer	Tegengaan van onderbreking van bedrijfsactiviteiten en bescherming van kritieke bedrijfsprocessen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.
Naleving	Voorkomen van schending van enige wetgeving, wettelijke en regelgevende of contractuele verplichtingen, en van enige beveiligingseisen. Bewerkstelligen dat systemen voldoen aan het beveiligingsbeleid en de beveiligingsnormen van de organisatie. Doeltreffendheid van audits van het informatiesysteem maximaliseren en verstoring als gevolg van systeemaudits minimaliseren.

2.3.9 Overeenkomsten en verschillen binnen de richtlijnen voor informatiebeveiliging in de publieke sector

Al met al is het *'Information Security Management Systeem'* bij elk van de Nederlandse richtlijnen toegepast als normenkader. In de richtlijn NIST Special Publication 800-27 wordt dit anders ingevuld door uit te gaan van life cycle planning. Dit onderdeel richt zich op beveiliging van een systeem of applicatie in iedere 'levens cyclus fase', deze fases zijn onderscheiden in initiatie, ontwikkeling/acquisitie, implementatie, operatie en verwijdering. Bij elk adviespunt wordt aangegeven in welke fase dat punt van belang is. Daarbij wordt er zwaarte aan meegegeven door

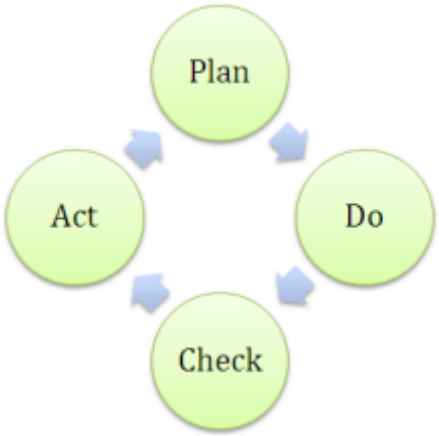
bij grotere zwaarte twee vinkjes in plaats van één vinkje te plaatsen. Dit geeft een andere invulling aan het normenkader waardoor deze niet gescheiden is- en een onderdeel is van de vereisten ofwel tactisch kader. Het normenkader van alle baselines en het SA-MBO ICT programma Informatiebeveiliging, bestaat uit afspraken over de scope, uitgangspunten, randvoorwaarden, plaatsbepaling en reikwijdte, beleid, verantwoordelijkheden, opzet, beheer en onderhoud. Dit normenkader betreft een los hoofdstukstuk voorafgaand aan het pakket aan vereisten zoals beschreven in het tactisch kader. Bij het SURF Startkit betreft het voornamelijk een stappenplan om tot een informatiebeveiligingssysteem te komen. De indeling van de Baselines betreft een structuur met drie niveaus van categorieën, waarin de daadwerkelijke eisen staan beschreven. In bepaalde categorieën zijn er geen eisen opgenomen, en bepaalde eisen hebben geen laag in de categorieën. De andere baselines hebben deze structuur overgenomen, aangepast en aangevuld. Wat opvalt, is dat de andere richtlijnen minder vereisten bevatten, terwijl deze zich ook zijn gebaseerd op de ISO-IEC 27000 series. Het SA-MBO ICT- Toetsingskader is op relatief minder bronnen gebaseerd dan de overige richtlijnen, en heeft minder eisen dan de andere Nederlandse richtlijnen. In Tabel 8 is opgenomen hoeveel vereisten er per richtlijn zijn opgenomen.

Tabel 8 Richtlijnen voor informatiebeveiliging in de publieke sector

Baseline Informatiebeveiliging Rijksdienst (2012)		**SA-MBO ICT- Toetsingskader Informatiebeveiliging cluster 1 t/m 6 (2015)**	
Bedrijfscontinuïteitsbeheer	10	Cluster beleid en organisatie	21
Beheer van bedrijfsmiddelen	9	Continuïteit	15
Beheer van Communicatie- en Bedieningsprocessen	88	Controle en logging	10
Beheer van Informatiebeveiligingsincidenten	8	Personeel, studenten en gasten	7
Beveiligingsbeleid	2	Ruimten en apparatuur	15
Fysieke beveiliging en beveiliging van de omgeving	35	Toegangsbeveiliging en integriteit	17
Naleving	11		
Organisatie van de Informatiebeveiliging	25		
Personele beveiliging	16		
Toegangsbeveiliging	55		
Verwerving, ontwikkeling en onderhoud van Informatiesystemenen	39		
	298	Totaal aantal vereisten	85
Baseline Informatiebeveiliging Waterschappen (2013)		**Tactische Baseline Informatiebeveiliging Gemeenten (2013)**	
Bedrijfscontinuïteitsbeheer	4	Bedrijfscontinuïteitsbeheer	4
Beheer van bedrijfsmiddelen	9	Beheer van bedrijfsmiddelen	10
Beheer van Communicatie- en Bedieningsprocessen	70	Beheer van Communicatie- en Bedieningsprocessen	79
Beheer van Informatiebeveiligingsincidenten	11	Beheer van Informatiebeveiligingsincidenten	10
Beveiligingsbeleid	2	Beveiligingsbeleid	5
Fysieke beveiliging en beveiliging van de omgeving	33	Fysieke beveiliging en beveiliging van de omgeving	38
Naleving	6	Naleving	7
Organisatie van de Informatiebeveiliging	23	Organisatie van de Informatiebeveiliging	27
Personele beveiliging	14	Personele beveiliging	17
Toegangsbeveiliging	18	Toegangsbeveiliging	52
Toegangsbeveiliging voor besturingssystemen	19	Verwerving, ontwikkeling en onderhoud van Informatiesystemen	42
Verwerving, ontwikkeling en onderhoud van Informatiesystemen	37		
Totaal aantal vereisten	246	Totaal aantal vereisten	291
NIST Special Publication 800-27 Rev A Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A			
Design with Network in Mind	4		
Ease of Use	4		
Increase Resilience	8		
Reduce Vulnerabilities	6		
Risk Based	7		
Security Foundation	4		
Totaal aantal vereisten	33		

2.4 Information Security Management System

In de NEN-ISO/IEC 27001:2013 is er sprake van het 'Information Security Management Systeem' deze is te definiëren al een type kwaliteitsmanagementsysteem. Het betreft het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System (ISMS) in het kader van de algemene bedrijfsrisico's voor de organisatie. Een ISMS is een kwaliteitssysteem. Er is sprake van een kwaliteitsmanagementsysteem wanneer een organisatie op een bewuste en systematische manier invulling geeft aan kwaliteit. Linker (2006, p. 280) geeft de volgende definitie aan kwaliteit "Net iets meer dan voldoen aan de steeds toenemende uitgesproken en vanzelfsprekende verwachting"(idem). Deze cirkel is opgebouwd uit vier stappen. Deze stappen zijn: *'plan', 'do', 'check'* en *'act'*.



1. *Plan: bepalen van de doelstelling en de inrichting van processen om deze doelstellingen te realiseren;*
2. *Do: de uitvoering van het plan;*
3. *Check: nagaan of de doelstellingen de inrichting van processen zoals vastgesteld bij 'plan' wordt nageleefd*
4. *Act: verbeteren en bijstellen van van de richting en inrichting naar aanleiding van (management) informatie, welke is ontleend tijdens stap* 'check'

Een kwaliteitssysteem wordt als volgt gedefinieerd: *'een continue verbetering van de inrichting, verrichting en bijsturing van processen'*. Met dit uitgangspunt is er meer aandacht voor het gehele proces en wordt continuiteit gewaarborgd; de integrale benadering. Het gaat minder om het resultaat in nummers en indicatoren, en meer om het resultaat naar aanleiding van inspanning en organisatie. Ook het systematisch borgen van kwaliteit kent valkuilen. Zo is uitdijing van beleid en het verbeteren om te verbeteren een uitwerking waarbij de doelstellingen van beleid uit het oog worden verloren (Linker, 2006, pp. 287-288). Daarbij is niet ieder incident te voorkomen of the bestrijden. Hierbij kan verregaande regulering een organisatie logger maken.

2.5 Bepalende factoren binnen een informatiebeveiligingssysteem

In deze paragraaf zijn de factoren welke, conform '*State of the Art',* van belang zijn voor het organiseren van informatiebeveiliging in de publieke sector. Deze zijn gebaseerd op de bovenstaande beschrijving van academische benaderingen en richtlijnen van de laatste 15 jaar. De pluriformiteit binnen de bestaande richtlijnen is hoog, waardoor deze multi-interpreteerbaar zijn en is er overlap aanwezig tussen de verschillende categorieën. In dit onderzoek is er een vertaling gemaakt van richtlijnen en theorie naar factoren. Factoren zijn specifieker, waardoor een duidelijke scheiding aangebracht kan worden tussen de factoren. Voor het verhogen van de betrouwbaarheid

en validiteit voor wetenschappelijk onderzoek is een duidelijke scheiding nodig; het kunnen aanduiden van een feitelijk gegeven op basis van vastgestelde meetwaarden.

Er zijn zeven factoren opggesteld, welke onderstaand nader zijn beschreven. Deze factoren zijn gedestilleerd uit een selectie academische literatuur en uit een selectie aan richtlijnen. De keuze voor de zeven factoren is gebaseerd op de nadruk op een integrale aanpak en de veel voorkomende onderwerpen uit de richtlijnen. Integraal betekent in deze definitie *'het toepassen van een informatiebeveiligingssysteem in de gehele organisatie'*. Voor de toepassing van de factoren geldt de aanwezigheid van een informatiebeveiligingssysteem als voorwaarde. Bij een informatiebeveiligingssysteem is er sprake van procesmatige sturing. Hierbinnen passen geen vereisten die enkel gericht zijn op wat er in orde moet zijn voor de beveiliging van informatie en passen. Wel passen de vereisten die aangeven hoe informatie beveiligd kan worden. Hierbij is de onderliggende vraag 'in hoeverre is er uiting van de aandachtsgebieden binnen een informatiebeveiligingssysteem te herkennen?' ten opzichte van een typische audit waarbij de vraag 'wordt voldaan aan de vereisten?' centraal staat. In

Tabel 9 is een overzicht van de dekking van de factoren ten opzichte van de categorieën die zijn beschreven in dit hoofdstuk opgenomen. Het uitgebereidde tabel is te vinden in Bijlage 5.

Het blijkt zowel vanuit de academische benaderingen als de inhoud van de gestelde richtlijnen dat er gepleit wort voor een kwaliteitssysteem. Daarbij zijn er in de Nederlandse richtlijnen meer dan 84 specifieke vereisten opgenomen waaraan een concrete actie is verbonden. Kritiek op het informatiebeveiligingssysteem betreft dat het kan leiden tot uitdijing met als gevolg verregaande regulering en een loggere organisatie (Linker, 2006, pp. 287-288). Kritiek op het informatiebeveiligingsstandaarden betreft een tekortkoming op het gebied van verschillen tussen organisaties, sociale achtergronden van beleidsproblemen, ondersteuning bij hoe te komen tot besluitvorming en conflicten tussen reguliere standaarden in de organisatie en informatiebeveiligingsstandaarden (Baskerville & Siponen, 2002). Hiertoe zijn er geen specifieke eisen in de onderstaande factoren opgenomen. Daarbij dienen de factoren onderdeel te zijn van een informatiebeveiligingssysteem, dit borgt enige vorm van afbakening. Zodoende is er getracht de kritiek in acht te nemen dat op zowel het gebruik van standaarden als informatiebeveiligingssystemen gegeven word.

1. Strategie

Vanuit de missie, visie en bestuurlijke doelstellingen van de organisatie dient gekeken te worden naar het strategisch besturingsniveau van de aanwezige applicaties en systemen. De organisatie van informatiebeveiliging dient in de ideale situatie aan te sluiten, bij de missie, visie en doelstellingen van de organisatie. Binnen de organisatiestructuur van informatiebeveiliging(IT) wordt de strategie gevormd door de IT-architectuur van de gehele organisatie. De architectuur bevat "Een beschrijving van een complex geheel, en van de principes die van toepassing zijn op de ontwikkeling van het geheel en zijn onderdelen" (Goutier & van Lieshout, 2010, p. 69). Dit biedt een totaaloverzicht van alle systemen, applicaties, data-opslag en de koppelingen in het gehele netwerk waardoor er inzicht ontstaat op de risico's en knooppunten.

2. Beleid

Er dient een formeel geformuleerd, afgestemd en geïmplementeerd beleid aanwezig te zijn hoe de informatiebeveiligingsmaatregelen uit te voeren in de organisatie. Eveneens dient er handhaving en actualisatie plaats te vinden op dit beleid. Dit dient plaats te vinden op basis van een risicoanalyse.

3. Gebruiksbeheer

De informatiebeveiligingsmaatregelen dienen, voor zover mogelijk, te passen binnen de dagelijkse handelingen van de eindgebruikers en de beheerders/gebruikers met meer rechten (priveleged users). Eveneens is er sprake van een informatiebeveiligingscultuur. Gebruikers dienen kennis te hebben van de aanwezige informatiebeveiligingsrisico's; er dient acceptatie aanwezig te zijn in de organisatie om de informatiebeveiligingsmaatregelen optimaal te kunnen uitvoeren. Gebruikersbeheer richt zich op het gedrag van- en het gemak voor de gebruikers van informatievoorzieningen op operationeel niveau én de balans naar de benodigde maatregelen vanuit strategisch niveau. Bij een hoge mate van ongemak is er de kans dat men het systeem omzeilt of het onjuist gebruikt. Zo zou een gebruiker vertrouwelijke gegevens onopzettelijke kunnen lekken. Hiermee is het gedrag binnen de organisatie minder voorspelbaar, complexer, dit brengt andere risico's met zich mee.

4. Gegevensbeheer

De aanwezigheid van gegevens, vertaald in bijvoorbeeld data en documenten, dienen kwalitatief voldoende te zijn geborgd in de organisatie. Gegevens zijn aanwezig in diverse applicaties op diverse niveaus. De gegevens dienen overzichtelijk, toegankelijk, terugdvindbaar, volledig, betrouwbaar en integer te zijn. Middels classificaties worden gegevens op basis van de mate van vertrouwelijkheid afgeschermd. Indien de gegevens juist gelabeld zijn, is de kans op onjuiste classificatie en daarmee onbedoelde openbaarheid kleiner. Gegevensbeheer richt zich op de kwaliteit en juistheid van gegevens en daarmee de beheersbaarheid van informatie in een organisatie op operationeel niveau én de balans naar de benodigde maatregelen voor de uitvoerbaarheid van het beleid.

5. Ruimte, apparatuur en systemen

Informatiebeveiliging is er zowel op applicatie, hardware als op fysiek niveau. Toegangsbeheer van informatie dient te zijn ingeregeld op alle aspecten om onbevoegd en oneigenlijk gebruik van informatie te voorkomen. Tevens dienen de fysieke ruimten met gebruikers, applicaties, apparatuur en systemen voldoende te zijn beveiligd. Dit voorkomt het onderdruk zetten van gebruikers bij bijvoorbeeld een publieksbalie en/of diefstal.

6. Incidentmanagement

Incidentmanagement dient te zijn ingericht voor zowel het voorkomen als actief handelen bij een incident. Incidentmanagement dient te waarborgen dat de veiligheid van informatie is geborgd bij elk (nood)scenario. Dit aspect richt zich op het bewaken van de continuïteit tijdens- en direct na een incident. Hiervoor is er een incidentenplan beschikbaar welke periodiek geoefend wordt, vergelijkbaar aan een regulier calamiteitenplan.

7. Compliance

Informatiebeveiliging dient in lijn te zijn met de aanwezige Wet- en Regelgeving. Structurele toetsing hiervan, en handelen naar de uitkomsten van deze toets, is een randvoorwaarde om te komen tot betrouwbare informatiebeveiliging. De aanwezige Wet- en Regelgeving dient opgesteld te zijn in één richtinggevend kader.

Tabel 9 Dekking van bepalende factoren voor een informatiebeveiligingssysteem ten opzichte van tactische kaders

Model	Categorie	Strategie	Beleid	Gebruiksbeheer	Gegevensbeheer	Ruimte, Apparatuur en Systemen	Incidentmanagement	Compliance
NIST Special Publication 800-27	Security Foundation	√	√					
	Risk Based		√					
	Ease of Use			√				
	Increase Resilience						√	
	Reduce Vulnerabilities	√	√		√	√	√	
	Design with Network in Mind	√						
SA-MBO ICT- Toetsingskader Informatiebeveiliging cluster 1 t/m 6	Beleid en organisatie	√	√			√		
	Personeel, studenten en gasten			√		√		
	Ruimten en apparatuur					√		
	Continuïteit						√	
	Controle en logging				√			
	Toegangsbeveiliging en integriteit			√	√	√		
Baseline Informatiebeveiliging Rijksdienst, Tactische Baseline Informatiebeveiliging Gemeenten & Baseline Informatiebeveiliging Waterschappen	Beveiligingsbeleid	√	√					
	Organisatie van de Informatiebeveiliging	√	√			√		
	Beheer van bedrijfsmiddelen				√	√		
	Personele beveiliging		√	√				
	Fysieke beveiliging en beveiliging van de omgeving					√		
	Beheer van Communicatie- en Bedieningsprocessen			√	√	√		
	Toegangsbeveiliging			√	√	√		
	Verwerving, ontwikkeling en onderhoud van Informatiesystemenen			√	√	√		
	Beheer van Informatiebeveiligingsincidenten						√	
	Bedrijfscontinuïteitsbeheer						√	
	Naleving							√
Factoren erkend door academici op het gebied van informatieveiligheid	Strategie	√						
	Management	√	√					√
	Operationeel		√	√	√	√	√	
	Technisch				√	√	√	
	Informatiebeveiligingssysteem	√	√					√

3. Methodologie

In dit hoofdstuk is beschreven welke onderzoeksmethode is gehanteerd om te komen tot de beantwoording van de centrale onderzoeksvraag;

'Welke factoren zijn conform State of the Art van belang voor het organiseren van informatiebeveiliging in de publieke sector en in hoeverre komt dit tot uiting bij de Dienst Uitvoering Onderwijs in de periode van 2010-2015?'

Conform de in dit onderzoek gehanteerde definitie van informatiebeveiliging[2], is informatie veilig als vertrouwelijke informatie niet openbaar is alsmede geen ongeautoriseerd en opzettelijk misbruik wordt gemaakt van informatiesystemen. Er is geen betrouwbare registratie of beschrijving aanwezig dat de hoeveelheid vertrouwelijke informatie mogelijk is gelekt en hoe vaak er ongeautoriseerd en opzettelijk misbruik is gemaakt van informatiesystemen. Het is onbekend of de onveiligheid van informatiebeveiliging überhaupt wordt opgemerkt ofwel gemeld door de desbetreffende organisatie; hierdoor kan de omvang rondom onveiligheid van informatiebeveiliging groter zijn dan bekend is. Verder hebben de prioriteiten en aandacht vanuit de politiek invloed op het signaleren van onveiligheid. De onderwerpen waarop vanuit de politiek meer aandacht is, wordt wellicht vaker geregistreerd of raakt des te meer verborgen. Dit kan leiden tot *dark numbers* (Wittebrood & Nieuwbeerta, 2006). Het fenomeen *dark numbers* heeft veelal betrekking op 'onzichtbare' onveiligheid met betrekking tot bijvoorbeeld criminaliteit *(Vanderveen, 2011, p. 93).* Dit maakt dat zowel met het gebruik van enkel kwantitatieve gegevens als enkel kwalitatieve gegevens het beeld van moeilijk zichtbare onveiligheid onbetrouwbaar is. Het gebruik van een gecombineerde onderzoeksmethode wordt aanbevolen bij onderzoek met betrekking tot onveiligheid (Vanderveen, 2011). Het uitgangspunt in deze masterscriptie is dat het nauwelijks aan te tonen is of beleidsmaatregelen voor informatiebeveiliging effectief zijn. Dit omdat het onduidelijk is in welke mate deze maatregelen leiden tot veiligere informatievoorziening. Stone (2012) geeft aan dat perfecte veiligheid onhaalbaar is en dat het wetenschappelijke ideaal bestaat uit het streven naar het maximaliseren van veiligheid en het minimaliseren van schade door het gebruiken van beschikbare kennis. *"In the scientific ideal, analysts recognize that perfect security is unachievable, but they use all available knowledge to maximize security and minimize harms, given the realities and uncertainties of the real world (risk analysis)"(Stone, 2012, p. 133)*.

Met bovenstaande gegevens is in deze masterscriptie onderzocht welke factoren er conform de beschikbare kennis nodig zijn om veiligheid te maximaliseren en schade te minimaliseren. Vervolgens is geanalyseerd in hoeverre deze maatregelen tot uiting komen bij de DUO over de periode van 2010 tot en met 2015. In dit hoofdstuk is een nadere beschrijving van het type onderzoek, de selectie van de casus, de operationalisering, de dataverzameling en –analyse en de betrouwbaarheid en validiteit opgenomen.

[2] De definitie rondom informatiebeveiliging die in dit onderzoek wordt gehanteerd betreft: 'Informatiebeveiliging betreft het totaalpakket aan preventieve maatregelen dat eraan bijdraagt dat vertrouwelijke informatie niet openbaar beschikbaar is door bescherming te bieden tegen ongeauthoriseerd en opzettelijk misbruik van informatiesystemen.'

3.1 Type onderzoek

Zoals eerder benoemd is het belang van informatiebeveiliging steeds meer erkend, terwijl er nog niet veel wetenschappelijk onderzoek is verricht. De kern in dit onderzoek betreft het vraagstuk over wat conform S*tate of the Art* als effectieve informatiebeveiliging wordt beschouwd en in hoeverre dit tot uiting komt in de praktijk. Er zijn vanuit de beschikbare literatuur en geldende richtlijnen zeven factoren gedestilleerd die als noodzakelijk voor effectieve informatiebeveiliging worden beschouwd. De initiële benadering is hiermee in deze masterscriptie is deductief.

Om tot een veiligere informatievoorziening te komen zijn er conform *State of the Art* meerdere factoren, ook wel variabelen, nodig. Een simpele redenering betreft het 'Als X (onafhankelijke variabel) dan Y (afhankelijke variabel)'. In dezen ligt de redenering achter effectieve informatiebeveiliging complexer, het betreft als 'X1 EN X2 EN X3…(factoren t/m 7)…dan Y (veiligere informatie)'. Vanwege de complexe redenering en de deductieve aard is er voor een enkelgevalstudie gekozen. Met een enkel geval studie is het mogelijk om de diverse factoren te doorgronden om zo tot een beter begrip te komen van de maatschappelijke vraagstukken (Babbie, 2010). Daarbij is er gekozen voor een longitudinaal element in de vorm van een retroperspectief onderzoek. De mate van uiting van de factoren voor informatiebeveiliging hangt af van gebeurtenissen bij de DUO in het recente verleden 2010-2015. Hierbij is het interessant om na te gaan of er bepaalde ontwikkelingen of veranderingen bij de onderzoekseenheid (DUO) hebben plaatsgevonden (Thiel, 2015, p. 70).

3.2 Selectie van de casus

Yin (2009) maakt onderscheid in vijf typen van casussen betreffende gevalstudies. De typologie *Critical Case*" sluit het meest aan bij de vraagstelling in dit onderzoek. De beschrijving hierover betreft het volgende: het gebruik van een ontwikkelde theorie om zodoende meer inzicht te krijgen over de omstandigheden waarin de hypothese wel of niet blijft staan. Een beschrijving van een *Critical Case* bevat een situatie, vertaald in een casus, waarin de verwachte situatie zich voordoet. Vanwege de eerder benoemde complexiteit van de lastige meetbaarhed van veiligheid, is het van belang om uit te gaan van een situatie waar niet is voldaan aan een adequate borging van vertrouwelijke gegevens.

Het wetenschappelijke uitgangspunt voor de casus in deze masterscripte is dat de aanwezige situatie onveilig is en niet voldoet aan het volgende uitgangspunt; als is voldaan aan de zeven factoren dan is er een informatiebeveiligingssysteem conform de *State of the art* dan is de informatiebeveiliging effectief. De casus is gekozen om de geselecteerde factoren te kunnen gebruiken voor een analyse en om te kijken in hoeverre deze in de praktijk tot uiting komen. De casus (DUO) betreft een publieke instelling, met publieke taken en vertrouwelijke gegevens; DUO heeft te maken met informatiebeveiligingsincidenten. Hiermee is DUO geschikt als casus binnen de maatschappelijke relevantie van deze masterscriptie; het publieke domein én het gebruik van persoonsgegevens van zowel Nederlandse burgers als buitenlandse nationaliteiten. De specifieke casus is de organisatie van informatiebeveiliging na het incident van 9 november 2010 bij, onderzoekseenheid van deze masterscriptie, de DUO. Het incident is het uitganspunt; waarmee het

uitgangspunt in deze masterscriptie is dat op een specifiek moment niet is voldaan aan adequate borging van vertrouwelijke informatie. Daarnaast krijgt DUO sinds 2011 extra aandacht van de Algemene Rekenkamer op dit gebied. Hierdoor is er publieke informatie beschikbaar over de informatiebeveiliging bij de DUO. Dit maakt de casus geschikt als onderzoekseenheid; openbare bronnen zijn bescihkbaar voor het doen van een documentanalyse waarmee het fenomeen informatiebeveiliging beter begrepen kan worden.

3.3 Dataverzameling en -analyse

Vanwege de keuze voor een casestudy met als benadering 'retroperspectief onderzoek', is er gekozen voor twee typen van data-analyse:

- *Documentanalyse*
- *Semigestructureerde expertinterviews.*

De keuze van deze twee typen is gebaseerd op de tijdsdimensie in dit onderzoek (Thiel, 2015, p. 70).

3.3.1 Documentanalyse

Voor de documentanalyse is bestaand materiaal gebruikt. *'Deze strategie is vooral geschikt voor historisch onderzoek, bijvoorbeeld om een ontwikkeling over de tijd te kunnen beschrijven of om de achtergronden (context) van een onderzoeksprobleem te leren kennen.' (Thiel, 2015, p. 128).* Normaliter zijn de belangrijkste voordelen van een documentanalyse dat er veel materiaal beschikbaar is, en dat het onderzoek efficiënter uit te voeren is (Babbie, 2010; Thiel, 2015). Hoewel de benoemde voordelen meespelen, is het belangrijkste voordeel dat zonder het gebruik van secundaire documentatie analyse niet mogelijk is. Dit komt doordat het vanwege vertrouwelijkheid niet mogelijk is om te observeren en primair materiaal te verzamelen. Deze documenten bevatten samengevatte conclusies over audits op het gebied van informatiebeveiliging. Tevens zijn de audits *an sich* niet beschikbaar.

Bij het gebruik van een documentanalyse zijn twee kanttekeningen te identificeren. Ten eerste *'…bestaand materiaal is voor een ander doel geproduceerd dan het onderzoek waarvoor de bestuurskundige onderzoeker het wil gebruiken. Daardoor sluit de informatie niet altijd aan op de onderzoeksvragen'* (Thiel, 2015, p. 127). Ten tweede heeft secundair materiaal een beperkte betrouwbaarheid, doordat het de vraag is of de inhoud van de documenten voldoende overeenkomt met de werkelijkheid (Babbie, 2010, p. 348). Hierbij is in de analyse rekening gehouden met de problematiek rondom onderzoek naar beleidsmaatregelen die leiden tot maximale veiligheid en minimale schade. Om de analyse in goede banen te leiden, is informatiebeveiliging bij DUO geanalyseerd op basis van een vooraf bepaald (deductief) coderingstabel. Bij het coderen is in de hoofdcode rekening gehouden met of de factor benoemd wordt in het formele document. Indien deze aanwezig is, wordt het oordeel over de tactische toepassing van de factor bij de DUO meegecodeerd middels een subcode. Daarnaast is er eenzelfde soort codetabel voor de elementen uit het normenkader (plan, do, check, act). Vooraf zijn de bestaande beleidsdocumenten voor de documentanalyse geselecteerd (zie Bijlage 4), waarbij er rekening is gehouden met de vergelijkbaarheid door voor ieder jaar gelijksoortige documenten te gebruiken zoals de jaarlijkse

verantwoordingsrapporten. Voor het coderen is gebruik gemaakt van het analyseprogramma voor kwalitatieve tekstanalyse MAXQDA 12 (Release 12.1.4, Build 160601).

3.3.2 Semigestructureerde expertinterviews

Het doel van semigestructureerde interviews is een verdere verdieping van de documentanalyse. Het gaat niet om het al dan niet verifiëren van de documentanalyse (immers beleidsdocumenten zijn opgesteld), wel om de toevoeging van expertkennis. *'In deductief onderzoek worden de interviewvragen afgeleid uit de operationalisatie van de variabelen uit het theoretisch kader (maar let op, vermijd jargon)' (Thiel, 2015, p. 115).* De vragen bieden een leidraad voor een open gesprek met de expert, waarbij ten minste alle factoren ter sprake komen en er gevraagd wordt naar trends en gebreken op het gebied van informatiebeveiliging. De verwerking van de interviews is gedaan middels een verslag. Dit verslag bevat een samenvatting van het gesprek vanuit de interpretatie van de onderzoeker over wat de expert heeft gezegd (Thiel, 2015, p. 119). Daarbij is het verslag per e-mail naar de respondent verzonden met het verzoek tot verificatie van de inhoud. Deze vorm van interviewen is bewust gekozen. Het onderwerp leent zich ertoe dat bepaalde informatie ter tafel kan komen die vertrouwelijk is, dit heeft tevens te maken met de kennis en achtergrond van de onderzoeker. Een gesprek opnemen voor het transcriberen, kan een barrière vormen voor de openheid in het gesprek, waardoor er mogelijk vanwege voorzichtigheid minder informatie gedeeld wordt. Er is gekozen voor interviews met 5 experts, die vanuit hun positie meer inzicht en overzicht kunnen verschaffen over de organisatie van informatiebeveiliging bij de DUO. De interviews met deze experts verschaffen voldoende informatie om de centrale onderzoeksvraag te kunnen beantwoorden.

3.4 Betrouwbaarheid en validiteit

Om de betrouwbaarheid te bewaken bij een deductieve benadering is een vooraf gestructureerde aanpak van belang. Het onderzoek is gebaseerd op theorieën en modellen waarin is bepaald welke beveiligingsmaatregelen effectief zijn. Hierdoor heeft de aanpak invloed op de interpretatie van de onderzoeker. Tevens zijn de te analyseren factoren vooraf ontwikkeld door de onderzoeker zelf. Om de beoordeling op basis van dit model in goede banen te leiden zijn de aspecten uit het model geanalyseerd, op basis van een codesysteem, middels een contentanalyse van de kwalitatieve data. Hiermee is de ruimte tot interpretatie enigszins ingeperkt en verhoogd het de reproduceerbaarheid van de analyse. De validiteit is geborgd door in eerste instantie formele documenten als basis te gebruiken. Verder zijn de interviews digitaal vastgelegd, waardoor de interne validiteit en betrouwbaarheid worden vergroot, deze zijn daarbij achteraf geverifieerd bij de respondent. Het onderzoek kan hierdoor worden gecontroleerd en de transparantie is groot.

3.5 Operationalisering

In deze paragraaf is de operationalisering in een tabel weergegeven. De toelichting per geformuleerde indicator is te vinden in de Bijlage 3. Tevens bevat deze coderingstabel een verdere verdieping op het onderstaande operationaliseringstabel. In onderstaande tabel is per factor een aantal indicatoren opgenomen. In de tabel is 'gebruikers' genoemd. De gebruiker is zowel de eindgebruiker, de gebruiker die input levert, de beheerder als de ontwikkelaar van de toepassing.

Tabel 10 Operationalisatie tabel

Factoren	Indicatoren	Gegevensbron
Strategie	*Overzicht van alle noodzakelijke functionaliteiten* *Overzicht van alle IT-systemen* *Overzicht van alle locaties met dataopslag*	Formele beleidstukken
Beleid	*Risicoanalyse* *Adequaat informatiebeveiligingsbeleid*	Formele beleidstukken
Gebruiksbeheer	*Bewustwordingsactiviteiten* *Ondersteuning voor gebruikers* *Gebruikers zijn periodiek betrokken bij wijzigingen*	Formele beleidstukken, semigestructureerde interviews met experts
Gegevensbeheer	*Centraal informatiebeveiligingsbeheer* *Monitoring gegevens kwaliteit* *Autorisatiebeheer* *Audittrail*	Formele beleidstukken
Ruimte, apparatuur en systemen	*Periodieke technische testen* *Periodieke updates* *Gelaagde systeemopbouw* *Controle en toezicht mobiele gegevensdragers en middelen die autorisatie tot gegevensdragers verschaffen*	Formele beleidstukken
Incidentmanagement	*Incidentenplan* *Periodieke incidentenoefening*	Formele beleidstukken, semigestructureerde interviews met experts
Compliance	*Kader en/of richtlijn* *Periodieke controle*	Formele beleidstukken, semigestructureerde interviews met experts
Informatiebeveiligings-systeem	*Beheersingsmaatregel ten behoeve van 'Plan'* *Beheersingsmaatregel ten behoeve van 'Do'* *Beheersingsmaatregel ten behoeve van 'Check'* *Beheersingsmaatregel ten behoeve van 'Act'* *Beheersingsmaatregel ten behoeve toepassing van een informatiebeveiligingssyteem*	

4. Resultaten

In dit hoofdstuk zijn de belangrijkste resultaten van de dataverzameling en –analyse opgenomen. De uitkomsten van de documentanalyse zijn opgenomen in de resultatentabel die is opgenomen in Bijlage 1. Allereerst is in hoofdstuk 4.1 een korte beschrijving van de casus 'DUO & Informatiebeveiliging in beeld' beschreven. Vervolgens zijn de resultaten van de documentanalyse en interviews beschreven vanuit de, voor dit onderzoek, gehanteerde zeven factoren voor de organisatie van informatiebeveiliging. Ten slotte is in hoofdstuk 4.3 de toepassing van een informatiebeveiligingssysteem beschreven alsook in hoeverre alle factoren hierbinnen tot uiting komen bij de DUO.

4.1 Casus: DUO & Informatiebeveiliging in beeld

4.1.1 Beschrijving van de organisatie

De DUO is een baten-lastendienst (voormalig agentschap) van het Ministerie van OCW. Dit betekent dat de DUO namens het OCW haar taken mag uitvoeren. Hiermee zijn zij een zelfstandig organisatieonderdeel. Het OCW is wel eindverantwoordelijk voor de DUO.

"De hoofdtaken van de DUO zijn:

- Bekostigen van onderwijsinstellingen;
- Verstrekken van studiefinanciering en tegemoetkoming schoolkosten;
- Innen van lesgelden en studieschulden;
- Erkennen van diploma's, beheren Diplomabank;
- Organiseren van school-, staats- en inburgeringsexamens;
- Verzorgen van proces van aanmelding, selectie en plaatsing hoger onderwijs;
- Verzamelen en beheren van onderwijsgegevens in diverse registraties;
- Verrijken van onderwijsgegevens tot informatieproducten;
- Fungeren als Nationaal Europass Centrum Nederland;
- Verzamelen en beheren van gegevens in het landelijk register kinderopvang en peuterspeelzalen." (Rijksoverheid, 2016)

Vanuit het interview met de IT-Audit coördinator OCW/ADR is de '*governance'* als volgt beschreven. De DUO is opgedeeld in twee locaties; enerzijds is er in Groningen het beheer van de gegevens van studenten en studiefinanciering, anderzijds vindt in Zoetermeer de bekostiging van de instellingen plaats.

De centrale regiegroep BIR/OCW is sinds 2012 vanuit het ministerie van OCW actief. Deze regiegroep komt maandelijks samen en representeert alle verschillende dienstonderdelen van het OCW (waaronder de DUO). Het doel van de regiegroep betreft het toetsen en begeleiden van de implementatie van de BIR. De regiegroep is een commissie die ondersteunend is aan de secretaris-generaal en de regiegroep heeft de bevoegdheid om daar waar nodig lijnmanagers aan te spreken ter verbetering van de compliance op de BIR.

Naast de toetsing op de BIR vindt, bij het OCW, toetsing plaats van de op 1 januari 2016 in werking getreden Wet Meldplicht Datalekken. Binnen deze wet speelt informatiebeveiliging een prominente rol.

Voor het gedeelte auditing van de organisatie van informatiebeveiliging bij de DUO wordt gebruikgemaakt van ADR-Cluster regio Noord-Nederland. De Chief Information Officer (CIO) is gesitueerd te Groningen. Eveneens is er een functionaris gegevensbeheer en er zijn diverse privacy officers. Zij zijn voornamelijk gericht op de naleving van de Wet Bescherming Persoonsgegevens.

4.1.2 Regulering & incidenten

Vanaf 2012 is de BIR leidend als regulering van de organisatie van informatiebeveiliging binnen de Rijksoverheid; en daarmee eveneens leidend voor de DUO. De BIR is een samenstelling van een vijftal (voormalige) richtlijnen en is gebaseerd op de NEN-ISO/IEC 27001 en 27002. In 2013 is de, op 1 januari 2016, ingetreden Wet meldplicht datalekken en meldplicht ICT-inbreuken door de voormalige minister van Veiligheid en Justitie aangekondigd. Volgens de respondenten was voornamelijk het Besluit voorschrift informatiebeveiliging rijksdienst 2007 (VIR 2007) leidend, voor het nemen van maateregelen aangaande informatiebeveiliging, alvorens de intreding van de BIR.

De wet- en regelgeving is vlak na de grotere incidenten Diginotar en Lektober tot stand gekomen. Diginotar was de certificatenverlener, waarbij het mogelijk werd om valse certificaten te genereren. Als gevolg was het voor hackers mogelijk om willekeurige certificaten te genereren, waardoor het in de browser lijkt of de pagina te vertrouwen is. Tegelijkertijd konden er persoonsgegevens gestolen worden. Tijdens Lektober werd opgeroepen om lekken te melden bij de website Webwereld.nl. In oktober 2011 werd pijnlijk duidelijk hoe 'lek' Nederland was. Het incident/lek dat als startpunt is genomen in dit onderzoek was van een jaar daarvoor, november 2010. In de nieuwsberichten zijn de volgende drie incidenten en storingen bij de DUO waargenomen: In 2010 konden studenten in hun eigen omgeving gegevens zien van andere studenten (Schellevis, 2010). In 2011 is er een groep hackers geweest die een lek op de website heeft gevonden ("Hacker ontdekt gat in website DUO," 2011). Én in 2013 is de website een week uit de lucht geweest vanwege een storing bij KPN (Digitaal Universiteitsblad UU, 2013). In geen


08 november 2010 21:39

Studiegegevens op straat door fout

Studenten kregen dit weekend ongevraagd privacy-gevoelige informatie van anderen te zien als ze inlogden op de site van DUO, de voormalige IB-groep.

Door een fout in het computersysteem van de Dienst Uitvoering Onderwijs kregen mensen die met hun eigen code op de site inlogden, de gegevens van iemand anders te zien.

"RTL Nieuws (2010)"

Overheidsorganisatie laat privégegevens studenten uitlekken

Door Joost Schellevis, dinsdag 9 november 2010 09:10, 67 reacties • Feedback

De Dienst Uitvoering Onderwijs heeft persoonlijke gegevens van studenten laten uitlekken. Gebruikers die via DigiD inlogden op de DUO-website, konden gegevens van anderen te zien krijgen. Het lek zou in enkele gevallen zijn voorgekomen.

"Tweakers (2010)"

07 juni 2011 16:44

Hacker ontdekt gat in website DUO

Voor de tweede keer zat er een lek in de website van de Dienst Uitvoering Onderwijs (DUO), de oude IB-Groep. Criminelen konden via de site DigiD-gegevens stelen of mensen geld afhandig maken. RTL Nieuws kwam het lek op het spoor na een tip van een hacker.

"RTL Nieuws (2011)"

DUO waarschijnlijk morgen weer online

dinsdag 5 november 2013 – 11:50

Vanaf morgen kunnen studenten weer inloggen bij de Dienst Uitvoering Onderwijs. Althans, daar lijkt het op. Volgens KPN is de storing voorbij, maar DUO wil niet te vroeg juichen.

"Digitaal Universiteitsblad UU (2013)"

Figuur 2 Overzicht nieuwskoppen incidenten DUO

van de gevallen is daadwerkelijk (opzettelijk) misbruik onderkend. De respondenten geven aan dat zowel regulering, het oordeel van de Algemene Rekenkamer als incidenten redenen zijn waardoor de aandacht voor informatiebeveiligingsmaatregelen intensiveert.

4.2 De mate van uiting van de zeven factoren bij de DUO

Bij de analyse van de uiting van de zeven factoren voor de organisatie van informatiebeveiliging, is in het onderzoeksmateriaal onderscheid gemaakt tussen de interviews, documenten met betrekking tot verantwoording en controle, het OCW-informatiebeveiligingsbeleid 2014 en de VIR 2007. Hiermee worden de beleidsdocumenten los gezien van de documenten met betrekking tot verantwoording en controle. Beleidsdocumenten geven aan wat de bedoeling is en zeggen weinig over de daadwerkelijke invulling en uitvoering van informatiebeveiliging. Verantwoordings- en controledocumenten stellen een oordeel over de staat van de organisatie ten aanzien van informatiebeveiliging; de nadruk ligt voornamelijk op de onvolkomenheden. De VIR 2007 betrof het uitgangspunt voor de invulling van informatiebeveiliging voor de BIR.

De beleidsdocumenten en interviews zijn aanvullend materiaal waarmee een vollediger beeld ontstaat, waaronder voor de factoren die in mindere mate aangetroffen zijn in de verantwoordings- en controledocumenten. Tevens is er onderscheid gemaakt tussen de aanwezigheid van factoren en de toepassing van factoren. Daarbij dient opgemerkt te worden dat de oordelen die zijn aangetroffen, voor enkel van een deel van de organisatie gelden. Een voorbeeld hiervan is het oordeel over de risicoanalyse; deze is niet toegepast. Dit betekent niet dat er, wellicht, nergens een risicoanalyse is toegepast; voor de specifieke, onderzochte organisatieonderdelen ontbreekt een risicoanalyse. Het komt dus voor dat in de verschillende documenten uit hetzelfde jaar soms tegenstrijdige oordelen zijn gegeven. De resultaten van de analyse over de mate van uiting van de zeven factoren voor de organisatie van informatiebeveiliging bij de DUO geeft dus niet de mate van de daadwerkelijke aanwezigheid in de dagelijkse praktijk aan. De resultaten zijn gericht op de verdeling van en aandacht voor de factoren binnen de geanalyseerde documenten. Met deze aandacht kan een beeld geschetst worden over de uiting van de zeven factoren bij de DUO in de periode van 2010-2015. In deze paragraaf is per factor beschreven in hoeverre deze tot uiting komen in de organisatie van informatiebeveiliging bij de DUO.

4.2.1 Strategie

De factor strategie is onderverdeeld in drie indicatoren: overzicht van alle noodzakelijke functionaliteiten, overzicht van alle IT-systemen en overzicht van alle locaties. Deze indicatoren zijn voornamelijk onderdeel van het vakgebied IT-architectuur en kunnen als basis dienen voor de risicoanalyse als onderdeel van de factor beleid.

De factor strategie is in de verantwoordings- en controledocumenten tweemaal in de documentgroep 2015, van de in totaal 192 aangetroffen duidingen, aangetroffen. In het document Staat van de Rijksverantwoording (Algemene Rekenkamer, 2015, p. 28) wordt hier aandacht aan geschonken:

> "Met name het vervangen van oude en onderling verweven ICT-systemen vereist een goede voorbereiding en daarbij behorende expertise, middelen en tijd. Daarbij zijn een langetermijnperspectief op het ICT-landschap (architectuur), een goed proces van portfoliomanagement en realistische business cases voor zowel vernieuwing als onderhoud van groot belang."(Idem)

Uit de interviews blijkt dat de factor strategie als volgt geuit wordt bij de DUO: Het toetsen van de BIR is opgedeeld in aandachtsgebieden. DUO adviseurs Control & Compliance stellen dat aan elk aandachtsgebied een lijnmanager is gekoppeld. IT-architectuur heeft geen koppeling met deze aandachtsgebieden. Op het niveau van de DUO is veel in kaart gebracht. Het architectuurprincipe is: 1 functie voor 1 applicatie. Vanwege de historie kan er dubbeling plaatsvinden. Dit wordt aangepast bij vernieuwingen. Soms wordt besloten om er anders mee om te gaan, dit moet dan uitgelegd worden door de verantwoordelijken. Iedere directie draagt zijn eigen verantwoordelijkheid. Verschillende directies hebben verschillende applicaties. Op directieniveau ontstaan er daardoor ook dubbelingen. Deze directies hebben vanwege historiciteit en verschillende behoeften verschillende inrichtingen van ICT.

De DUO maakt gebruik van een 'architectuur-wiki', hierin is een Enterprise-architectuur weergegeven. Dit bestaat uit een IST-situatie uit 2014, een SOLL-situatie en een Roadmap. De Roadmap dient als plan om tot de SOLL-situatie te komen. Bij het opstellen van een Enterprise-architectuur is er samenwerking met het Rijk. Tevens worden hier referentiearchitecturen gebruikt. Deze referentiearchitecturen worden ook gebruikt door de partijen waarmee de DUO samenwerkt. Referentiearchitecturen brengen uniformiteit met zicht mee, waardoor de samenwerking eveneens wordt verbeterd. De referentiearchitecturen die worden gebruikt zijn:

- **NORA:** "NORA is bedoeld als richtinggevend en sturend instrument. Het bevat kaders en bestaande afspraken voor het inrichten van de informatiehuishouding van de Nederlandse overheid. Het realiseren van voorzieningen binnen die kaders en afspraken zorgt ervoor dat ze goed samenwerken met andere voorzieningen en dat optimaal hergebruikgemaakt wordt van bestaande oplossingen"; (ICTU, 2016)

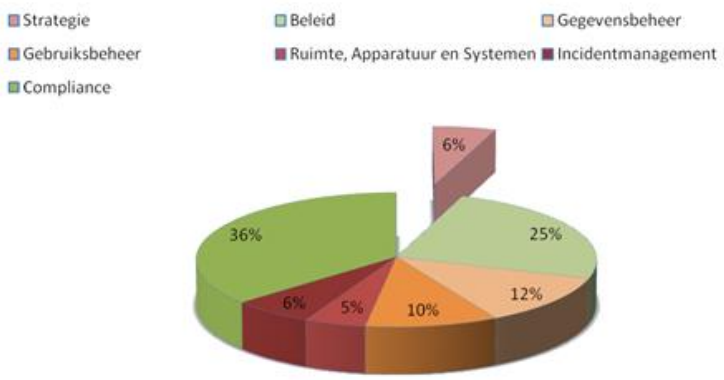
- **EAR:** "EAR biedt een samenhangende beschrijving van de organisatie en inrichting van de informatiediensten en -voorzieningen van de Rijksdienst. Het is een houvast voor iedereen die, vanuit de concerngedachte, stappen wil zetten om de samenwerking tussen en binnen delen van de Rijksdienst te verbeteren";(Rijksoverheid, n.d.)

- **ROSA:** "Vanuit deze ontwikkelingen kijkt ROSA als referentiearchitectuur voor het gehele onderwijsdomein over de grenzen van onderwijssectoren heen. ROSA weerspiegelt onderwijsbrede principes en afspraken die noodzakelijk zijn om de gewenste ambities te realiseren en de daarbij benodigde inrichting van de informatiehuishouding te ondersteunen. ROSA richt zich dan ook op vraagstukken die voortvloeien uit ketensamenwerking en op generieke, bovensectorale behoeften". (Bureau Edustandaard, 2016)

In de Enterprise-architectuur zijn hoofdstukken opgenomen voor strategische doelstellingen en informatiebeveiliging. De afdeling IT-supply wil proactief zijn en is daarom meer bezig met het plannen van datgene wat nodig is, en kijkt vervolgens of het voldoet aan de wet- en regelgeving. Informatiebeveiliging is onderdeel van de architectuur, maar is niet het hoofddoel. Er dient altijd een afweging gemaakt te worden tussen verdere inrichting van beveiliging en flexibiliteit. De DUO adviseur bij ICT-Supply geeft aan dat de CIO-office zich richt op samenwerking en een integrale aanpak. Ze zijn bijvoorbeeld bezig met ideeën over een Rijksportaal waarop de verschillende diensten van de gehele Rijksoverheid afgenomen kunnen worden. Daarbij kan de gebruiker actief geholpen worden door middel van tips en aandacht voor wat, al dan niet voor de specifieke klant, van toepassing is. Verder is er aandacht voor inzicht voor de gebruiker over wie en wanneer gegevens van de gebruiker raadpleegt of gebruikt. Momenteel loopt er een pilot met de KU Leuven. Hierop kan de Nederlandse student inloggen en kan de student zelf aanvinken of de KU Leuven zijn/haar gegevens mag ophalen bij de DUO. Hierbij bepaalt de student zelf de toegangsrechten van de universiteit.

Verder geeft de IT-Audit coördinator OCW/ADR aan dat de organisatie van infrastructuur en systemen is versnipperd. Dit komt volgens de coördinatoe doordat er sprake is van veel externe leveranciers die het netwerk in stand houden en de systemen onderhouden. Deze externe leveranciers worden geaudit. Externe leveranciers zijn in zekere mate door een verhoogde complexiteit een risico voor de informatiebeveiliging. Er wordt overgaan naar het publieke datacenter: ODC-noord. Dit is een beweging van het huidige versnipperde landschap naar centralisatie. Naar aanleiding van overleg tussen de CIO en de ADR bestaat de wens voor een BIR-compliancytoets van het ODC-noord, zodat meerdere publieke partijen gemakkelijk aan kunnen sluiten op het publieke datacenter. Het ODC-noord is eigendom van OCW. Er is een bepaalde mate van afhankelijkheid van de techniek dat door andere organisaties wordt ontwikkeld. Als blijkt dat de werking anders loopt dan verwacht, is dit een risico voor de keten waarin de DUO opereert. Om dit te beheersen worden er altijd systeemtesten en functionele testen uitgevoerd.

IT-architectuur is, met de bijbehorende Roadmaps, 10 tot 20 jaar aanwezig bij de DUO. De IT-architectuur is groeiende en wordt steeds meer de basis van de DUO, dat is volgens de DUO adviseur bij ICT-Supply ook de wens van de hoofddirectie. IT-architectuur groeit ook omdat het aantal systemen en applicaties in de jaren is toegenomen. De beste verbeteringen in de ontwikkeling van de IT-architectuur lijken, volgens de DUO adviseur bij ICT-Supply, vanaf 2010 plaats te vinden.



Figuur 3 Aandeel van de factor strategie in het OCW-informatiebeveiligingsbeleid 2014

In het informatiebeveiligingsbeleid van het OCW gaat 6 procent van de codering van alle factoren naar de factor strategie. Het onderwerp is zevenmaal, van de in totaal 126 aangetroffen duidingen, aangetroffen in het informatiebeveiligingsbeleid van het OCW en richtte zich voornamelijk op de indicatoren an sich die bij strategie behoren. De uiting van deze indicatoren is belegd in het taakgebied van de CIO:

> "CIO13: functioneert namens het MT OCW als opdrachtgever voor generieke ICT-voorzieningen voor OCW; ontwikkelt en onderhoudt de departementale architectuur en standaarden vanuit de rijksbreed afgesproken (informatiebeveiligings)kaders; bewaakt samenhang in informatievoorziening en ICT-projecten door applicatie- en projectenportfoliomanagement met daarin opgenomen een overzicht van informatiesystemen en hun eigenaars; vertaalt de beveiligingsnormen naar eisen aan de processen en systemen en controleert of projecten voldoen aan deze eisen; doet voorstellen voor de verbetering van de besturing van ICT binnen het ministerie; is bevoegd voorstellen over de start/bijsturing/opschorting van nieuwe ICT-projecten aan MT OCW; signaleert bij het voornemen om nieuwe informatiesystemen in productie te nemen het eventueel ontbreken van een risicoanalyse (en maatregelen) aan de lijnmanager en I-BVA;" (Ministerie van Onderwijs, 2014, p. 17)

4.2.2 Beleid

De factor beleid is onderverdeeld in twee indicatoren: risicoanalyse en een adequaat informatiebeveiligingsbeleid. Adequaat informatiebeveiligingsbeleid bevat minimaal:

- De strategische uitgangspunten en randvoorwaarden die de organisatie hanteert ten aanzien van informatiebeveiliging, waaronder de inbedding van in- en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid;
- Het doel van het informatiebeveiligingsbeleid;
- De organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden;
- De toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers;
- De gemeenschappelijke betrouwbaarheidseisen en -normen die voor de organisatie van toepassing zijn;
- De frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd;
- De bevordering van het beveiligingsbewustzijn (Kwaliteitsinstituut Nederlandse Gemeenten, 2013).

Uit de documentanalyse blijkt dat na compliance de meeste aandacht uitgaat naar beleid. Van de in totaal 91 aangetroffen duidingen zijn er 55 gericht op de risicoanalyse, 22 op adequaat informatiebeveiligingsbeleid en 14 op de factor beleid in zijn algemeenheid (zie Bijlage 1). Zowel in de verantwoordings- en controledocumenten als vanuit de interviews is er in de periode 2010-2015

een bepaalde mate van aandacht voor de factor beleid waargenomen. Er is in de verantwoordings- en controledocumenten in mindere mate aandacht voor de factor beleid in 2011 en 2012. De invoering van de BIR lijkt hierop van invloed te zijn geweest:

> "In afwachting van besluitvorming over nieuwe regelgeving op het gebied van informatiebeveiliging, de Baseline Informatiebeveiliging Rijksdienst (BIR), is het informatiebeveiligingsbeleid in 2012 niet geëvalueerd en aangepast door de DUO. De BIR is in september 2012 vastgesteld". (Algemene Rekenkamer, 2012b)

Van 2010 tot en met 2013 wordt de factor beleid 22 maal van de 58 duidingen niet of deels toegepast. Vervolgens is in de jaren 2014 en 2015 van de factor beleid het onderdeel risicoanalyse in 2014 een enkele keer aangemerkt als deels toegepast. In 2010 werd door het OCW en de Algemene Rekenkamer beschreven dat er bij een aantal organisatieonderdelen geen risicoanalyse is toegepast (Algemene Rekenkamer, 2010; Ministerie van Onderwijs, 2010). De Algemene Rekenkamer rappelleert hierover in 2011 en 2012. De IT-Audit coördinator OCW/ADR geeft aan dat sturen op risicoanalyses een belangrijk aandachtspunt is vanuit de ADR. Daarbij voorziet de IT-Audit coördinator OCW/ADR persoonlijk dat informatiebeveiligingsmaatregelen georganiseerd zouden kunnen worden op basis van geïdentificeerde risico's. Daarmee betreft het niet zozeer de beheersing richten op de volledige BIR, maar de beheersing concentreren op de risico's.

Uit de interviews blijkt dat het informatiebeveiligingsbeleid van het OCW dateert van 2007 en 2014. In de tussentijd is er geen ander beleid geweest. In het verlengde van het informatiebeveiligingsbeleid van OCW heeft de DUO aanvullend een addendum informatiebeveiliging 2014-2017. Deze is een aantal malen gewijzigd, met de laatste wijziging in 2015. Voorafgaand van de BIR was de VIR 2007 van kracht (deze is nog steeds in werking). Destijds was er geen specifiek beleid, de VIR 2007 werd als richtlijn aangehouden. DUO adviseurs Control & Compliance geven aan dat er, voordat de BIR werd geïmplementeerd, veel was georganiseerd op het gebied van informatiebeveiliging. Er bestaat echter een vertekend beeld, omdat pas in 2009 de DUO is ontstaan vanuit een fusie met de IB-groep en Centrale Financiën Instellingen (CFI) als voormalig Zelfstandige Bestuursorganen (ZBO). Als ZBO hoefde de organisatie niet het OCW-beleid te volgen. Na de fusie liep de DUO als nieuwe organisatie achter bij het opstellen van beleid en regelgeving conform die van OCW. Er was organisatie omtrent informatiebeveiliging; deze organisatie was echter anders georganiseerd dan bij het OCW. Hierdoor voldeden de richtlijnen van voor de fusieorganisatie niet aan dezelfde richtlijnen waaraan het OCW moest voldoen. Vanwege het hoge aantal persoonsgegevens waar de DUO over beschikt, is er veel aandacht voor privacy en fraude. Destijds werden dezelfde typen activiteiten als na de implementatie van de BIR uitgevoerd, deze waren minder gelieerd aan de normatiek op het gebied van informatiebeveiliging. Daarbij was het niet duidelijk genoeg wie waarvoor verantwoordelijk was. Het informatiebeveiligingsbeleid uit 2014 van OCW is inherent onderdeel van de factor beleid.

4.2.3 Gebruiksbeheer

De factor gebruiksbeheer is onderverdeeld in drie componenten: bewustwordingsactiviteiten, ondersteuning voor gebruikers en periodieke betrokkenheid van gebruikers bij wijzigingen. In de onderzochte documentatie over de toepassing van informatiebeveiligingsmaatregelen is waar te nemen dat er op dit vlak vooral aandacht is voor bewustwordingsactiviteiten. De DUO heeft een eigen bedrijfsschool, die verantwoording voor bewustwording neemt. Alle nieuwe medewerkers krijgen training en voorlichting over informatiebeveiliging. Externe medewerkers op de stafafdeling krijgen dit niet altijd. In totaal krijgt elke medewerker een uur aan bewustwordingsactiviteiten per jaar.

In de verantwoordings- en controledocumenten komt de indicator 'ondersteuning voor gebruikers' vanaf 2012 aan bod. Er is ondersteuning voor gebruikers in de vorm van een helpdesk. Hier kunnen ook de incidenten gemeld worden. Deze helpdesk bevat medewerkers van de DUO en is niet op afstand geplaatst. Verder vindt ondersteuning plaats in de vorm van handleidingen, instructies en procedures. Gebruikers bij de DUO zijn te onderscheiden in de interne en de externe gebruiker. Voor de DUO is ondersteuning van externe gebruikers belangrijk:

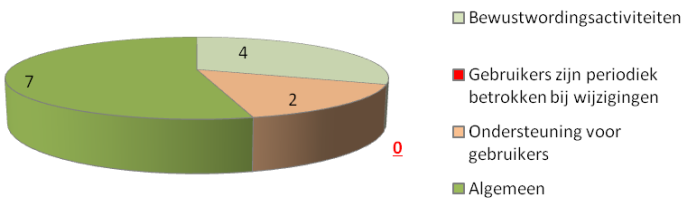
> "Betrouwbare informatievoorziening en goede dienstverlening aan onderwijsinstellingen en onderwijsdeelnemers staan centraal in het dagelijks werk van de Dienst Uitvoering Onderwijs (DUO). Daarnaast is de DUO continu bezig met het verbeteren en vernieuwen van de dienstverlening, om te kunnen blijven voldoen aan de steeds hogere eisen die de gebruikers stellen aan de toegankelijkheid, betrouwbaarheid en actualiteit van informatie." (Ministerie van Onderwijs, 2013, p. 16)

De DUO adviseur bij ICT-Supply geeft aan dat de DUO erop is gericht om klanten zoveel als mogelijk digitaal te bedienen. Hier wordt rekening gehouden met minderheden die er digitaal niet uitkomen. Voor deze doelgroep (de zogenoemde digibeten) blijft de fysieke servicedesk en de telefooncentrale bestaan. Doordat bij de fysieke servicedesk en telefooncentrale minder vragen binnenkomen en het vaak specifieke vragen betreffen van een kleinere groep mensen, lijkt deze helpdesk de klant beter te bedienen.

Vanuit de BIR wordt niet getoetst in hoeverre de gebruikers het gebruik hanteerbaar vinden. DUO adviseurs Control & Compliance geven aan dat het een uitdaging is om de vele handvatten die beschikbaar zijn te laten landen bij de eindgebruikers. Deze worden, tussen alle overige informatie, veelal niet gelezen ofwel opgemerkt. De IT-Audit coördinator OCW/ADR neemt een mate van digitale weerstand waar. Daarbij stelt hij dat er door bezuinigingen minder capaciteit is om met systemen te (leren) werken. Verder is er sprake van vergrijzing op de werkvloer en is er sprake van medewerkers die afkerig zijn van vernieuwing. Op termijn is het door de IT-Audit coördinator OCW/ADR als struikelblok voorzien, maar nu nog niet. De weerstand en moeilijkheden zijn volgens de coördinator waar te nemen via kleine incidenten; er is geen sprake van grote incidenten.

In de documentatie die gebruikt is voor de analyse is nergens sprake van het periodiek betrekken van gebruikers bij wijzigingen in systemen en applicaties. Dit laatste krijgt in de praktijk voornamelijk vorm via key-usergroepen of gebruikerstesten. DUO adviseurs Control & Compliance geven in het interview aan dat er wel sprake is van panelgroepen en key-usergroepen, maar dat zij hier vanuit de compliancy met de BIR niet betrokken bij zijn. De DUO adviseur bij ICT-Supply geeft aan dat de eindgebruikers worden betrokken bij de testen. Er wordt veel getest met gebruikers. De DUO voert systeemtesten, functionele testen, schaduwtesten en gebruikerstesten uit. Voor het testen bestaan er ontwikkelstraten, deze bestaan uit verschillende testomgevingen waarin de testen plaatsvinden. De reguliere interne gebruiker werkt in de productieomgeving.

De indicator 'ondersteuning voor gebruikers' is in mindere mate onderdeel van de bedrijfsvoering rondom informatiebeveiliging en des te meer onderdeel van fraudebestrijding en de werking van de ICT. Fraude is belegd bij de afdeling handhaven en inspectie. Hier is er een verschil tussen fraude in het apparaat en fraude in het programma. Van apparaatfraude is sprake wanneer medewerkers intern frauderen of dat er bijvoorbeeld gefraudeerd wordt met de jaarrekening. Van programmafraude is sprake wanneer het geld voor instellingen en/of studenten (on)opzettelijk niet op de juiste plek terechtkomt. Dit is op een andere afdeling georganiseerd. De BIR wordt wel over de gehele organisatie getoetst. In het OCW-informatiebeveiligingsbeleid is er van de 10% die is besteed aan de factor gebruiksbeheer voornamelijk aandacht voor beveiligingsbewustwording. De aandacht voor de factor gebruiksbeheer is binnen de DUO aanwezig, in het informatiebeveiligingsbeleid van het OCW is deze abstracter beschreven. "De klassieke informatiebeveiligingsaanpak waarbij inperking van de mogelijkheden de boventoon voert, maakt plaats voor veilig faciliteren" (Ministerie van Onderwijs, 2014, p. 9).



Figuur 4 Verdeling factor gebruiksbeheer in het OCW-informatiebeveiligingsbeleid 2014

4.2.4 Gegevensbeheer

De factor gegevensbeheer is onderverdeeld in de volgende indicatoren: centraal informatiebeveiligingsbeheer, monitoring gegevenskwaliteit, autorisatiebeheer en audittrail. Net als bij de factor beleid is er vanuit de documentanalyse een stagnatie van aandacht voor gegevensbeheer zichtbaar in 2011 en 2012. Tot 2013 is er nog enige vorm van kritiek op de toepassing van centraal informatiebeveiligingsbeheer, monitoring gegevenskwaliteit en autorisatiebeheer. Voor audittrail, ook wel bekend als logging, is in de verantwoordings- en controledocumenten geen enkele aandacht.

DUO adviseurs Control & Compliance geven aan dat er bij de DUO centraal functioneel beheer is ingericht. Daarbij geven de DUO adviseurs Control & Compliance aan dat er een AO-systeem is

(Mavim). Hierin is een volledig gestructureerd overzicht van alle procedures en betrokken functies opgenomen. Het voordeel van Mavim is dat als er een functie wegvalt, te zien is op welke procedures dit betrekking heeft. Dit biedt een eenduidig beeld. Kritiek die vanuit de documentanalyse is waargenomen, richt zich niet op centraal functioneel beheer *an sich*; het richt vooral op een centrale en overzichtelijke organisatie middels verantwoordelijkheden, om zo het geheel te kunnen beheren.

Het monitoren van gegevenskwaliteit betreft monitoring en rapportage over de kwaliteit van data. Denk hierbij aan: dubbele opslag, juistheid van gegevens, verkeerde opslag en onjuiste classificaties. De IT-Audit coördinator OCW/ADR geeft aan dat de DUO vooral te maken heeft met risico's die naar buiten zijn gericht via webservices. Er is intern geen sprake van vertrouwelijke documenten, zoals de classificatie departementeel vertrouwelijk en staatsgeheim. Vertrouwelijke gegevens bij de DUO betreffen voornamelijk persoonsgegevens. Persoonsgegevens worden gecontroleerd op juistheid via controles op externe fraude, aldus de IT-Audit coördinator OCW/ADR. Deze controles zijn handmatig en geautomatiseerd gebaseerd op vooraf vastgestelde patronen (ook middels queries). Vanuit de documentanalyse is voornamelijk aandacht voor het belang van de controle van de kwaliteit van gegevens. Deze aandacht is gericht op de beschikbaarheid, integriteit en vertrouwelijkheid.

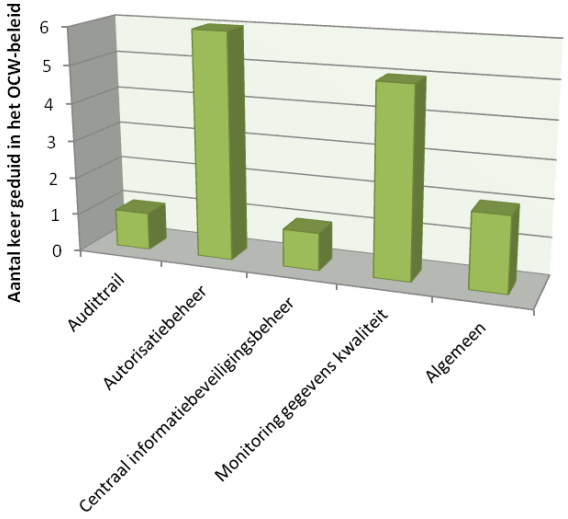
Autorisatiebeheer is de basiscomponent van informatiebeveiliging. In de resultatentabel (Bijlage 1) is te zien dat hier binnen de geanalyseerde documenten weinig aandacht voor is. In 2010 en 2011 is enkele kritiek op de logische[3] toepassing van autorisatiebeheer waargenomen. In het document 'Achtergronddocument Informatiebeveiliging en vertrouwensfuncties' (Algemene Rekenkamer, 2011b, p. 19) is benoemd dat toegangsbeveiliging voor verbetering vatbaar is. In 2010 is er een melding uitgelicht die duidt op onzorgvuldigheid:

"Voor drie personen stonden aanvragen van het Bureau BVA voor het uitvoeren van een veiligheidsonderzoek uit bij de AIVD, terwijl de betrokkenen al waren belast met de uitoefening van een vertrouwensfunctie." (Algemene Rekenkamer, 2010, p. 10).

DUO adviseurs Control & Compliance geven aan dat autorisatiebeheer als volgt georganiseerd is: logische toegang is via het toekennen van profielen aan medewerkers georganiseerd. De manager bepaalt welk profiel past bij de medewerker en speelt dit door naar de senior user. Daarbij krijgt de beheerder een melding als een persoon te veel rechten krijgt die niet samengaan. Hierop vindt een geautomatiseerde controle plaats. Iedere maand krijgt de desbetreffende manager een overzicht van de rechten/profielen per medewerker; hiermee wordt de juistheid gecontroleerd. De manager heeft niet altijd voldoende kennis van de achtergronden van systemen en applicaties. De senior user speelt hierin een belangrijke rol.

[3] Logische duidt op niet fysieke toegang

Over audittrail, ofwel logging, is niet geschreven in de documenten die zijn gebruikt voor de documentanalyse. Dit betekent niet dat er geen sprake van is. DUO adviseurs Control & Compliance geven het volgende aan over de audittrail. Alle handelingen van gebruikers worden gelogd, zo ook het raadplegen van Suwinet (externe applicatie met persoonsgegevens). Dit helpt onder andere bij het ontdekken van (interne) fraude. Tevens wordt het bekijken van atypische sites gelogd (goksites e.d.). Daarbij is er een zware spamfilter in werking. Hoewel de factor gegevensbeheer niet altijd de aandacht krijgt in de documentanalyse, is dit een factor die tot uiting komt bij de DUO. Ook in het OCW-informatiebeveiligingsbeleid is hier aandacht voor. Het valt op dat de indicatoren centraal informatiebeveiligingsbeheer en monitoring gegevenskwaliteit net als in de verantwoordings- en controledocumenten meer genoemd worden dan autorisatiebeheer en audittrail.



Figuur 5 Verdeling factor gegevensbeheer in het informatiebeveiligingsbeleid

4.2.5 Ruimten, apparatuur en systemen

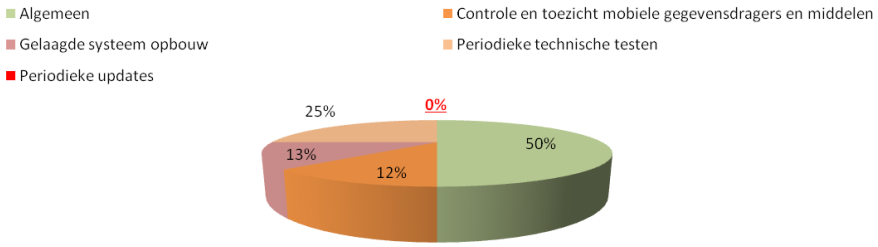
De factor ruimten, apparatuur en systemen is onderverdeeld in de indicatoren: periodieke technische testen, periodieke updates, gelaagde systeemopbouw, inzicht in welke apparaten er zijn en welke wanneer door wie in gebruik zijn, controle en toezicht mobiele gegevensdragers en middelen. In de verantwoordings- en controledocumenten uit de documentanalyse wordt vanaf 2013 in bepaalde mate aandacht geschonken aan dit onderwerp. Er is geen enkele aandacht voor de indicatoren: gelaagde systeemopbouw, inzicht in welke apparaten er zijn én welke wanneer door wie in gebruik zijn en controle en toezicht mobiele gegevensdragers en -middelen. Dit betekent niet dat dit niet georganiseerd is. In de Bijlage 3 zijn alle indicatoren nader toegelicht. Ter begeleiging voor de lezer is de toelichting op deze indicatoren opgenomen in deze paragraaf.

Tabel 11 Toelichting per indicator van de factor ruimten, applicaties en systemen

Factor	Indicator	Korte toelichting
Ruimte, Apparatuur en Systemen	**Periodieke (technische) testen**	a. Beschikbaarheid, toegankelijkheid en integriteit is technisch getest. b. Er is sprake van een frequente prestatietest, kan het systeem de hoeveelheid vraag aan. c. Toegangsbeveiliging, wordt getest met een professionele hacker/mystery guest.
	Periodieke updates	d. Er is sprake van periodieke wijzigingen, al dan niet op basis van a, b en c.
	Gelaagde systeemopbouw	e. Er is sprake van gelaagdheid in toegang en opbouw van systemen (technisch).

	Controle en toezicht mobiele gegevensdragers en middelen	f. Er is controle en toezicht op mobiele gegevensdragers en middelen die autorisatie tot gegevensdragers verschaffen. Hierdoor is er inzicht in welke apparaten er zijn en welke wanneer door wie in gebruik zijn.

DUO adviseurs Control & Compliance geven aan dat er relatief veel aandacht is aan fysieke toegangsbeveiliging. Het is niet mogelijk om bijvoorbeeld bij de computerruimten te komen, als je hiervoor niet bevoegd bent. Het gebouw is opgebouwd in verschillende compartimenten met verschillende toegangsrechten. Het gebouw is ingedeeld in verschillende compartimenten met verschillende toegangsrechten. De fysieke toegang is georganiseerd vanuit Informatiebeveiliging, wordt uitgevoerd door het Facilitaire bedrijf en is in beheer bij de private eigenaar van het gebouw. De toegang wordt gedeeld met de belastingdienst. De projectleider Algemene Rekenkamer geeft aan dat het laatste jaar de toegang tot ruimten en systemen, apparaten goed op orde is. Hierbij is geleerd van incidenten in het verleden. Doordat het dusdanig op orde is, wordt hier door de Algemene Rekenkamer niet meer specifiek naar gekeken. De IT-Audit coördinator OCW/ADR geeft aan dat er bij de DUO de risico's voornamelijk in het gebruik van de websites liggen. Via de websites kunnen studenten en instellingen hun gegevens inzien en wijzigen. De DUO is regelmatig een doelwit van partijen, en zo ook van de studenten zelf die de websites proberen te hacken. De IT-Audit coördinator OCW/ADR geeft aan dat om dit te beheersen er een periodieke penetratie plaatsvindt. Dit is een vorm van legal hacking, waarbij de vraag wordt gesteld of er voldoende is georganiseerd om hacking te voorkomen (beheersingsmaatregelen). Daarnaast wordt er frequent een *mystery guest* ingezet om de informatiebeveiliging op de werkvloer te toetsen. De DUO adviseur bij ICT-Supply geeft aan dat de hackers als hoofdtaak het inbreken op de eigen systemen hebben om zo, zoveel als mogelijk, problemen voor te zijn. Deze hackers nemen ook deel aan conferenties en evenementen speciaal voor hackers. Voor bedrijfsprocessen van de DUO is risicoklasse 2 de standaard, hierdoor is het niet mogelijk om zomaar een dienst op te tuigen. De DUO adviseur bij ICT-Supply geeft aan dat deze vraag wel (om met spoed een dienst op te tuigen) vanuit de politiek en beleid gesteld wordt. Hierbij geeft hij aan dat de politiek en beleid wellicht minder belang hebben bij informatiebeveiliging, of zij begrijpen de impact hiervan op informatiebeveiliging niet volledig. Ook al is er een ad-hocvraag vanuit beleid of politiek, er worden geen diensten zomaar opgetuigd. Door de informatiebeveiliging kost het meer tijd en geld en is het complexer om IT te ontwikkelen. De DUO voert systeemtesten, functionele testen, schaduwtesten en gebruikerstesten uit. Voor het testen bestaan er ontwikkelstraten, deze bestaan uit verschillende testomgevingen waarin de testen plaatsvinden. De reguliere interne gebruiker werkt in de productieomgeving.



Figuur 6 Verdeling factor ruimten, apparatuur en systemen in het OCW-informatiebeveiligingsbeleid 2014

Uit de documentanalyse blijkt dat er, in zowel het samenvattend auditrapport (Auditdienst Rijk, 2013, p. 20) als het rapport bij het jaarverslag (Algemene Rekenkamer, 2014), is aangegeven dat er verbeteringen moeten plaatsvinden op het gebied van toegangs-, test- en systeemdocumentatie. In het OCW-informatiebeveiligingsbeleid van 2014 worden de meeste indicatoren opgenomen in het beleid. Over de periodieke updates is er niets opgenomen.

4.2.6 Incidentmanagement

De factor incidentmanagement is onderverdeeld in de indicatoren incidentenplan en periodieke incidentenoefening. Het incidentenplan wordt bij de DUO het bedrijfscontinuïteitsplan genoemd. In de verantwoordings- en controledocumenten uit de documentanalyse is nauwelijks aandacht voor het incidentenplan en is er geen aandacht voor de incidentenoefening (één uitzondering in 2010). Vanaf 2014 beschikt de DUO over een volledig bedrijfscontinuïteitsplan; hiervoor was deze onvolledig. In het samenvattend auditrapport (Auditdienst Rijk, 2013, p. 20) is hier het volgende over opgenomen:

> "De DUO heeft niet gewerkt aan het bedrijfscontinuïteitsplan (BCP) maar aan het bedrijfscontinuïteitsmanagement (BCM). In 2011 hebben wij aangegeven dat het concept BCP nog onvoldoende de relaties en afhankelijkheden weergaf tussen het bestaande beleid en plannen die, op deelgebieden, aangeven hoe er bij continuïteitsproblemen moet worden gehandeld. Het concept BCP was een globaal, op hoofdlijnen beschreven document voor de DUO Groningen. Door capaciteitsdruk heeft de DUO in 2012 niet verder gewerkt aan het concept BCP, maar heeft besloten om een plan over BCM op te zetten. BCM geeft aan welke producten en processen moeten leiden tot een geborgde bedrijfscontinuïteit. Eind 2012 is het conceptplan BCM opgeleverd. Het niet hebben van een volledig BCP vergroot het risico - bij manifestatie van een calamiteit - dat niet de meest doelmatige procedures worden gevolgd. Hierdoor kan de calamiteit groeien tot een groot politiek afbreukrisico. Wij adviseren u om in 2013 capaciteit vrij te maken voor het opstellen van een overkoepelend BCP." (idem)

Uit het rapport van het jaarverslag (Algemene Rekenkamer, 2014, p. 40) blijkt dat het bedrijfscontinuïteitsplan nog niet voldeed: "Verder ontbreken voor een aantal kritische processen nog de bedrijfscontinuïteitsplannen. Dat zijn plannen waarin staat aangegeven wat er moet gebeuren als kritieke ICT-infrastructuur uitvalt" (idem).

In de resultatentabel is te zien dat er in 2015 binnen de verantwoordings- en controledocumenten geen aandacht meer is voor het incidentenplan. DUO adviseurs Control & Compliance geven aan dat er op dit moment, in 2016, een gedegen incidentenplan is. De IT-Audit coördinator OCW/ADR geeft aan dat incidentmanagement een verminderde prioriteit en capaciteit heeft; het is geen *ongoing concern*.

Er is geen sprake van incidentoefeningen. DUO adviseurs Control & Compliance vermelden hierover dat het moeilijk is incidenten na te kijken en dat het tijdelijk stopzetten van bepaalde systemen risico's met zich meebrengt. Tevens geeft de projectleider Algemene Rekenkamer aan dat oefenen

ingrijpend is voor de bedrijfsvoering. De IT-Audit coördinator OCW/ADR geeft aan dat het nabootsen van incidenten wel wordt gedaan door legal hacking en mystery guests. Daarnaast wordt er op risico's ingespeeld met cruciale systemen. Voor cruciale systemen is er een back-upplan. Een voorbeeld hiervan is dat als er een betaalsysteem platligt, er een noodbetaalprocedure beschikbaar is.

In het OCW-informatiebeveiligingsbeleid is de aandacht vergelijkbaar. Het blijkt dat er veel aandacht is voor het melden van, het rapporteren over en het acteren op individuele incidenten.

> "Inbreuken op de informatiebeveiliging, die aantoonbare schade aan de belangen van OCW veroorzaken, moeten worden gemeld bij de I-BVA. Welke incidenten het betreft en de afhandeling hiervan is beschreven in het document: "Informatiebeveiligingsincidenten en meldingsprocedure" (zie bijlage E). Informatiebeveiligingsincidenten en de afhandeling daarvan worden besproken in het informatiebeveiligingsoverleg. Medewerkers van OCW die een (vermoeden van een) incident of een inbreuk op de informatiebeveiliging constateren, melden dit onmiddellijk bij hun informatiebeveiligingscoördinator en/of lijnmanager die de I-BVA in kennis stellen, en in geval van een ICT-incident bij de ICT-Helpdesk" (Ministerie van Onderwijs, 2014, p. 22).

DUO adviseurs Control & Compliance geven aan dat het melden van incidenten als volgt is georganiseerd: incidenten worden gemonitord en gebundeld en er wordt (bij)gestuurd op de stand van zaken rondom incidenten. Hier wordt bekeken of er naar aanleiding van specifieke incidenten of patronen in incidenten DUO-brede maatregelen moeten worden getroffen. Een lek op een afdeling heeft impact op de hele organisatie, een dergelijk lek moet in de hele organisatie gedicht worden. Er is geen meldingsplicht, daarbij is het niet heel duidelijk wat men al dan niet moet melden. Openheid aangaande incidenten is van belang om deze op te kunnen lossen. Er is een aantal meldpunten bij helpdesk, diefstal, signalen van externe partijen (zoals instellingen en studenten). Er spelen momenteel veel ontwikkelingen op dit terrein, zoals het van kracht worden van de meldplicht datalekken, een tijdrovende klus. Verschillende typen incidenten worden gemeld bij de ICT-helpdesk en bij opgave van diefstal. Daarnaast is er sprake van signalen van externe partijen (zoals instellingen en studenten).

4.2.7 Compliance

De factor compliance is onderverdeeld in de indicatoren: kader, wet en/of richtlijn en periodieke controle. Alle bekeken verantwoordings- en controledocumenten komen voort uit de audit van de ADR. Doordat dit een controlefunctie betreft, is er inherent aandacht voor de factor compliance. Vanuit de documentanalyse is dit de enige factor die voor 2012 meer aandacht kreeg dan na 2012. Dit heeft voornamelijk te maken met de wet- en regelgeving waar men zich voor de komst van de BIR op moest focussen; er zijn meer aandachtsgebieden binnen de BIR dan binnen de VIR 2007.

Vanuit de interviews is er over de factor compliance de volgende informatie verzameld: de OCW-regiegroep toetst en begeleidt de implementatie van de BIR. Verder voert zowel de ADR als de

Algemene Rekenkamer controle uit op de BIR. Naast de toetsing op de BIR vindt er toetsing plaats op de Wet meldplicht datalekken. Voor auditing van de organisatie van informatiebeveiliging bij de DUO wordt gebruikgemaakt van ADR-Cluster regio Noord-Nederland. De CIO is gesitueerd in Groningen. De rapporten van de Algemene Rekenkamer zijn gebaseerd op de uitgevoerde audits door de ADR. De Algemene Rekenkamer reviewt het werk van de ADR. Hieruit maakt de projectleider Algemene Rekenkamer op dat de audits van de ADR bruikbaar zijn. Er wordt door de Algemene Rekenkamer meegekeken in Teammate (samenwerkingsplatform) van de ADR naar de uitvoering van de audits, en er zijn gesprekken met de auditors over de uitvoering. Aan het einde van de gehouden audits geeft de ADR een controleverklaring BIR-dossier aan de DUO. Dit jaar doet de ADR onderzoek naar de evaluatie van de implementatie van de BIR. De DUO heeft naast BVA van OCW een eigen BVA. Deze geeft strategisch richting aan de uitvoering van de audits. Iedere directeur geeft jaarlijks op informatiebeveiligingsterrein een in-control statement af.

Het ADR-auditrapport is een interne aangelegenheid. De Algemene Rekenkamer publiceert openbaar en vooral richting Tweede Kamer. Hierdoor hebben deze rapporten de politieke aandacht. Het is voor gecontroleerde organisaties niet wenselijk om problemen uit te moeten leggen aan de minister/staatssecretaris in de Tweede Kamer. Hierdoor zijn de controles een stimulans om de zaken die worden gecontroleerd op orde te hebben. Daarbij geeft de projectleider Algemene Rekenkamer aan dat het erop lijkt dat bedrijfsvoering de laatste jaren belangrijker wordt gevonden. Zo worden de audits van de ADR op het niveau van de SG/DG-commissie besproken. Tevens is recentelijk besloten dat de auditrapporten openbaar beschikbaar moeten zijn, maar de achtergronden en documenten zullen waarschijnlijk, omwille van veiligheid, niet openbaar worden. De projectleider Algemene Rekenkamer stelt: een dergelijke publicatie is een stok achter de deur voor het bevorderen van de bedrijfsvoering. Verder is het afhankelijk van wie de leiding heeft over een departement en of er al dan niet veel acties op het gebied van bedrijfsvoering worden genomen.

DUO adviseurs Control & Compliance geven aan dat er bij de DUO 15 kritieke bedrijfsprocessen zijn uitgelicht, die periodiek aan de BIR middels een beveiligingsanalyse worden getoetst. Nieuwe processen en systemen worden voorafgaand aan de implementatie getoetst. Bedrijfskritieke processen worden eenmaal per drie jaar getoetst. Het bleek, volgens de DUO adviseurs Control & Compliance, discussie op te leveren over wat al dan niet als bedrijfskritiek aangemerkt zou worden. Indien het proces als bedrijfskritiek is aangemerkt, wordt er meer aandacht en geld vrijgemaakt om een en ander op orde te krijgen. Voor de beveiligingsanalyse is de BIR opgeknipt in aandachtsgebieden; per aandachtsgebied is er een lijnmanager als verantwoordelijke aangewezen. Na een analyse kan, daar waar niet voldoende is voldaan aan de BIR, per deelgebied de lijnmanager worden aangesproken. Dit gaat, op basis van voorwaarden en risico's, van de compliancy-afdeling via de controllers. Vervolgens is de lijnmanager verantwoordelijk voor het al dan niet actie ondernemen op deze constateringen. De lijnmanager heeft ook de financiële zeggenschap over het aandachtsgebied. Bewustwording en sturing was voor de BIR gericht op wat niet mag en niet goed is. Nu is dit meer gericht op de voorwaarden waaraan moet worden voldaan.

De keus is belegd bij de lijnmanager. De lijnmanager dient een bewuste keuze te maken. Indien wordt gekozen om niets te doen aan een risico, betreft het een geaccepteerd risico. Het betreft in dit geval het 'pas toe of leg uit'-mechanisme. Momenteel worden de processen geanalyseerd via de proceseigenaar. De controles en de uitslagen hiervan zijn direct te verbinden aan een verantwoordelijke van het proces of aandachtsgebied. DUO adviseurs Control & Compliance geven aan dat tot 2014 niet altijd duidelijk was wie er verantwoordelijk waren op deelgebieden in informatiebeveiliging.

Voor de BIR was er voornamelijk de VIR 2007. Destijds was er geen specifiek beleid, maar werd de VIR 2007 als richtlijn aangehouden. Beveiligingscontroles werden met hulp van de VIR 2007 conform de CRAMM-methode uitgevoerd. De laatste update van de CRAMM (als systeem) was in 2004 en was niet compliant te maken met de BIR. De gedachtegang achter CRAMM is gebruikt voor het ontwikkelen van een nieuwe type analyse, die wel compliant is aan de BIR.

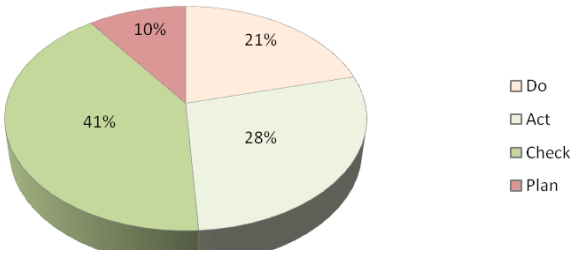
De projectleider Algemene Rekenkamer geeft aan dat de organisatie van informatiebeveiliging bij de DUO behoorlijk is verbeterd de laatste jaren, in 2015 heeft de Algemene Rekenkamer de onvolkomenheid op informatiebeveiliging laten vallen. De informatiebeveiliging is nog niet volledig op orde, sommige systemen zijn bijvoorbeeld niet toegewezen aan een lijnverantwoordelijke. ICT is bij de DUO, gezien de aard van de werkzaamheden, ontzettend belangrijk. Ook daarom blijft het voor de Algemene Rekenkamer een aandachtspunt. Dit wordt, volgens projectleider Algemene Rekenkamer, gedaan om een vinger aan de pols te houden. De aandacht is vooral gefocust op de uitvoering van informatiebeveiliging met betrekking tot de bedrijfsvoering. Hoewel het opvalt dat er relatief veel aandacht en tijd wordt geschonken aan wet- en regelgeving en de controle hierop, geeft de IT-Audit coördinator OCW/ADR aan dat de implementatie van de BIR moeizaam verloopt. De BIR is een brede richtlijn waarin normen door elkaar lopen. In principe is, volgens de IT-Audit coördinator OCW/ADR, de opzet van informatiebeveiliging binnen de DUO geregeld. De opzet betreft de documentatie, de structuren en de organisatie. Het is, volgens de IT-Audit coördinator OCW/ADR, lastig na te gaan hoe deze opzet uiteindelijk in de praktijk werkt. Tot nu toe is het, volgens de IT-Audit coördinator OCW/ADR, onvoldoende mogelijk om de naleving van de opzet na te gaan en daardoor is er geen duidelijk beeld. Daarbij geeft de IT-Audit coördinator OCW/ADR aan dat de BIR onvoldoende diepgang bevat om zichtbare beheersmaatregelen daadwerkelijk te meten. De Nederlandse wet- en regelgeving is het uitgangspunt, en daarmee compliance, van het informatiebeveiligingsbeleid (Ministerie van Onderwijs, 2014, p. 9).

4.3 Toepassing van het informatiebeveiligingssysteem

In deze paragraaf is de mate waarin een informatiebeveiligingssysteem aanwezig is bij de DUO beschreven. De zeven factoren dienen onderdeel te zijn van een informatiebeveiligingssysteem. Hiertoe is eerst beschreven in hoeverre er aandacht is voor en uiting is van Plan, Do, Check en Act. Vervolgens is beschreven in hoeverre de factoren, bij elkaar genomen, onderdeel zijn van een informatiebeveiligingssysteem.

4.3.1 Plan, Do, Check en Act

Een werkend informatiebeveiligingssysteem wordt gedreven door het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System (ISMS). Dit is onderverdeeld in de indicatoren: *Plan, Do, Check en Act*. Voor elk van de indicatoren, behalve in 2014, is er vanuit de documentanalyse in ieder jaar aandacht. De meeste aandacht gaat naar *Check* en de minste aandacht gaat naar *Plan* in de verantwoordings- en controledocumenten. Er is meer aandacht voor de factor beleid, dat gelieerd is aan *Plan*. Deze is grotendeels gericht op de risicoanalyse, dit is 55 maal van de in totaal 91 duidingen aangetroffen in de documentanalyse op de factor beleid. De risicoanalyse op zich is geen uiting van *Plan.*



Figuur 7 Verdeling PDCA in de verantwoordings- en controledocumenten

Binnen de factoren beleid en strategie vallen minder indicatoren dan onder de andere factoren. Het valt op dat er in 2014 weinig is beschreven over het informatiebeveiligingssysteem bij de DUO. In 2014 ligt de nadruk op in hoeverre de opzet van het systeem is ingericht en dat er nog meer aandacht uit moet gaan naar de daadwerkelijke uitvoering en de verbetering van informatiebeveiliging;

> "In 2013 werd bij het Ministerie van OCW de uitvoering van de informatiebeveiliging bij het baten-lastenagentschap Dienst Uitvoering Onderwijs (DUO) door ons gekwalificeerd als een onvolkomenheid. Ook bij de DUO zijn in 2014 veel maatregelen genomen, waardoor de informatiebeveiliging verbeterd, maar nog niet geheel op orde is. Ook bij de DUO is nog niet vastgesteld of de maatregelen in de praktijk goed werken, waardoor de Algemene Rekenkamer deze onvolkomenheid ook handhaaft". (Algemene Rekenkamer, 2014, p. 40)

In de verantwoordings- en controledocumenten wordt de aanmerking 'niet en deels toegepast' aangaande uitvoering (do) en verbetering (act) vijfmaal aangetroffen van de in totaal 33 duidingen in de periode 2014-2015. Hier dient rekening gehouden te worden met de vermelding van de IT-Audit coördinator OCW/ADR dat het lastig is om te toetsen hoe de plannen en de wet- en regelgeving daadwerkelijk worden nageleefd, waardoor het algehele beeld van de toepassing van de uitvoering en verbetering ontbreekt. In de periode 2010-2011 is door de Algemene Rekenkamer (2011a) beschreven dat de eerder opgemerkte onvolkomenheden nog niet zijn opgelost.

In 2010 is er in de verantwoordings- en controledocumenten voor *Plan* en *Check* juist meer aandacht dan in de jaren erna. Hier is te zien dat in verschillende organisatieonderdelen *Plan* en *Check* wel, dan wel deels, zijn georganiseerd. In het geval van *Plan* is dit in verantwoordings en controledocumenten uit 2010 een enkele keer als niet toegepast beoordeeld ten opzichte van tweemaal volledig toegepast. De aandacht aangaande *Plan* is vooral gericht op het nemen van verantwoordelijkheid door het management. Daarbij is door de projectleider Algemene

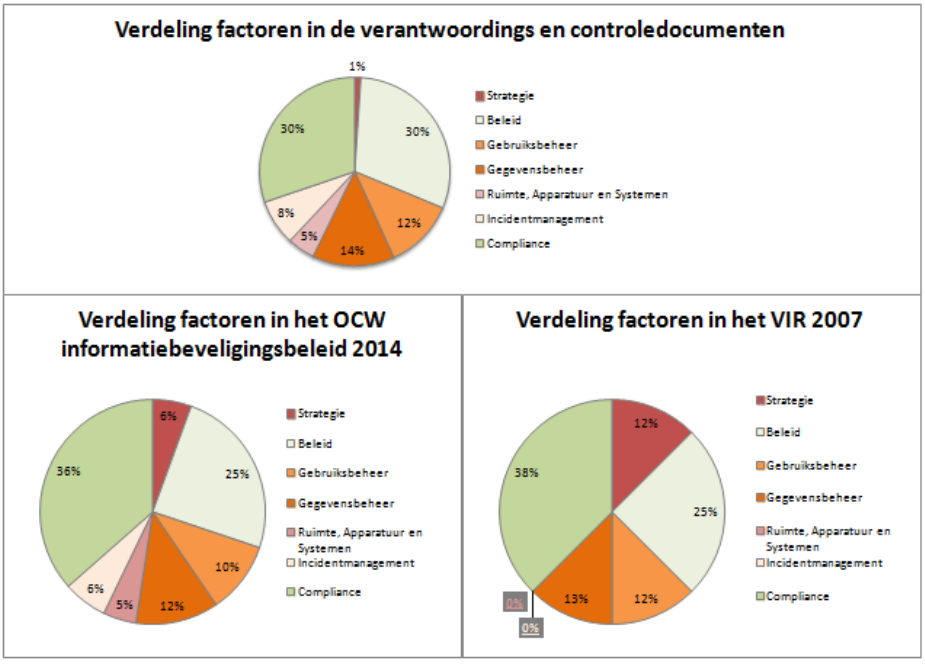
Rekenkamer aangegeven dat het oordeel van de Algemene Rekenkamer met name op het OCW-brede aspect is toegepast. In 2010 was er minder specifieke aandacht voor de DUO vanwege de fusie in 2009. Uit het interview met de DUO adviseurs Control & Compliance lijkt het erop dat de DUO niet voldeed aan het OCW-beleid vanwege de recente fusie. Na de invoering van de zijn BIR de verantwoordelijkheden toebedeeld, hierdoor zijn informatiebeveiligingsmaatregelen aan specifieke personen toegewezen. Verder is er vanaf 2014 een eigen DUO-beleid in de vorm van het addendum. Voor de BIR was *Plan* voornamelijk gericht op de VIR 2007, en was het niet duidelijk genoeg wie waarvoor verantwoordelijk was.

Betreffende de aandacht voor *Check* in de verantwoordings- en controledocumenten in 2010 wordt enerzijds beoordeeld dat het volledig toegepast is en anderzijds dat dit deels is toegepast. Wederom betreft het de OCW-brede aanpak, waarbij er naar aanleiding van uitgevoerde audits monitoring plaatsvindt. Over de jaren heen is er vanuit de documentanalyse brede aandacht voor *Check*; de gebruikte documenten voor de analyse komen voort uit een controle- en verantwoordingsactie.

4.3.2 Toepassing van factoren binnen het informatiebeveiligingssysteem

Voor deze masterscriptie is gesteld dat het van belang is voor informatiebeveiliging dat er, conform State of the Art, zeven factoren binnen een informatiebeveiligingssysteem zijn georganiseerd. Uit de documentanalyse en de interviews blijkt dat elk van de factoren in bepaalde mate tot uiting komt in de organisatie van informatiebeveiliging bij de DUO. Aan de factoren compliance en beleid is in meerdere mate - en voor de factoren strategie en ruimte, apparatuur en systemen in mindere mate - aandacht geschonken (Bijlage 1). In fFiguur 4 is de verdeling van de aandacht voor de factoren bij de geanalyseerde documenten weergegeven. De verdeling van de factoren in de verantwoordings- en controledocumenten en het OCW-informatiebeveiligingsbeleid 2014 is vergelijkbaar. Daarbij is in de VIR 2007, die voor 2013 bij de DUO als richtlijn voor beleid werd gehanteerd, niets voor de factoren incidentmanagement en ruimte, apparatuur en systemen aangetroffen.

Figuur 8 Verdeling van de aandacht voor de zeven factoren bij de geanalyseerde documenten



Uit de interviews blijkt dat er voor de factoren strategie en ruimten, applicaties en systemen in de praktijk niet per se minder aandacht is. Zo stelt de DUO adviseur bij ICT-Supply dat er binnen de DUO veel aandacht is voor techniek. Er wordt getracht om zoveel mogelijk digitaal te organiseren, met het oog op de digitale agenda vanuit de politiek. Op dit moment is bijna alles elektronisch geregeld. Ook geeft deze adviseur aan dat de IT-architectuur 10 tot 20 jaar aanwezig is.

In de resultatentabel (bijlage 1) is te zien dat er in 2010, 2011 en 2012 33 van de 87 indicatoren als niet of deels aangemerkt zijn (38%), in 2013, 2014 en 2015 zijn dit er 18 van de 106 (17%). Tevens is zichtbaar dat na de invoering van de BIR er minder onvolkomenheden op het gebied van informatiebeveiliging zijn aangemerkt. Vanuit zowel de interviews als de documentanalyse is duidelijk dat vanaf de invoering van de BIR de belegde verantwoordelijkheden in de organisatie van informatiebeveiliging toegespitst zijn op de diverse aandachtsgebieden die binnen de BIR gelden. Voorts is door de respondenten aangegeven dat verbetering van de organisatie van informatiebeveiliging voornamelijk wordt gestimuleerd door: incidenten, wet- en regelgeving en in dit specifieke geval een negatief rapport van de Algemene Rekenkamer. Al met al kan gesteld worden dat alle factoren in bepaalde mate tot uiting komen in de organisatie van informatiebeveiliging bij de DUO.

5.Conclusie

Voor deze masterscriptie is onderzocht welke factoren conform *State of the Art* van belang zijn bij de organisate van informatiebeveiliging binnen de publieke sector. Daarnaast is geanalyseerd in hoeverre deze factoren tot uiting komen bij de DUO in de periode van 2010 tot en met 2015. In dit hoofdstuk is antwoord gegeven op de centrale onderzoeksvraag. De onderzoeksvraag is tweeledig. Ten eerste is, vanuit het theoretisch kader, antwoord gegeven op de vraag '*Welke factoren zijn conform State of the Art van belang voor het organiseren van informatiebeveiliging in de publieke sector?'.* Ten twee is de vraag '*in hoeverre komt dit tot uiting bij de Dienst Uitvoering Onderwijs (DUO) in de periode van 2010-2015?'* beantwoord aan de hand van de onderzoeksresultaten. Dit hoofdstuk is afgesloten met een paragraaf discussie waarin een aantal overwegingen en beperkingen zijn opgenomen met suggesties voor verder onderzoek. De discussie is afgerond met een aantal praktische aanbevelingen.

5.1 Conclusie

In het theoretisch kader zijn op basis van academische literatuur en informatiebeveiligingsrichtlijnen zeven factoren geformuleerd. Deze zeven factoren zijn conform *State of the Art* van belang voor de organisatie van informatiebeveiliging. In de geraadpleegde literatuur en richtlijnen voor informatiebeveiliging zijn de gestelde voorwaarden voor de organisatie van informatiebeveiliging pluriform en daarmee multi-interpreteerbaar. Eveneens is er overlap aanwezig tussen de verschillende voorwaarden. De zeven factoren zijn specifieker en bevatten een duidelijke scheiding onderling. Deze verdieping verhoogd de betrouwbaarheid en validiteit voor wetenschappelijk onderzoek; het kunnen aanduiden van een feitelijk gegeven op basis van vastgestelde meetwaarden. Een integrale aanpak voor informatiebeveiliging middels een informatiebeveiligingssysteem staat centraal in de geanalyseerde academische literatuur en richtlijnen. Het informatiebeveiligingssysteem bevat conform de Deming cirkel: *Plan, Do, Check en Act*. Daarbinnen gelden de factoren als voorwaarden die zijn gericht op hoe informatie beveiligd kan worden. Er is onderscheid gemaakt in de volgende zeven factoren:

1. Strategie;
2. Beleid;
3. Gebruiksbeheer;
4. Gegevensbeheer;
5. Ruimten, apparatuur en systemen;
6. Incidentmanagement;
7. Compliance.

In hoeverre deze factoren tot uiting komen bij de DUO in de periode 2010-2015 is onderzocht middels een documentanalyse en semi-gestructureerde expert interviews. Hieruit bleek dat elk van de factoren tot uiting komt bij de DUO. Op basis van de documentanalyse en de interviews komen de factoren compliance en beleid in meerdere mate-, en strategie en ruimten, apparatuur en systemen in mindere mate tot uiting in de organisatie van informatiebeveiliging. Dit geeft niet aan in hoeverre deze al dan niet meer of minder in de praktijk worden toegepast. De bijbehorende

indicatoren bij de factoren zijn allen onderdeel van organisatie van informatiebeveiliging bij de DUO, hiervan is echter niet de daadwerkelijke werking aan te tonen. Daarbij is er voor de onderwerpen strategie, digitale weerbaarheid, audittrails, periodieke updates van systemen, periodieke technische testen alsmede controle en toezicht op mobiele gegevensdragers en middelen in de documenten weinig tot geen duiding aangetroffen. Tijdens de interviews bleken deze factoren wel georganiseerd te zijn. Verder bleek uit zowel de documentanalyse als de interviews dat het incidentplan nauwelijks tot niet geoefend wordt. Hiervoor is als reden gegeven dat het te veel risico's met zich mee brengt en dat het een te grote impact heeft op de bedrijfsvoering. Bij de DUO is er een informatiebeveiligingssysteem in werking, er zijn beleidsplannen, er is uitvoering van diverse maatregelen, er is controle via interne beveiligingsanalyses, auditrapporten van de ADR en controle door de Algemene Rekenkamer. Eveneens stelt de DUO verbeterplannen op en is er door de Algemene Rekenkamer geconcludeerd dat de organisatie van informatiebeveiliging bij de DUO verbeterd is. Conform de zeven factoren als onderdeel van een informatiebeveiligingssysteem kan gesteld worden dat de DUO, met uitzondering van het oefenen van het incidentenplan, de opzet van de organisatie van informatiebeveiliging op orde heeft.

5.2 Discussie

In de paragraaf discussie wordt ingegaan op de validiteit en beperkingen die van toepassing zijn binnen dit onderzoek. De discussie behelst kortweg de volgende kanttekeningen. Er is sprake van beperkingen aangaande de academische literatuur en er is een gebrek aan data over incidenten. Verder is vanwege het onderwerp 'informatiebeveiliging' gebrek aan beschikbaarheid van- en toegang tot informatie. Tenslotte zijn de factoren bruikbaar voor een analyse naar de uiting van *State of the Art* informatiebeveiliging, maar is het inzicht op de toepassing van de factoren beperkt. Vervolgens zijn er praktische aanbevelingen geformuleerd,

De tijdens het onderzoek verkregen academische literatuur beperkt zich tot een klein aantal auteurs. Getracht is om dit onderzoek de meest recente artikelen te onderzoeken om het onderzoek zo betrouwbaar mogelijk te maken. De selectie van de juiste literatuur bleek niet eenvoudig. De gebruikte artikelen zijn veelal geschreven tussen 2002 en 2008. Vanwege de opvolging van ontwikkelingen in de ICT kunnen deze achterhaald zijn. Als tegenhanger zijn er een klein aantal recentere artikelen gebruikt. Daarnaast zijn de artikelen over informatiebeveiliging matig wetenschappelijk onderbouwd. De artikelen zijn veelal onderbouwd vanuit één of twee casussen. Daarbij baseerde deze zich vooral op het overbruggen van de conventionele scheiding tussen socio-organisatorische en technische aspecten van informatiebeveiliging. De conventionele scheiding is niet direct te herleiden in de richtlijnen die medio de jaren negentig zijn opgesteld. Er zijn geen gefundeerde bewijzen gevonden over hoe en waarom deze scheiding er precies is.

Eveneens ontbreekt het in de wetenschappelijke literatuur over informatiebeveiliging aan een maatschappelijk aspect; wat is het effect op de maatschappij indien er sprake is van een datalek? In dit onderzoek is op basis van literatuur over veiligheid conform Stone (2012) uitgegaan dat een datalek het vertrouwen in de overheid schaadt. Er is niets bekend over het al dan niet meer willen

delen van persoonlijke informatie met een publieke instelling. Het is aan te bevelen om meer maatschappelijk onderzoek uit te voeren naar de gevolgen en oorzaken van misbruik van persoonsgegevens.

Daarnaast is er weinig data beschikbaar aangaande datalekken en incidenten. Wat zijn nu de oorzaken en gevolgen van deze lekken? In hoeverre is er een typologie van incidenten? De in werking treding Wet meldplicht datalekken kan op termijn hier mogelijk meer inzicht over verschaffen. Hierbij dient rekening gehouden te worden met het *dark numbers* fenomeen (P.27). Een van de moeilijkheden bij het onderzoek naar informatiebeveiliging is dat juist diefstal of misbruik (lang) verborgen blijft. Voorbeelden hiervan zijn malware en de virus Trojan Horse, hierbij is het doel om juist onzichtbaar gegevens te verzamelen. Dit maakt het onmogelijke om stelling te nemen over of maatregelen leiden tot veilige informatie; enkel tot veiligere informatie. Hierbij past het gezegde 'Je weet niet wat je niet weet'.

Een van de kanttekeningen bij dit onderzoek is dat niet al het wenselijk onderzoeksmateriaal vrij verkrijgbaar is. Zo is gesteld dat de IT-audits openbaar beschikbaar zijn, deze zijn niet beschikbaar. Deze bleken wel beschikbaar te zijn indien er een WOB-verzoek, Wet Openbaarheid van Bestuur, ingediend zou worden. Omwille van tijdsbeperking was dit niet meer mogelijk. Verder was het niet mogelijk om de factoren in de praktijk te toetsen. De reden hiervoor is tweeledig, vertrouwelijkheid en de DUO telt 1797 medewerkers (Dienst Uitvoering Onderwijs, 2016, p. 3) waardoor het niet, binnen deze masterscriptie, haalbaar is om de gehele organisatie door te lichten.

Uit de analyses blijkt dat elk van de factoren tot uiting komt bij de DUO. Het is echter niet vast te stellen in hoeverre de opzet van de informatiebeveiliging in de dagelijkse praktijk wordt nageleefd. Tevens zijn de rapporten voornamelijk gericht op onvolkomenheden en minder gericht op de volkomenheden van informatiebeveiliging. De mate van aandacht van de organisatie van de factoren geeft summiere informatie over de daadwerkelijke toepassing van deze factoren. Verder geven de respondenten aan dat zowel incidenten, een negatief rapport van de algemene rekenkamer als wet- en regelgeving van invloed zijn op de verbetering van de organisatie van informatiebeveiliging. Dit is echter niet voldoende om te stellen dat deze zaken daadwerkelijk leiden tot een al dan niet betere organisatie. Naast deze invloeden zouden ook andere aspecten invloed kunnen hebben zoals; toename van kennis over informatiebeveiliging, toename van e-dienstverlening, toegenomen bewustwording, toegenomen inzicht op het vraagstuk, verbeterde techniek, gebruiksvriendelijkere techniek, enzovoort.

De factoren *an sich* zijn bruikbaar bij het verkrijgen van inzicht over de organisatie van informatiebeveiliging bij de DUO. De factoren kunnen gebruikt worden voor een vergelijkend onderzoek. Binnen zo'n onderzoek is aan te raden om dezelfde type onderzoekseenheden te kiezen maar waarbij de ene groep relatief minder incidenten ervaart en de andere relatief meer. Hiermee kan worden onderzocht of er verschillen aanwezig zijn. Daarnaast ontstaat er meer inzicht in de werking van informatiebeveiliging. Om dit uit te kunnen voeren is inzicht op incidenten noodzakelijk.

5.2.1 Praktische aanbevelingen

Bovenstaand zijn reeds enkele suggesties gedaan voor verder onderzoek. In deze paragraaf gaat de aandacht uit naar praktische aanbevelingen. De eerste aanbeveling is gericht aan de DUO. Vervolgens is de tweede aanbeveling gericht aan het Ministerie van Binnenlandse Zaken, deze treedt als penvoerder op voor de BIR. Zoals de IT-Audit coördinator OCW/ADR aangaf kan de focus verlegd worden naar wat er nodig is door in meerdere mate de risicoanalyse als uitgangspunt te nemen. Dit betekent in mindere mate te focussen op het voldoen aan de maatregelen zoals zijn voorop gesteld binnen de BIR.

Oefen het incidentenplan

Uit de analyse is gebleken dat het incidentenplan niet wordt geoefend. Reden als te risicovol en te belastend voor de bedrijfsvoering worden genoemd. Binnen het vakgebied crisismanagement is oefenen een veel gebruikt middel. Hier wordt veelal gebruik gemaakt van spelsimulaties en in steeds meerdere mate van *'serious games'* en van het fysiek oefenen van wat te doen tijdens een ramp door bijvoorbeeld evacuaties na te bootsen.

> "3Er bestaan meerdere definities voor een Serious Game, samenvattend faciliteert een Serious Game een veilige omgeving waarin (risicovolle) praktijksimulaties kunnen plaatsvinden in de vorm van een spel en waarin men streeft om vooraf bepaalde leerdoelen te behalen." (Dijkstra & Weel, 2016, p. 4)

Serious gaming is hiertoe een geschikt middel om het incidentenplan mee te oefenen. Deze methode is aan te bevelen voor de DUO om zo de factor incidentmanagement op orde te stellen.

Herzien van de Baseline Informatiebeveiliging Rijksdienst

De BIR wordt momenteel herzien om tot een nieuwe versie te komen. Naar aanleiding van deze masterscriptie is aan te bevelen om met de volgende overwegingen rekening te houden:

In het theoretisch kader is aangemerkt dat het gebruik van richtlijnen als risico uitdijing heeft. Dit betekent dat de kans bestaat dat het aantal regels en vereisten binnen een richtlijn groeit. De tactische baseline is opgebouwd uit *best practices*, hierbij dients zoals benoemd in het theoretisch kader de vraag wat er allemaal mogelijk is het uitgangspunt te zijn. De BIR bestaat momenteel uit 298 vereisten. Hierbinnen is bijvoorbeeld onder andere de regel getroffen: "Eten en drinken is verboden in computerruimtes"(Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2012, p. 26). Hierbij kan afgevraagd worden wat er wordt verstaan onder computerruimten en in hoeverre leidt eten in deze ruimte tot onveiligheid van informatie? Het is te adviseren om enkel doelmatige vereisten op te nemen. De vereisten dienen bij te dragen aan maatregelen die leiden tot veiligere informatie.

Tenslotte is het van belang dat de BIR zo opgesteld wordt dat het aan de hand van richtlijn mogelijk wordt om de daadwerkelijke werking van de organisatie van informatiebeveiliging te toetsen. Hiermee biedt het extra handvaten om de organisatie te kunnen verbeteren.

Literatuur

Algemene Rekenkamer. (2010). *Rapport bij het jaarverslag 2010 van het Ministerie van Onderwijs Cultuur en Wetenschap (VIII)*.

Algemene Rekenkamer. (2011a). *Rapport bij het jaarverslag 2011 van het Ministerie van Onderwijs Cultuur en Wetenschap (VIII)*.

Algemene Rekenkamer. (2011b). *Rijksbreed bedrijfsvoeringsonderzoek in het kader van het verantwoordingsonderzoek 2011 - Achtergronddocument Informatiebeveiliging en vertrouwensfuncties*

Algemene Rekenkamer. (2012a). Bij 7 ministeries en 6 baten-lastenagentschappen zijn beheer en beveiliging van ICT-systemen nog niet op orde. Retrieved 26-7-2016, from http://verantwoordingsonderzoek.rekenkamer.nl/2012/rijksbreed/bedrijfsvoering/bij-7-ministeries-en-6-baten-lastenagentschappen-zijn-beheer-en

Algemene Rekenkamer. (2012b). *Rapport bij het jaarverslag 2012 van het Ministerie van Onderwijs Cultuur en Wetenschap (VIII)*.

Algemene Rekenkamer. (2014). *Rapport bij het jaarverslag 2014 van het Ministerie van Onderwijs Cultuur en Wetenschap (VIII)*.

Algemene Rekenkamer. (2015). *Staat van de rijksverantwoording 2015;Rijksbrede resultaten verantwoordingsonderzoek*.

Auditdienst Rijk. (2013). *Samenvattend auditrapport 2013 Ministerie van Onderwijs, Cultuur en Milieu (VIII)*.

Babbie, E. (2010). The Practice of Social Research (ed.). California: Cengage Learning: Inc.

Baskerville, R. (1993). Information systems security design methods: implications for information systems development. *ACM Computing Surveys (CSUR), 25*(4), 375-414.

Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management, 15*(5/6), 337-346.

Beck, U. (1992). Risk society: towards a new modernity. *Theory, culture and society*.

Beynon-Davies, P. (2002). *Information systems: An introduction to informatics in organisations*: Palgrave Macmillan.

Bureau Edustandaard. (2016). Hoofdpagina.

College en Forum Standaardisatie. (2016). 'Pas toe of leg uit' lijst. Retrieved februari 15, 2016, from https://lijsten.forumstandaardisatie.nl/lijsten/open-standaarden?lijst=Pas%20toe%20of%20leg%20uit&status%5B%5D=Opgenomen&pagetitle=pastoeof

David, J. (2002). Policy enforcement in the workplace. *Computers & Security, 21*(6), 506-513.

Dhillon, G. (2007). *Principles of Information Systems Security: text and cases*: Wiley New York, NY.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal, 11*(2), 127-153.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal, 16*(3), 293-314.

Dienst Uitvoering Onderwijs. (2014). Applicatielandschap. Architectuur-wiki.

Dienst Uitvoering Onderwijs. (2016). *Kerncijfers 2015; Dienst Uitvoering Onderwijs*. Retrieved from https://duo.nl/organisatie/images/duo-kerncijfers-2015.pdf.

Digitaal Universiteitsblad UU. (2013, november 5, 2013). DUO waarschijnlijk morgen weer online. Retrieved juli 8, 2016, from http://www.dub.uu.nl/artikel/nieuws/duo-waarschijnlijk-morgen-weer-online.html

Dijkstra, D. H. C., & Weel, M. (2016). Adviesrapport Pilot Serious Game Informatiebeveiliging; de gebruiker aan zet: BECIS BV.

Doherty, N. F., & Fulford. (2006). Aligning the information security policy with the strategic information systems plan. *Computers & security, 25*(1), 55-63.

D'Arcy, J., & Hovav, A. (2008). Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures. *Journal of Business Ethics, 89*(1), 59-71.

Ferris, J. M. (1994). Using standards as a security policy tool. *StandardView, 2*(2), 72-77.

Flores, W., Sommestad, T., Holm, H., & Ekstedt, M. (2011). Assessing future value of investments in security-related IT governance control objectives? Surveying IT professionals. *Electronic journal of information systems evaluation, 14*(2), 216-227.

Goutier, H., & van Lieshout, J. (2010). NORA 3.0 Principes voor samenwerking en dienstverlening. *Den Haag, E-Overheid*.

Hacker ontdekt gat in website DUO. (2011, juni 7, 2011). Retrieved juli 10, 2016, from http://www.rtlnieuws.nl/nieuws/binnenland/hacker-ontdekt-gat-website-duo

Hirschheim, R., & Klein, H. K. (1989). Four paradigms of information systems development. *Communications of the ACM, 32*(10), 1199-1216.

Houngbo, P. J., & Hounsou, J. T. (2015). Measuring Information Security: Understanding And Selecting Appropriate Metrics. *International Journal of Computer Science and Security (IJCSS), 9*(2), 108.

IBD. (2013). *Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten*.

ICTU. (2016). NORA online.

Janczewski, L. (1999). Managing security functions using security standards. *Internet and Intranet Security Management: Risks and Solutions*, 81-105.

Jensen, K., & van der Aalst, W. P. (2009). Process-Aware Information Systems: Lessons to Be Learned from Process Mining *Transactions on Petri Nets and Other Models of Concurrency II* (Vol. 5460, pp. 1-26): Springer Berlin Heidelberg.

Jorritsma-Lebbink, A. (2013). *Aanbiedingsbrief: Resolutie Informatieveiligheid, randvoorwaarde voor de professionele gemeente*. Retrieved from https://vng.nl/files/vng/brieven/2013/20131031_ledenbrief_resolutie-informatieveiligheid-randvoorwaarde-voor-de-professionele-gemeente.pdf.

Kwaliteitsinstituut Nederlandse Gemeenten. (2013). *Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten*.

Lindup, K. R. (1995). A new model for information security policies. *Computers & Security, 14*(8), 691-695.

Linker, P.-J. (2006). *Sturing in de Rijksdienst*: Uitgeverij Van Gorcum.

Mataracioglu, T., & Ozkan. (2011). Governing Information Security in Conjunction with COBIT and ISO 27001. *International Journal of Computer Science & Information Technology, 3*(3), 288-293.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2012). *Baseline Informatiebeveiliging Rijksdienst*.

Ministerie van Onderwijs, Cultuur en Wetenschap,. (2010). *Jaarverslag van het Ministerie van Onderwijs, Cultuur en Wetenschap (VIII)*

Ministerie van Onderwijs, Cultuur en Wetenschap,. (2013). *Jaarverslag van het Ministerie van Onderwijs, Cultuur en Wetenschap (VIII)*.

Ministerie van Onderwijs, Cultuur en Wetenschap,. (2014). *Informatiebeveiligingsbeleid, Ministerie van OCW*.

Mishra, S., & Powel, J. (2011). Identifying information security Governance dimensions: A multinomial analysis. *Issues in information systems, 12*(1), 271.

Ngo Higgins, H. (1999). Corporate system security: towards an integrated management approach. *Information Management & Computer Security, 7*(5), 217-222.

Panteia. (2014). *Identiteit in cijfers*.

Pieters, W. (2011). The (Social) Construction of Information Security. *The Information society, 27*(5), 326-335.

Rijksoverheid. (2016). Dienst Uitvoering Onderwijs (DUO). Retrieved juli 22, 2016, from https://www.rijksoverheid.nl/ministeries/ministerie-van-onderwijs-cultuur-en-wetenschap/inhoud/organisatie/organogram/dienst-uitvoering-onderwijs-duo

Rijksoverheid. (n.d.). De Enterprise Architectuur Rijksdienst. Retrieved 25 juli, 2016, from http://www.earonline.nl/index.php/Wat_is_de_Enterprise_Architectuur_Rijksdienst

SA-MBO ICT. (2015). *SA-MBO ICT- Normenkader Informatiebeveiliging MBO*.

Salini, P., & Kanmani, S. (2015). Effectiveness and performance analysis of model-oriented security requirements engineering to elicit security requirements: a systematic solution for developing secure software systems. *International Journal of Information Security*, 1-16.

Schellevis, J. (2010, november 9, 2010). Overheidsorganisatie laat privégegevens studenten uitlekken. Retrieved februari 2, 2016, from http://tweakers.net/nieuws/70674/overheidsorganisatie-laat-privegegevens-studenten-uitlekken.html

Spruit, M. E. M. (2010). Informatiebeveiliging en bewustzijn. *De IT-Auditor*(1), 24-27.

Stone, D. (2012). *Policy paradox : the art of political decision making* (3 ed.). New York: W. W. Norton & Company.

Straub Jr, D. W. (1990). Effective IS Security. *Information Systems Research, 1*(3), 255-276.

Thiel, S. v. (2015). *Bestuurskundig onderzoek: een methodologische inleiding*: Bussum: Coutinho.

Unie van Waterschappen. (2013). *Baseline Informatiebeveiliging Waterschappen*.

US NIST. (2015). About NIST. februari 15, 2016, from http://www.nist.gov/public_affairs/nandyou.cfm

van Lieshout, M. J., Kool, L., Bodea, G., Schlechter, J., van Schoonhoven, B., & Kennisopbouw, O. I. (2012). *Stimulerende en remmende factoren van Privacy by Design in Nederland*: Delft: TNO.

Vanderveen, G. N. G. (2011). Meten van onveiligheid. 91-104.

Veiga, J. H. P., & Eloff. (2007). An Information Security Governance Framework. *Information systems management, 24*(4), 361-372.

Waterschappen, U. v. (2013). *Baseline Informatiebeveiliging Waterschappen*.

Wulp, P. J. v. d. (2004). *Het Meten van Security*: Erasmus universiteit: TNO Telecom.

Yang, T.-H., Ku, C.-Y., & Liu, M.-N. (2016). An integrated system for information security management with the unified framework. *Journal of Risk Research, 19*(1), 21-41.

Bijlagen

Bijlage 1- Resultatentabel

Bijlage 2- Respondentenlijst

Bijlage 3- Coderingstabel

Bijlage 4- Documentenlijst voor de -analyse

Bijlage 5- Dekking van bepalende factoren voor een informatiebeveiligingssysteem ten opzichte van tactische kaders

Bijlage 6- Gecodeerde segmenten MAXQDA