MASTER'S THESIS

De invloed van cloud computing op de security architectuur van overheidsorganisaties

Schollaart, A.

Award date:
2021

De invloed van cloud computing op de security architectuur van overheidsorganisaties

The influence of cloud computing on the security architecture of governmental organizations

Opleiding:	Open Universiteit, faculteit Bètawetenschappen Masteropleiding Business Process Management & IT
Programme:	Open University of the Netherlands, faculty of Science Master of Science Business Process Management & IT
Cursus:	IM0602 Voorbereiden Afstuderen BPMIT IM9806 Afstudeeropdracht Business Process Management and IT
Student:	Annet Schollaart
Identiteitsnummer:	
Datum:	31-08-2021
Afstudeerbegeleider:	Dr. R. Bos
Meelezer:	Ir. L. Cuijpers
Versienummer:	1.0
Status:	Definitief

Abstract

Er is weinig bekend over de invloed van cloud computing op de vormgeving van de security architectuur van overheidsorganisaties. Dit onderzoek richt zich op een eerste aanzet in het vaststellen van deze invloed, met als doel om security architectuurbeslissingen van overheids-organisaties beter te kunnen onderbouwen.
Uit de resultaten blijkt dat er niet altijd sprake is van een formeel vastgelegde security architectuur binnen een overheidsorganisatie. Dat cloud computing invloed heeft op de security van een overheidsorganisatie is duidelijk vast te stellen. Cloud computing heeft invloed op veiligheids-aspecten, zoals: wet- en regelgeving, beheersbaarheid van processen en systemen en gegevens-bescherming. Overheidsorganisaties moeten op het gebied van cloud security aan aanvullende overheidsvoorschriften voldoen.

Sleutelbegrippen

Security architectuur; publieke sector; cloud computing; overheidsorganisatie; cloud security

Samenvatting

Ondanks de toenemende vraag naar IT-diensten via cloud computing bij overheidsorganisaties, is er weinig bekend over de invloed van cloud computing op de vormgeving van hun security architectuur. Dit onderzoek richt zich op een eerste aanzet in het vaststellen van de invloed van cloud computing op de security architectuur van overheidsorganisaties, met als doel om security architectuurbeslissingen van overheidsorganisaties beter te kunnen onderbouwen. Hiervoor is eerst literatuuronderzoek uitgevoerd en zijn er vervolgens kwalitatieve gegevens verzameld bij een overheidsorganisatie door middel van interviews en documentatie over het onderwerp binnen de context van de organisatie.

Uit de resultaten blijkt dat er niet altijd sprake is van een formeel vastgelegde security architectuur binnen een overheidsorganisatie. Dat cloud computing invloed heeft op de security van een overheidsorganisatie is duidelijk vast te stellen. Cloud computing heeft invloed op veiligheids-aspecten, zoals: wet- en regelgeving, beheersbaarheid van processen en systemen en gegevens-bescherming. Overheidsorganisaties moeten voldoen aan aanvullende overheidsvoorschriften ten aanzien van cloud security. De caseorganisatie ervaart dat leveranciers hierdoor moeite kunnen hebben om tegemoet te komen aan de eisen die in overeenkomsten worden gesteld. Wat betreft de beheersbaarheid van processen en systemen ervaart zij dat zij door cloud computing op een aantal onderdelen in sterke mate haar controle en beheersmogelijkheden aan de cloud serviceproviders afstaat. Dit leidt tot de behoefte om beleid te formuleren waarin de organisatie bepaalt onder welke voorwaarden zij bereid is om haar processen en systemen in de cloud onder te brengen. Een tweede stap hierin is dat zij vastlegt hoe zij dit beleid op naleving gaat controleren. Hoewel het bewustzijn dat deze controle nodig is groeit, is er nog een verdere cultuuromslag nodig binnen de organisatie om hier verder op te acteren. Gegevensbescherming wordt als een van de belangrijkste aspecten van clouddiensten ervaren. Het veilig koppelen van dataopslagsystemen is belangrijk voor de organisatie, mede omdat zij met ketenpartners samenwerkt. Verder geldt voor de organisatie dat zij over een sectorale referentie architectuur beschikt, met eigen normen en standaarden voor ICT-producten en -diensten. Dit sluit aan op wat er in literatuur is teruggevonden, namelijk: dat er sprake is van een gebrek aan standaardisatie tussen overheden en dat hun verscheidenheid aan eisen tot een beperkt hergebruik van bestaande cloud concepten en architecturen leidt. Ten slotte hebben respondenten aangegeven dat de organisatie bij datalekken, vanwege haar publieke taak, meer risico op imagoschade loopt dan bij private organisaties het geval is.

Het onderzoek vormt een verkenning op het gebied van cloud security, in de context van een overheidsorganisatie. Om te bepalen onder welke voorwaarden een overheidsorganisatie bereid is om haar processen en systemen onder te brengen in de cloud is het noodzakelijk dat zij hier beleid voor formuleert. Hierin dient ook te worden beschreven hoe de organisatie op naleving van het beleid gaat controleren. Wanneer het security beleid van een organisatie is vastgesteld kan een security architectuur, door middel van een set samenhangende modellen en principes, efficiënt en flexibel richting geven aan de invulling hiervan.

Omdat dit onderzoek zich op één organisatie heeft gericht, is aanvullend onderzoek noodzakelijk om vast te stellen in hoeverre andere overheidsorganisaties van een security architectuur gebruikmaken en wat de invloed van cloud computing hierop is.

Summary

Despite the increasing demand for IT services through cloud computing by governmental organizations, little is known about the influence of cloud computing on the design of their security architecture. This study focuses on a first step in determining the influence of cloud computing on the security architecture of governmental organizations, with the aim of providing a better foundation for security architecture decisions by governmental organizations. For this purpose, first a literature review was conducted and then qualitative data collected from a governmental organization by means of interviews and documentation on the subject within the context of the organization.

The results show that there is not always a formally established security architecture within a governmental organization. However, it is clear that cloud computing has an influence on the security of a governmental organization. Cloud computing influences security aspects, such as: legislation and regulations, manageability of processes and systems and data protection. Governmental organizations have to comply with additional government regulations regarding cloud security. As a result, the case organization experiences that it can be difficult for suppliers to meet the requirements set in agreements. With regard to the manageability of processes and systems, it experiences that due to cloud computing it has largely transferred its control and management options to cloud service providers. This leads to the need to formulate a policy in which the organization determines the conditions under which it is prepared to transfer its processes and systems to the cloud. A second step is to establish how this policy will be monitored for compliance. Although awareness of the need for control is growing, a further cultural shift is required within the organization in order to act upon it. Data protection is considered as one of the most important aspects of cloud services. The secure linking of data storage systems is important for the organization, partly because of its cooperation with chain partners. Furthermore, the organization has a sectoral reference architecture, with its own norms and standards for ICT products and services. This is in line with what was found in literature, namely: that there is a lack of standardization between governments and that their diversity of requirements leads to a limited reuse of existing cloud concepts and architectures. Lastly, respondents indicated that data breaches could lead to more reputational damage for governmental organizations, because of their public duty.

This study is an exploration of cloud security, in the context of a governmental organization. To determine the conditions under which a governmental organization is prepared to place its processes and systems in the cloud, a policy needs to be formulated. It should also describe how it will be monitored for compliance. Once an organization's security policy has been established, a security architecture can guide its implementation efficiently and flexibly through a set of coherent models and principles.

Because this study focuses on a single organization, additional research is needed to determine to what extent other governmental organizations use a security architecture and what influence cloud computing has on them.

Inhoudsopgave

1. Introductie

1.1. Achtergrond

Organisaties zijn steeds meer afhankelijk van cloud computing. Het functioneren van een organisatie hangt daarom sterk samen met de wijze waarop zij met cloud computing omgaat, waaronder de bijbehorende veiligheidsaspecten. Ondanks de toenemende vraag naar IT-diensten via cloud computing bij overheidsorganisaties, is er weinig bekend over de invloed van cloud computing op de vormgeving van hun security architectuur. Dit onderzoek richt zich op een eerste aanzet in het vaststellen van de invloed van cloud computing op de security architectuur van overheids-organisaties, met als doel om security architectuur-beslissingen van overheidsorganisaties beter te kunnen onderbouwen.

1.2. Gebiedsverkenning

Voor een beter begrip van dit onderzoek, beschrijft deze paragraaf wat er onder cloud computing, overheidsorganisaties en security architectuur wordt verstaan.

Cloud computing

In het boek *Cloud Computing for Enterprise Architectures* van Mahmood en Hill (2011, p. 3) wordt cloud computing kortweg geïntroduceerd als een algemene term die betrekking heeft op het leveren van gehoste services via internet. Het National Institute of Standards and Technology (NIST) gaat uit van de volgende definitie:

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (Mell & Grance, 2011). (p. 2)

Overheidsorganisaties

Er zijn diverse instellingen van de overheid en instellingen die onder de zeggenschap van de overheid vallen. Gezamenlijk vormen zij de publieke sector. Volgens Oosten (2014, p. 16) vallen alle publiek-rechtelijke organisaties en privaatrechtelijke organisaties die zich op publieke taken richten onder de publieke sector.

Security architectuur

In de IEEE Standaard 1471-2000 wordt architectuur gedefinieerd als “the fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution” (Institute of Electrical and Electronics Engineers, 2000, p.3).

Enterprise Architectuur (EA) helpt een organisatie bij het ontwikkelen en verwoorden van een visie voor het gebruik van informatietechnologie (IT) om haar strategische bedrijfsprioriteiten te ondersteunen (Tamm, Seddon, Shanks, Reynolds & Frampton, 2015; Ross, Weill & Robertson, 2006, p. 9). Shanks, Gloet, Asadi Someh, Frampton en Tamm (2018) stellen het volgende: “Enterprise Architecture (EA) defines the current and desirable future states of an organization’s processes,

capabilities, application systems, data, and IT infrastructure and provides a roadmap for achieving this target from the current state". (p. 139)

EA vormt de basisarchitectuur voor een organisatie en kan subarchitecturen bevatten zoals een business architectuur, application architectuur, data architectuur, technical architectuur en een security architectuur (Mahmood & Hill, 2011, pp. 14, 198). Dit onderzoek beperkt zich in scope op de security architectuur.

1.3. Probleemstelling, motivatie en relevantie

Bij cloud computing hebben overheidsorganisaties vaak onvoldoende zicht op welke invloed dit type afname van IT-diensten heeft op haar security architectuur. Ook vanuit de literatuur is er geen eenduidig theoretisch kader dat aangeeft hoe bepaald kan worden wat de invloed is van cloud computing op de security architectuur van overheidsorganisaties (Baheer, Lamas & Sousa, 2020; Hussain, Fatima, Saeed, Raza & Shahzad, 2017). Hierdoor is het lastig voor overheidsorganisaties om vast te stellen wat de impact van cloud computing is op het gebied van security en hoe hun security architectuur hierop kan worden vormgegeven. In de vormgeving van hun security architectuur geldt voor overheidsorganisaties dat op een aantal veiligheidsaspecten, zoals naleving van wet- en regelgeving, extra nadruk ligt. Daarnaast bezitten overheidsorganisaties een publieke functie waardoor het belang groot is dat zij op betrouwbare wijze omgaan met de middelen en informatie waarover zij beschikken. Dit zijn redenen waarom juist overheidsorganisaties over veilige cloud architecturen zouden moeten beschikken en kennistoename over dit onderwerp noodzakelijk is. Ook draagt dit onderzoek bij aan het vergroten van de theoretische kennis omtrent dit onderwerp.

1.4. Opdrachtformulering

Dit afstudeeronderzoek richt zich op het vaststellen van de invloed die cloud computing heeft op de security architectuur van overheidsorganisaties. De hoofdvraag die hieruit voorkomt luidt als volgt:

> Op welke wijze en in welke mate heeft cloud computing invloed op de vormgeving van de security architectuur van overheidsorganisaties?

Om een antwoord te kunnen geven op deze hoofdvraag is het onderzoek verdeeld in drie deelvragen:

1. Welke security architecturen bestaan er voor overheidsorganisaties?
2. Welke veiligheidsaspecten zijn in het kader van cloud computing specifiek relevant voor overheidsorganisaties?
3. In welke mate heeft cloud computing invloed op de vormgeving van de security architectuur van overheidsorganisaties?

1.5. Aanpak in hoofdlijnen

In hoofdstuk twee zal het literatuuronderzoek worden besproken. Hoofdstuk drie beschrijft de onderzoeksmethodiek. Vervolgens wordt het vervolgonderzoek voorbereid en uitgevoerd. Het verloop van het onderzoek wordt in hoofdstuk vier beschreven, evenals de resultaten van het onderzoek. In hoofdstuk vijf worden de conclusie, discussie en aanbevelingen besproken.

2. Theoretisch kader

2.1. Onderzoeksaanpak

Het literatuuronderzoek wordt gebruikt om (wetenschappelijke) literatuur over security architecturen bij overheidsorganisaties, en de invloed van cloud computing op security architecturen bij overheidsorganisaties, te onderzoeken. Doel is om hiermee de onderzoeksvragen te beantwoorden.

2.2. Uitvoering

Voor het literatuuronderzoek is gebruikgemaakt van de onlinebibliotheek van de Open Universiteit en Google Scholar.

Een voordeel in het gebruik van de onlinebibliotheek van de Open Universiteit is dat er makkelijk kan worden vastgesteld of de literatuur peer-reviewed is. Voor literatuur die gevonden is via Google Scholar is dit onderscheid niet helder, daarom zijn de titels van relevante artikelen die via deze zoekmachine zijn gevonden, ingevoerd in de onlinebibliotheek van de Open Universiteit, om zo van een aantal bronnen alsnog vast te kunnen stellen of zij peer-reviewed zijn.

Om het aantal gevonden hits terug te dringen is de invoer voor de parameter publicatiedatum soms verder beperkt. Wanneer er sprake was van weinig hits, is deze soms verruimd. Wanneer er een relevante titel gevonden werd, werd het abstract gelezen om te bepalen of de publicatie moest worden bewaard. Van de verzamelde, bewaarde publicaties is de inhoud verder bekeken om te bepalen of deze bruikbaar zijn voor het beantwoorden van de onderzoeksvragen.

Een andere zoekstrategie die is gebruikt in dit onderzoek is om vanuit de referentielijst van reeds gevonden publicaties naar andere publicaties te zoeken. Andersom, is er vanuit gevonden publicaties bekeken in welke andere publicaties deze als referentie zijn opgenomen.

Omdat er weinig peer-reviewed literatuur te vinden is over de relatie tussen cloud computing en security architectuur bij overheidsorganisaties, is er ook gezocht naar bronnen die niet peer-reviewed zijn. Zo is er bijvoorbeeld gebruikgemaakt van overheidsbronnen zoals rapporten en online artikelen. Deze secundaire bronnen helpen om een completer beeld te verkrijgen van het onderwerp (Saunders, Lewis & Thornhill, 2016, pp. 183, 316; Hakim, 2000, p. 49).

In de onderstaande tabel worden de voornaamste zoektermen vermeld die voor dit onderzoek zijn gebruikt. Meer details van de uitgevoerde query's zijn te vinden in Bijlage 1.

Tabel 1 - Zoektermen

Combinaties gebruikte zoektermen	Gebruikte resultaten	Peer-reviewed
security architecture AND cloud computing AND government	3	2
cloud security architecture AND government	1	0
IT security architecture AND cloud computing AND government	2	1
IT outsourcing AND government AND cloud security	0	0
compliance AND cloud computing AND government	3	3

2.3. Resultaten en conclusies

Deze paragraaf geeft op basis van het literatuuronderzoek, voor zover mogelijk, antwoord op de deelvragen.

Deelvraag 1: Welke security architecturen bestaan er voor overheidsorganisaties?

Het literatuuronderzoek levert zeer beperkt informatie op over welke security architecturen er bestaan voor overheidsorganisaties, zowel in het algemeen als specifiek in relatie tot cloud computing.

Twee voorbeelden van security architecturen die worden genoemd zijn de Open Security Architecture (OSA) en de NIST Cloud Computing Security Reference Architecture (NCC-SRA). Het Nationaal Cyber Security Centrum (NCSC, 2012) licht in haar whitepaper *Cloud computing & security* de OSA als cloud security referentie architectuur toe omdat dit raamwerk vanuit het oogpunt van security is opgesteld en een specifieke uitwerking beschrijft voor cloud computing. De NCC-SRA is ontwikkeld door het NIST, als standaard voor Amerikaanse overheidsorganisaties (Caballero, 2020, p. 456; Fernandez, Monge & Hashizume, 2016).

Er is een grote verscheidenheid aan overheidseisen en certificeringen waaraan een cloudoplossing moet voldoen voor deze voor overheidsgegevens mag worden gebruikt. Als de cloudoplossing een kwestie van nationale veiligheid wordt, zal elke regering onafhankelijkheid en strakke controle over haar gegevens willen behouden. Daarom is het onwaarschijnlijk dat regeringen in de nabije toekomst overeenstemming zullen bereiken over een internationale standaard voor dergelijke cloudsystemen (Ali, Shrestha, Chatfield & Murray, 2020; Herre, 2020, pp. 396, 405-406). Het gebrek aan standaardisatie tussen overheden en hun eisen leidt tot een beperkt hergebruik van bestaande cloud concepten en architecturen van de overheid. Elke cloudimplementatie moet opnieuw worden gecreëerd voor de verschillende landen en regio's om aan de lokale compliancebehoeften te kunnen voldoen (Herre, 2020, p. 405). Caballero (2020, p. 457) stelt dat de meest geavanceerde en veilige cloudarchitecturen voorzien in de volgende zaken:

Tabel 2 - Securityvereisten meest geavanceerde en veilige cloudarchitecturen

1	Veilige scheiding van tenant data en compute resources wordt in de hoogst mogelijke mate geïmplementeerd.
2	Service assurance-level agreements zijn in overeenstemming met het hoogste securityniveau dat intern is vastgesteld op basis van de classificatie van gegevens.
3	Security en compliancevereisten zijn gelijk aan of overtreffen de eisen die binnen de interne IT-organisatie worden aangehouden.
4	Beschikbaarheid en gegevensbescherming worden gemaximaliseerd met elk redelijk controlemechanisme dat in overeenstemming is met de gevoeligheid van de gegevens die moeten worden verwerkt.
5	Tenantbeheer en controle zijn vastgelegd in duidelijke en compromisloze methoden, met consequenties wanneer hier een afwijking in optreedt.
6	Het beheer en de controle van de cloud serviceprovider wordt geminimaliseerd en een intern team van de cloud customer heeft volledig inzicht in alle acties van de provider.

De NCC-SRA biedt voldoende handvatten voor de inrichting van een security architectuur die voldoet aan de door Caballero (2020, p. 457) genoemde voorwaarden en zou bijvoorbeeld kunnen worden gebruikt voor de implementatie van een IaaS-omgeving die voldoet aan de overheidsnormen van het

NIST en gegevens van federale overheden bevat (Caballero, 2020, p. 456). De OSA biedt een uitgebreid overzicht van securitycomponenten, die ten grondslag liggen aan beslissingen die een rol spelen bij het ontwerpen van een effectieve security architectuur, en mede zijn gebaseerd op standaarden zoals NIST 800-53 revisie 2, ISO17799, PCI-DSS versie 2.0 en COBIT 4.1 (https:// www.opensecurity architecture.org/cms/library/0802control-catalogue/256-control-mapping). Hier kan echter vooral goed gebruik van worden gemaakt wanneer een security architectuur al is ontworpen.

Deelvraag 2: Welke veiligheidsaspecten zijn specifiek relevant in het kader van cloud computing voor overheidsorganisaties?

Security kent een aantal deelaspecten, namelijk: naleving van wet- en regelgeving, beheersbaarheid van processen en systemen, gegevensbescherming, relatie tot de leverancier, beschikbaarheid van de clouddienst, beheer van gebruikers, beheer van incidenten, beheer van wijzigingen, back-up en recovery en transparantie (NCSC, 2012). Vanwege het korte tijdsbestek voor dit onderzoek is er gekozen voor het belichten van de volgende drie veiligheidsaspecten:

1. naleving van wet- en regelgeving;
2. beheersbaarheid van processen en systemen;
3. gegevensbescherming.

Naleving van wet- en regelgeving en gegevensbescherming zijn specifiek relevant omdat er een grote verscheidenheid aan overheidseisen en certificeringen is waaraan een cloudoplossing moet voldoen voor deze voor overheidsgegevens mag worden gebruikt. Verder bezitten overheids-organisaties een publieke functie waardoor het belang groot is dat zij op betrouwbare wijze omgaan met de middelen en informatie waarover zij beschikken. Tevens brengt het uitbesteden van activiteiten als systeem- en serverbeheer, datawarehousing en gegevensverwerking spionagerisico's met zich mee (NCSC, 2012). Dit laatste vormt de aanleiding om ook het veiligheidsaspect beheers-baarheid van processen en systemen te belichten.

Naleving van wet- en regelgeving

Het gebruik van IT door overheidsorganisaties vormt een risico vanwege talloze kwetsbaarheden in IT-systemen. Deze kwetsbaarheden zijn potentiële doelwitten voor criminele activiteiten zoals digitale spionage, beïnvloeding en sabotage. Als gevolg hiervan bestaan er diverse overheidsvoor-schriften voor de bescherming van IT-systemen waarvan overheidsorganisaties afhankelijk zijn. Hoewel alle IT-systemen een risico vormen voor hun belanghebbenden, kunnen cloudgebaseerde informatiesystemen een nog hoger risico vormen omdat ze relatief nieuwere technologieën bevatten en doorgaans aan een bredere reeks potentiële bedreigingen worden blootgesteld. Om deze reden zijn er aanvullende overheidsvoorschriften ontwikkeld die zich richten op de beveiliging van cloudgebaseerde informatiesystemen (https://www.aivd.nl/onderwerpen/cyberdreiging; Gupta, 2020, pp. 387-388; Brumă, 2020).

Beheersbaarheid van processen en systemen

Wanneer een overheidsorganisatie gebruikmaakt van clouddiensten staat zij op een aantal onderdelen haar controle en beheersmogelijkheden af aan de cloud serviceprovider. Voor het uitbesteden heeft zij daarom niet enkel vertrouwen nodig in de technologie van cloud computing, maar ook in de cloud serviceprovider als partij die op een aantal onderdelen de controle zal overnemen (Khan & Malluhi, 2010; Costa & Bijlsma-Frankema, 2007; Rashidi & Movahhedinia, 2012). Om te bepalen onder welke voorwaarden een overheidsorganisatie bereid is om haar

processen en systemen onder te brengen in de cloud is het noodzakelijk dat zij hier beleid voor formuleert. Dit beleid dient ook te beschrijven hoe de organisatie dit beleid op naleving gaat controleren. Op deze wijze kan een overheidsorganisatie haar verlies op het gebied van de beheersbaarheid van haar processen en systemen zoveel mogelijk beperken en monitoren of de cloud serviceprovider de voorgeschreven normen naleeft (NCSC, 2012; Ferrin, Bligh & Kohles, 2007; Bijlsma-Frankema & Costa, 2005).

Gegevensbescherming

De bescherming van gegevens in de cloud is een van de belangrijkste aspecten van clouddiensten (Ibiricu & van der Made, 2020). De toenemende verwevenheid van computersystemen en het koppelen van dataopslagsystemen maakt de gevoelige gegevens in systemen kwetsbaar. Daarnaast blijven organisaties zelf verantwoordelijk voor de beveiliging van gegevens, zelfs wanneer deze gegevens bij een cloud serviceprovider zijn ondergebracht (NCSC, 2012; Rîndaşu, 2018). Een overheidsorganisatie dient te bepalen welke van haar gegevens het gevoeligst zijn (dataclassificatie), hoe deze gegevens worden benaderd, hoe activiteiten binnen de omgeving kunnen worden gemonitord en hoe er snel kan worden gereageerd op eventuele afwijkingen (Kuner, Cate, Millard, Svantesson & Lynskey, 2015; Commission Nationale de l'Informatique et des Libertés, 2018; Brumă, 2020).

Deelvraag 3: In welke mate heeft cloud computing aantoonbaar invloed op de vormgeving van de security architectuur van overheidsorganisaties?

Een concreet antwoord op deze deelvraag is in de literatuur niet teruggevonden.

Om de invloed van cloud computing op de vormgeving van de security architectuur van overheidsorganisaties vast te stellen kan in kaart worden gebracht welke wijzigingen er plaatsvinden in de securitybehoeften van overheidsorganisaties, wanneer zij de beslissing maken om hun services en gegevens naar een cloudomgeving te migreren, en welke veiligheidsaspecten als gevolg hiervan in hun security architectuur worden geïmplementeerd (Koo, Oh, Lee & Kim, 2020; Sen, 2015, pp. 1-2, 7-25, 31-34; Hussain et al., 2017; Pohlmann, 2017). Voor een succesvolle adoptie van een cloud-gebaseerde oplossing dient de cloud customer in staat te zijn om de cloudspecifieke kenmerken van het systeem, de architectonische componenten en het implementatiemodel voor elk type dienst, en de rol van de cloudactoren bij het tot stand brengen van een veilig cloud-ecosysteem goed te begrijpen (Iorga & Karmel, 2020, p. 89).

2.4. Doel van het vervolgonderzoek

Dit onderzoek richt zich op een eerste aanzet in het vaststellen van de invloed van cloud computing op de security architectuur van overheidsorganisaties. Een toename in kennis over dit onderwerp biedt overheidsorganisaties de mogelijkheid om beslissingen ten aanzien van de vormgeving van hun security architectuur beter te onderbouwen. Het vervolgonderzoek wordt uitgevoerd bij een overheidsorganisatie en heeft als doel om verdere gegevens te verzamelen over het onderwerp en deze te analyseren.

3. Methodologie

3.1. Conceptueel ontwerp: keuze van onderzoeksmethoden

Zoals in het voorgaande hoofdstuk reeds is geconcludeerd is er weinig literatuur over het onderzoeksonderwerp te vinden. Het vervolgonderzoek richt zich daarom op het verdiepen van de kennis over de mate waarin cloud computing invloed heeft op de security architectuur van overheidsorganisaties en is verkennend van aard (Saunders et al., 2016, pp. 174-176).

Omdat er weinig literatuur over het onderzoeksonderwerp te vinden is, maakt dit het lastig om op basis van de literatuur vooraf een hypothese op te stellen die door middel van kwantitatief onderzoek kan worden getest. In het onderzoek zullen daarom kwalitatieve gegevens worden verzameld voor het genereren van theoretische inzichten. Het onderzoek heeft hiermee een inductieve benadering (Saunders et al., 2016, pp. 144-150, 166-170, 568-571). Voor verdiepend onderzoek, binnen een kort tijdsbestek, vormt een casestudy een geschikte onderzoeksmethode en kan deze methode worden aangevuld met archief- en documentair onderzoek (Yin, 2018, p. 34, 46, 49; Eisenhardt, 1989; Eisenhardt & Graebner, 2007; Dubois & Gadde, 2002; Ridder, Hoon & McCandless Baluch, 2014; Saunders et al., 2016, pp. 183-184, 187, 316; Hakim, 2000, p. 49).

3.2. Technisch ontwerp: uitwerking van de methode

Yin (2018, p. 62) onderscheidt vier casestudy strategieën, gebaseerd op twee dimensies:

1. enkelvoudige case versus meervoudige cases;
2. holistische case versus ingebedde case.

Omdat het onderzoek verkennend is van aard en er sprake is van een kort tijdsbestek voor het onderzoek wordt hier gekozen voor een enkelvoudige case. Als case wordt een representatieve gebruiker van cloud computing in de publieke sector onderzocht. Criteria om te bepalen of een gebruiker representatief is zijn dat het gaat om een organisatie die valt onder de publieke sector en waar gebruik wordt gemaakt van cloud computing en/of zij cloud services wil gaan afnemen en de organisatie hierdoor is of wordt geconfronteerd met veiligheidsaspecten die hierbij een rol spelen. Het onderzoek wordt holistisch uitgevoerd, wat betekent dat het onderzoek zich richt op de organisatie als geheel (Saunders et al., 2016, pp. 186-187).

Voor dit onderzoek worden gegevens middels interviews verzameld en worden deze eventueel aangevuld met documentatie over het onderwerp binnen de context van de organisatie. Interviews bieden met betrekking tot de onderzoeksvraag de gelegenheid om het fenomeen verder te verkennen. Eventuele, aangeleverde documentatie wordt beoordeeld en gebruikt om datatriangulatie toe te passen (Saunders et al., 2016, pp. 168, 175, 183, 207, 316, 392-393, 402; Hakim, 2000, pp. 47, 49).

De interviews zullen individueel worden afgenomen. Groepsinterviews zijn minder geschikt voor dit onderzoek omdat het aantal personen binnen de organisatie, dat over kennis beschikt ten aanzien van het onderzoeksonderwerp, beperkt is (<10). Respondenten worden geselecteerd op basis van hun expertise en betrokkenheid bij de security van de organisatie (Saunders et al., 2016, pp. 416-421).

De interviews die zullen worden afgenomen zijn, vanwege hun verkennend karakter, semigestructureerd en hebben een gemiddelde duur van een uur. Een volledig ongestructureerd

interview valt af omdat dit type interview te weinig structuur biedt om antwoorden te krijgen op de onderzoeksvragen. Een volledig gestructureerd interview is niet geschikt omdat de resultaten van tevoren niet zijn in te schatten in verband met de verkennende aard van het onderzoek. Er is gekozen voor interviews met een gemiddelde duur van een uur zodat respondenten van tevoren een beeld hebben van waar zij ongeveer op kunnen rekenen qua benodigde tijd en concentratie. Na afloop worden de interviews getranscribeerd (Saunders et al., 2016, pp. 235, 390-396, 572; Powney & Watts, 1987, p. 17).

3.3. Gegevensanalyse

De verzamelde gegevens worden op thematische wijze geanalyseerd. Thematische analyse biedt een systematische en tegelijk flexibele benadering om kwalitatieve gegevens te analyseren. Doel is om thema's en relaties tussen thema's te identificeren in de verzamelde gegevens, die gerelateerd zijn aan de onderzoeksvraag (Saunders et al., 2016, pp. 579-580, 587; Braun & Clarke, 2006).

Om structuur aan te brengen in de verzamelde gegevens zullen deze worden gecodeerd. Het codeerproces start met open coderen. Dit houdt in dat een document geheel wordt doorgelezen en aan relevante tekstfragmenten labels worden gekoppeld. Deze labels geven per tekstfragment aan wat het thema daarvan is. Vervolgens wordt er gebruikgemaakt van axiaal coderen. Hierbij worden labels met elkaar vergeleken. Codes kunnen worden gesplitst, samengesteld en opnieuw worden benoemd. Dit wordt gedaan door inhoudelijk te bekijken wat er over een onderwerp is gezegd of geschreven en hoe dat zich verhoudt ten opzichte van de onderzoeksvragen. Het streven is om zo een meer uniforme en valide codering te verkrijgen. Ook kunnen aan de hand van deze codering mogelijk verschillende groepen worden geïdentificeerd (Saunders et al., 2016, pp. 194, 580-585, 596-599).

Analyse vindt zowel tijdens als na de gegevenscollectie plaats. Terwijl gegevens worden verzameld kunnen belangrijke thema's, patronen en relaties worden herkend. Dit kan er mogelijk toe leiden dat bestaande gegevens opnieuw moeten worden gecategoriseerd om te zien of dezelfde thema's, patronen en relaties ook daarin kunnen worden herkend. Nadat de thema's en relaties tussen de thema's zijn gedefinieerd worden deze verder beoordeeld en verfijnd (Saunders et al., 2016, pp. 168, 571, 583; Corbin & Strauss, 2014, pp. 9-10, 58, 86-87).

3.4. Reflectie t.a.v. validiteit, betrouwbaarheid en ethische aspecten

<u>Interne validiteit</u>

Om de interne validiteit van dit onderzoek te verhogen ontvangen de respondenten voorafgaand aan de interviews een toelichting over het doel van het onderzoek en wat er van hun wordt verwacht (zie Bijlage 2). Dit biedt hun de mogelijkheid om zich in het onderwerp te verdiepen en daarmee de vragen die zij zullen krijgen beter te kunnen plaatsen en mogelijk meer complete antwoorden te kunnen geven. De interviews worden gehouden aan de hand van een protocol (zie Bijlage 3). Hiermee neemt het risico af op een bias bij zowel de respondenten als bij de onderzoeker. Nadat de interviews hebben plaatsgevonden zullen aan de hand van opnamen en aantekeningen zo snel mogelijk verslagen worden opgesteld. Op deze wijze zitten de waarnemingen nog vers in het geheugen van de onderzoeker en wordt het risico op misinterpretatie of onvolledigheid verminderd. Een tweede informatiebron, zoals in dit onderzoek geldt voor documentatie, biedt het voordeel dat

deze kan worden gebruikt voor datatriangulatie en zo de validiteit van het onderzoek kan verhogen. Vraag is wel in hoeverre documentatie over het onderwerp aanwezig is en of deze relevante informatie bevat. Als secundaire bron is de documentatie immers met een ander doel opgesteld dan om informatie te verschaffen voor het onderzoek. Om deze reden zal eventuele, aangeleverde documentatie kritisch worden beoordeeld om te bepalen of deze kan worden gebruikt voor datatriangulatie (Saunders et al., 2016, pp. 202-204, 206-207, 234-235, 237-238, 252-253, 335, 402, 572; Hakim, 2000, pp. 47, 49).

Externe validiteit

Omdat dit onderzoek wordt uitgevoerd bij één overheidsorganisatie is het onderzoeksresultaat niet zomaar te generaliseren naar de publieke sector in het algemeen. De externe validiteit van het onderzoek wordt verhoogd door de beschrijving van de onderzoeksvragen, het ontwerp, de context, bevindingen en resulterende interpretaties. Op deze wijze kan de kwaliteit van het onderzoeks-ontwerp worden beoordeeld (Saunders et al., 2016, pp. 202-206, 398-400; Eisenhardt, 1989).

Constructvaliditeit

Ten behoeve van de constructvaliditeit zijn de interviewvragen opgesteld op basis van de onderzoeksvragen en de resultaten van het literatuuronderzoek. Bij het formeren van de vragen is er tevens op gelet dat zij begrijpelijk moeten zijn voor de respondenten (Saunders et al., 2016, pp. 202, 449-453, 462-463, 466-467; Gibbert & Ruigrok, 2010).

Betrouwbaarheid

Bij het afnemen van de interviews wordt rekening gehouden met het risico op vooringenomenheid, mede omdat de onderzoeker bekend is met de organisatie en respondenten, en zich ervan bewust is dat gegevens zo objectief mogelijk dienen te worden verzameld. De interviews worden face-to-face afgenomen op een locatie van de organisatie waar de respondenten bekend mee zijn, zodat zij zich gedurende het interview in een vertrouwde omgeving bevinden en zich daardoor mogelijk gemakkelijker open kunnen stellen voor het interview. Om te voorkomen dat de respondenten minder durven te zeggen dan ze zouden willen, is toegezegd dat de resultaten anoniem zijn. Kwalitatief onderzoek is niet noodzakelijkerwijs bedoeld om te worden herhaald, omdat het de interpretaties weerspiegelt van deelnemers in een bepaalde omgeving op het moment dat het onderzoek wordt uitgevoerd. Een uitgebreide beschrijving van de onderzoeksvragen, het ontwerp, de context, bevindingen en resulterende interpretaties kan anderen wel helpen om een soortgelijk onderzoek te repliceren (Saunders et al., 2016, pp. 202-203, 205, 208, 235-239, 243, 255, 397, 410-413, 572; Eisenhardt, 1989).

Ethische aspecten

Om de ethiek van dit onderzoek te waarborgen geldt dat de respondenten vrijwillig deelnemen aan het onderzoek en op de hoogte zijn van hun vrijheid om zich op elk moment uit het onderzoek terug te trekken. Ook bezitten zij de vrijheid om af te zien van een face-to-face interview en kunnen zij kiezen voor een elektronisch interview. Gebruikte en verwerkte gegevens zijn niet direct te herleiden naar de respondenten en de organisatie. Opnamen van de interviews zijn enkel toegankelijk voor de onderzoeker. Na het onderzoek kunnen de opnamen worden vernietigd, wanneer hier expliciet toe is verzocht door de respondenten. Gedurende het onderzoek wordt er gewerkt volgens de Wet Bescherming Persoonsgegevens (AVG) en de Nederlandse Gedragscode Wetenschapsbeoefening (Saunders et al., 2016, pp. 55, 239-240, 243-246, 249-264; Vereniging van Universiteiten, 2014).

4. Resultaten

4.1. Uitvoering

Gedurende het onderzoek heeft er verschillende keren contact plaatsgevonden met de leidinggevende van het team, waar de respondenten deel van uitmaken, en een specialist op het gebied van security. Met hun is afgestemd welke personen het beste konden worden benaderd voor het onderzoek. De bereidwilligheid om deel te nemen aan het onderzoek was groot. Met betrekking tot twee personen bleek deelname aan het onderzoek qua planning niet haalbaar te zijn. In totaal zijn er vier personen geïnterviewd, gedurende de maanden mei en juni 2021. Drie interviews hebben op locatie plaatsgevonden en één, op verzoek van de respondent, via Microsoft Teams.

Alle interviews zijn zo snel mogelijk getranscribeerd. Daarbij is gebruikgemaakt van de online tool Amberscript. De resultaten hiervan zijn handmatig doorlopen en verbeterd. Soms was er sprake van vertrouwelijke informatie en is dit niet opgenomen in de transcripten. Verwijzingen naar personen en de organisatie zijn geanonimiseerd, dit geldt eveneens voor sommige verwijzingen naar applicaties en andere organisaties. Ook is bij het noemen van documentatie erop gelet dat deze niet direct naar de organisatie te herleiden mag zijn. Twee respondenten gaven tijdens het interview expliciet aan dat bepaalde informatie die zij gaven vertrouwelijk is. Eén respondent wil dat de opname van het interview wordt vernietigd na afronding van het onderzoek. Twee respondenten hebben aanvullend documentatie aangeleverd.

Voor het coderen van de transcripten en aangeleverde documentatie is Computer Assisted Qualitative Data Analysis Software (CAQDAS), namelijk ATLAS.ti, gebruikt. Het gebruik van CAQDAS kan de continuïteit in de analyse bevorderen en daarnaast zowel de transparantie als de methodologische nauwkeurigheid vergroten (Saunders, 2016, pp. 615-618). Het resultaat van de gegevensanalyse is te vinden in Bijlage 4.

In het vervolg van dit verslag wordt er, om de leesbaarheid van de tekst te vergroten, bij meer dan drie bronverwijzingen en links gebruikgemaakt van voetnoten. Alle interviewtekstfragmenten waarnaar wordt verwezen hebben een ID-nummer en zijn terug te vinden in Bijlage 5.

4.2. Resultaten deelvragen

Deelvraag 1: Welke security architecturen bestaan er voor overheidsorganisaties?

Uit het onderzoek blijkt dat de organisatie niet over een formeel vastgelegde security architectuur beschikt (ID147). Een van de respondenten geeft aan dat de Baseline Informatiebeveiliging Overheid (BIO, 2020) als “een soort framework” voor security kan worden gezien, dit is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen[1]. De BIO beschrijft de invulling van de NEN-ISO/IEC normen 27001 en 27002 voor de overheid. Het Forum Standaardisatie, een adviescommissie voor de publieke sector voor het gebruik van ICT-standaarden, heeft deze normen opgenomen in een lijst met verplichte standaarden voor de publieke sector (ID205, 208). De BIO ziet informatie-beveiliging als een belangrijk kwaliteitsaspect van de informatievoorziening van de overheid en als een proces waarbij steeds een Plan-Do-Check-Act cyclus dient te worden doorlopen (ID206). Risicomanagement vormt een belangrijk onderdeel in het proces en wordt toegepast om tot de juiste beveiliging van informatie en informatiesystemen te komen binnen de context van de

[1] ID69, 208; https://www. digitaleoverheid.nl/overzicht-van-alle-onderwerpen/informatieveiligheid/kaders-voor informatieveiligheid/baseline-informatiebeveiliging-overheid/

bedrijfsdoelstellingen (ID209). Aanvullend op de BIO zijn er nog enkele andere documenten die de organisatie ondersteunen in het vaststellen van haar securitybeleid. Een daarvan is een publicatie van het onderdeel Realisatie van de Vereniging van Nederlandse Gemeenten (VNG), namelijk: de Gemeentelijke Inkoopvoorwaarden bij IT (GIBIT, 2020). Deze publicatie is opgesteld om de uniformering en professionalisering van het inkoopbeleid bij gemeenten te bevorderen. De GIBIT kan worden gebruikt bij IT-contracten (ID83, 146, 238). Een tweede document is de Handreiking Inkoop Clouddiensten (2019), opgesteld door de Informatiebeveiligingsdienst voor gemeenten (IBD), ook onderdeel van het VNG. Deze handreiking is een nadere uitwerking van de BIO voor gemeenten. Naast deze handreiking biedt de IBD nog vele andere operationele kennisproducten aan die aansluiten op de BIO (ID146). Een derde document bevat de Veiligheidsregio ICT-kwaliteitsnormen van het Instituut Fysieke Veiligheid (IFV, 2021), bedoeld als addendum bij de GIBIT (2020). Bij gemeenten geldt dat onder de GIBIT-voorwaarden geleverde producten of diensten moeten voldoen aan de Gemeentelijke ICT-kwaliteitsnormen (2021). De organisatie vormt echter een decentrale overheid waarop een andere sectorale referentie architectuur van toepassing is, met eigen normen en standaarden voor IT-producten en diensten. Om deze reden zijn bij deze organisatie, een Veiligheidsregio, niet de Gemeentelijke ICT-kwaliteitsnormen van toepassing, maar de Veiligheids-regio ICT-kwaliteitsnormen (IFV, 2021; ID238). Naast de bovengenoemde documentatie beschikt de organisatie over een document dat een aantal richtlijnen en randvoorwaarden van de organisatie zelf beschrijft voor de aanschaf van nieuwe IT-systemen (ID82).

Veiligheidsregio Referentie Architectuur

In het tweede hoofdstuk van de Veiligheidsregio ICT-kwaliteitsnormen (IFV, 2021, p. 8) staat vermeld dat voor de ICT-prestatie de Veiligheidsregio Referentie Architectuur (VeRA) als kader geldt. VeRA beschrijft de inrichting van de gewenste informatiehuishouding van Veiligheidsregio's en de aansluiting daarvan op de omgeving.[2]

In zowel de ICT-kwaliteitsnormen als in VeRA wordt specifiek aandacht besteed aan gegevens-uitwisseling. Mede omdat Veiligheidsregio's veel samenwerken met ketenpartners is gegevens-uitwisseling, en daarmee veilige, betrouwbare koppelingen, van groot belang. Dit onderwerp werd ook door twee respondenten in de interviews genoemd.[3]

Kenmerken meest geavanceerde en veilige cloudarchitecturen

Gedurende de interviews is geïnventariseerd in hoeverre de respondenten de zes punten herkennen die Caballero (2020, p. 456; Tabel 2) als kenmerken voor de meest geavanceerde en veilige cloudarchitecturen benoemd. Het wisselt per punt in welke mate dit wordt herkend als iets waar de organisatie rekening mee houdt. Het enige punt dat volledig wordt onderschreven is punt 3 (ID21, 120).

De punten 2 en 4 worden als relevante onderwerpen herkend, maar de organisatie blijkt op dit gebied nog niet voldoende te hebben vastgelegd.[4] Twee respondenten geven aan dat er op het gebied van security nog geen duidelijk beeld is van wat er werkelijk nodig is en wat er qua veiligheidsmaatregelen moet worden gevraagd.[5] Een respondent geeft aan dat er bij de inkoop van nieuwe informatiesystemen door het team Inkoop en Contractmanagement moet worden gekeken of er een risicoanalyse moet worden uitgevoerd op het gebied van privacy en informatieveiligheid. Er is een basisrisicoanalyse en wanneer nodig een diepgaandere risicoanalyse. Ook beschikt dit team

[2] ID239-240, 243; https://www.veraonline.nl/index.php/ArchiMate_en_modelleerafspraken
[3] ID56, 101, 138, 145, 241; https://www.veraonline.nl/index.php/Visie_en_ principes; https://www.veraonline.nl/index.php/ Gegevensuitwisseling;
[4] ID19, 48, 59, 61-62, 147, 183
[5] ID17, 22-23, 31-32, 35, 45, 47, 50, 65

over de GIBIT.[6] Endpoint Management en Identity en Access Management worden toegepast.[7] Kritische systemen krijgen wat meer aandacht, hier worden bijvoorbeeld jaarlijks pentesten voor uitgevoerd en deze moeten altijd beschikbaar zijn (ID96, 118, 131). Application en Interface Security wordt herkend als een belangrijk punt, maar dit is nog onvoldoende op orde.[8] Het Problem Management is nog niet voor alle systemen goed ingericht.[9] Business Continuity Management heeft enigszins de aandacht[10], in het bijzonder als het gaat om eventuele uitval van servers. Ook moet de verbinding tussen een systeem met andere systemen kunnen worden verbroken, wanneer deze niet veilig blijkt te zijn. Interoperability en Portability hebben enigszins de aandacht (ID114, 241). Vendor lock-in krijgt weinig aandacht (ID40, 164, 168). Een respondent geeft aan dat er met de, op dit moment lopende, migratie van documenten vanaf de netwerkschijf naar Microsoft SharePoint / Teams beperkt aandacht is voor de vertrouwelijkheid van documenten (ID175). Dit komt mede door de grote hoeveelheid informatie die moet worden gemigreerd en het tijdsbestek voor de migratie.

De respondenten vonden het over het algemeen lastig om iets te zeggen over de punten 1 en 6 (ID61-62). Twee respondenten geven aan dat er bij aanbestedingen vragen over worden gesteld aan leveranciers (ID63, 113, 246). Een respondent geeft aan dat leveranciers op verschillende omgevingen zitten, zodat ze niet zomaar bij data van de organisatie kunnen (ID112). Logging speelt een rol, welke typen logging dat precies zijn is niet geheel helder.[11] Audits gebeuren nagenoeg niet. Contractueel wordt de mogelijkheid hiertoe wel vastgelegd.[12] Een respondent geeft aan het fijn te vinden wanneer de gehele security-inrichting jaarlijks door een derde, onafhankelijke partij zou worden nagelopen. Om zodoende hiervan te kunnen leren en meer zekerheid over de inrichting te hebben. Daarnaast kunnen auditrapporten als bewijs dienen voor het management van de organisatie.[13] Een andere respondent geeft aan dat er eigenlijk audits gehouden zouden moeten worden, maar dat deze prijzig zijn (ID95).

Punt 5 is meer herkenbaar. De organisatie is nog een beetje zoekende naar hoe zij dit het beste kan invullen. Dit geldt in het bijzonder voor haar eigen IaaS-omgeving, in mindere mate voor de infrastructuur van andere cloudoplossingen die zij afneemt (ID72). Volgens een respondent worden er vaak duidelijke afspraken gemaakt met leveranciers rondom beheer en change management. Er is een wijzigingscommissie binnen de organisatie aanwezig voor de grootste wijzigingen (ID122-123, 141). Wanneer het advies van de wijzigingscommissie echter niet wordt opgevolgd, of een wijziging niet wordt gemeld, is hier weinig controle op (ID124, 142-143). Twee respondenten geven aan dat zij vanwege een incident een keer meer hebben gezien in een tenant dan de bedoeling was (ID58, 174). Een respondent geeft aan dat een leverancier vrij makkelijk accounts aanmaakt, zonder goed overleg. Er zijn wel afspraken over, maar hier is onvoldoende controle op.[14]

Deelvraag 2: Welke veiligheidsaspecten zijn specifiek relevant in het kader van cloud computing voor overheidsorganisaties?

Naleving van wet- en regelgeving

Zoals reeds benoemd vormt de BIO (2020) het basisnormenkader voor informatiebeveiliging voor de organisatie. Nieuwe wetgeving kan ertoe leiden dat er aanpassingen in systemen moeten worden

[6] GIBIT, 2000; ID83-84; 146; 238
[7] ID149-150, 153, 155-156, 158, 167
[8] ID56, 86, 101, 138, 145
[9] ID32, 43, 50, 126
[10] ID104, 108-109, 114-115, 164-165, 203
[11] ID64, 125, 127-129, 178, 200, 247
[12] ID130, 132, 198, 201
[13] ID171, 179-180, 196
[14] ID170, 172, 176-177

aangebracht (ID49, 53). De respondenten noemen vaak de privacywetgeving als een belangrijke factor.[15] Verder certificeringen, normen, regels rondom informatie-uitwisseling.[16] Deze worden niet verder gespecificeerd. Twee respondenten geven aan dat de organisatie, omdat zij een overheidsorganisatie is, strengere eisen stelt aan leveranciers. Dit zou noodzakelijk zijn omdat de organisatie een voorbeeldfunctie vervult.[17] Met name kleinere partijen kunnen moeite hebben om aan deze eisen tegemoet te komen (ID15). In het sluiten van overeenkomsten blijkt het een uitdaging te zijn om zekerheid te verkrijgen over in welke rechtsgebieden de data wordt opgeslagen (ID88-90). Twee respondenten geven aan dat veel hostingpartijen met Amerikaanse bedrijven in zee zijn gegaan of een moederbedrijf in Amerika hebben.[18] Dit kan voor het team Inkoop en Contractmanagement leiden tot moeilijke afwegingen, waarin soms ook meespeelt dat het aanbod voor bepaalde systemen zeer beperkt kan zijn. In het vormen van inkoopadviezen kan meer duidelijkheid over beveiligingsniveaus en de hierbij passende veiligheidsmaatregelen helpend zijn (ID31-32, 35).

Beheersbaarheid van processen en systemen

Uit de interviews kwam duidelijk naar voren dat cloud computing een grote invloed heeft op de beheersbaarheid van processen en systemen. Eén reden daarvoor is de verbinding met het internet (ID6, 151-152). Hierdoor zijn zaken als Identity en Access Management en Endpoint Management extra belangrijk geworden (ID100, 149, 153). Een respondent geeft aan dat het gebruik van systemen die door veel meer organisaties gebruikt worden een risico kan vormen met betrekking tot cybercriminelen. Wanneer zij een zwak punt ontdekken in een systeem kunnen zij dit gebruiken om veel organisaties tegelijk aan te vallen en af te persen (ID154).

Het beeld dat initieel bestond bij de organisatie is dat cloud computing vooral de mogelijkheid biedt om ontzorgd te worden (ID24, 39, 97). Tot op bepaalde hoogte is dit nog steeds het geval, maar met name sinds de organisatie in de overgang zit van het afnemen van local virtual desktop infrastructures (VDIs) in combinatie met een aantal desktops as a service (DaaS) naar Microsoft Azure (IaaS) in combinatie met Microsoft 365 E3 (SaaS), groeit het bewustzijn van de eigen verantwoordelijkheid voor de cloud security van de organisatie (ID1, 30, 173). Voorheen hield de organisatie zich voornamelijk bezig met functioneel beheer voor SaaS-oplossingen, maar voor het beheer van een IaaS-oplossing is meer expertise nodig, ook op het gebied van security. Het besef dat cloud computing de eigen invloed op processen en systemen verkleint is duidelijk aanwezig.[19] Uit de interviews blijkt dat men binnen de organisatie nog zoekende is in hoe de eindverantwoordelijkheid hierin precies kan worden ingevuld en welke expertise hiervoor nodig is.[20] Bij twee respondenten is er een bepaald vertrouwen in leveranciers merkbaar, voornamelijk in grote partijen, en in het vastleggen van zaken door middel van contracten.[21] Tegelijk is er enige twijfel aanwezig of dit afdoende is.[22] Twee andere respondenten zien absoluut de noodzaak voor meer governance en expertise op het gebied van security. Volgens één van hun kun je bij cloud computing niet meer zomaar op leveranciers vertrouwen, gezien je als cloud customer beperkt zicht hebt op de maatregelen die zij nemen. Wanneer hier geen toezicht op wordt gehouden kun je als organisatie

[15] ID14, 87, 160, 244
[16] ID85-86, 163, 204
[17] ID25-26, 28, 134, 137
[18] ID11, 28, 161-162
[19] ID2, 13, 16-17, 36-37, 40, 54, 78-79, 91, 94, 157, 166
[20] ID73, 77, 80, 93, 98, 144, 194
[21] ID3, 7, 9, 38, 42, 57
[22] ID4-5, 8, 10

voor onverwachte, vervelende verrassingen komen te staan en dan ben je te laat met ingrijpen. Daarnaast ligt de eindverantwoordelijkheid doorgaans bij de organisatie zelf. De rol van de organisatie verandert naar die van regiehouder. De andere respondent geeft aan dat er qua IT en security strakkere richtlijnen noodzakelijk zijn omdat er anders te veel risico's bij komen kijken.[23] Er worden stappen gemaakt om de eigen inrichting qua security te verbeteren en de expertise te vergroten. Hiervoor wordt onder andere gebruikgemaakt van ondersteuning en advisering door leveranciers. Een kanttekening hierbij is dat deze partijen niet geheel onafhankelijk zijn in hun advies.[24] Het gebrek aan kennis binnen de organisatie kan leiden tot onduidelijkheid in de vraag richting leveranciers (ID181-183). Een factor die de vormgeving van meer governance kan bemoeilijken is de organisatiecultuur. Een respondent geeft aan dat de organisatie meer van het aanpakken dan van het noteren is (ID70). Een andere respondent geeft aan dat er een hands-on-mentaliteit in de organisatie heerst en medewerkers gewend zijn veel vrijheid te bezitten. Dit kan het vastleggen van zaken en beperken van vrijheden bemoeilijken (ID184).

Gegevensbescherming

Het veiligheidsaspect databeveiliging, of gegevensbescherming, werd vaak als eerste benoemd in de interviews (ID12, 46, 148). Een respondent geeft aan dat cloud computing op verschillende manieren invloed heeft op de gegevensbescherming en op waar data zich bevindt. Dit is namelijk niet enkel in je individuele systemen, op welke server dit draait en op welke locatie, maar ook op de koppelingen tussen systemen en welke informatie tussen systemen wordt overgeheveld (ID99). De risicoanalyse op het gebied van gegevensbescherming is uitgebreider geworden door cloud computing (ID103). Back-upbeleid en retentie spelen een rol op dit gebied (ID105-106). Twee respondenten geven aan dat de gegevensbescherming binnen de organisatie nog niet helemaal goed is geregeld (ID18, 60). Tegelijk is er het besef dat dit juist een belangrijk veiligheidsaspect is voor de organisatie. Een reden hiervoor is dat er gedeelde, kritieke systemen met andere overheidsorganisaties zijn, waarbij de beschikbaarheid van gegevens cruciaal is voor het verlenen van spoedeisende hulp en hier (bijzondere) persoonsgegevens bij worden verwerkt (ID139). Ook ervaren de respondenten dat de organisatie een zwaardere verantwoordelijkheid heeft op dit gebied richting burgers, vanwege haar publieke taak.[25] Een van de respondenten geeft aan dat je als overheidsorganisatie gegevens vastlegt vanuit een wettelijke taak en je daar extra zorgvuldig mee om dient te gaan. Burgers en bedrijven kiezen er vaak niet vrijwillig voor om hun gegevens door de organisatie op te laten slaan. Daarnaast word je als overheidsorganisatie (indirect) door hun betaald, via belastinggeld. En wanneer er sprake is van een datalek, hebben slachtoffers doorgaans niet de mogelijkheid om in zo'n situatie over te stappen naar een andere organisatie die zij meer vertrouwen (ID186-187, 191). Twee respondenten geven aan dat qua vertrouwen in overheidsorganisaties de zorg voor persoonsgegevens het gevoeligst ligt (ID27, 66). Een voordeel voor de organisatie is dat er voor haar als overheidsorganisatie, in het geval een datalek voorkomt, snel hulp voorhanden is (ID140).

Deelvraag 3: In welke mate heeft cloud computing aantoonbaar invloed op de vormgeving van de security architectuur van overheidsorganisaties?

Uit het onderzoek blijkt dat cloud computing invloed heeft op alle drie de veiligheidsaspecten die specifiek zijn belicht.[26] Verder blijkt er meer nadruk te liggen op het veiligheidsaspect beschikbaarheid van de clouddienst, vanwege informatiesystemen die voor het verlenen van spoedeisende hulp

[23] ID55, 75, 81, 92, 133, 172, 185
[24] ID33-34, 68, 169, 193, 195-196
[25] ID25-26, 29, 67, 135-137, 189-190, 192
[26] ID6, 12, 14, 46, 49, 53, 85-87, 100, 148-149, 151-154, 160, 163, 204, 244

worden gebruikt. Daarnaast hebben respondenten aangegeven dat de organisatie vanwege haar publieke taak meer risico loopt op imagoschade bij datalekken. Dit is naast het veiligheidsaspect gegevensbescherming ook gerelateerd aan het veiligheidsaspect beheer van incidenten.

4.3. Conclusie

De organisatie beschikt niet over een formeel vastgelegde security architectuur (ID147). Wel is er een referentie architectuur, namelijk VeRA, welke volgens de Veiligheidsregio ICT-kwaliteitsnormen (IFV, 2021) het kader vormt voor de ICT-prestatie. De organisatie beschikt over verschillende overheidsvoorschriften en -handreikingen die als hulpmiddelen kunnen worden gebruikt voor het vormgeven van haar security (ID69). Deze documenten worden voornamelijk ingezet voor inkooptrajecten van nieuwe IT-systemen (ID83). Uit het onderzoek komt naar voren dat er, ondanks de beschikbaarheid van deze middelen, onvoldoende duidelijkheid aanwezig is ten aanzien van beveiligingsniveaus en passende veiligheidsmaatregelen (ID31-32, 35). Het besef groeit dat er meer governance noodzakelijk is om de cloud security van de organisatie te borgen.[27] Om dit vorm te kunnen geven wordt er gewerkt aan het verhogen van het interne kennisniveau en worden er stappen gemaakt om meer te documenteren omtrent security beleid.[28]

Uit het onderzoek blijkt dat cloud computing invloed heeft op alle drie de veiligheidsaspecten die specifiek zijn belicht.[29] Verder blijkt er meer nadruk te liggen op het veiligheidsaspect beschikbaarheid van de clouddienst, vanwege informatiesystemen die voor het verlenen van spoedeisende hulp worden gebruikt. Daarnaast hebben respondenten aangegeven dat de organisatie vanwege haar publieke taak meer risico loopt op imagoschade bij datalekken. Dit is naast het veiligheidsaspect gegevensbescherming ook gerelateerd aan het veiligheidsaspect beheer van incidenten.

De organisatie ervaart dat zij, doordat zij een overheidsorganisatie is, moet voldoen aan aanvullende overheidsvoorschriften zoals de BIO, zwaardere eisen moet stellen aan leveranciers, meer te maken heeft met kritieke systemen en gevoelige gegevens, en dat zij bij datalekken meer risico loopt op imagoschade.[30] Een voordeel voor de organisatie is dat er, in het geval een datalek voorkomt, snel hulp voorhanden is (ID140).

[27] ID1, 4, 10, 62, 72-73, 75-76, 81, 92, 98, 133, 185
[28] ID20, 23, 42-43, 48, 77, 79-80, 93, 144, 183
[29] ID6, 12, 14, 46, 49, 53, 85-87, 100, 148-149, 151-154, 160, 163, 204, 244
[30] BIO, 2020; ID25-26, 28-29, 67, 134, 137, 139

5. Conclusie, discussie, aanbevelingen en reflectie

5.1. Conclusie

In dit onderzoek is een antwoord gezocht op de vraag: 'Op welke wijze en in welke mate heeft cloud computing invloed op de vormgeving van de security architectuur van overheidsorganisaties?' Hiervoor is literatuuronderzoek uitgevoerd en zijn er kwalitatieve gegevens verzameld bij een overheidsorganisatie door middel van interviews en documentatie over het onderwerp binnen de context van de organisatie.

Het literatuuronderzoek heeft beperkt informatie opgeleverd over welke security architecturen bestaan voor overheidsorganisaties, zowel in het algemeen als specifiek in relatie tot cloud computing. Er blijkt een grote verscheidenheid aan overheidseisen en certificeringen te zijn waaraan een cloudoplossing moet voldoen voor deze voor overheidsgegevens mag worden gebruikt. Het gebrek aan standaardisatie tussen overheden en hun eisen leidt tot een beperkt hergebruik van bestaande cloud concepten en architecturen van de overheid (Herre, 2020, pp. 396, 405). Vanuit de literatuur zijn er zes verschillende punten geïdentificeerd waaraan de meest geavanceerde en veilige cloudarchitecturen moeten voldoen. De NCC-SRA biedt voldoende handvatten voor de inrichting van een SA die voldoet aan deze genoemde voorwaarden en zou bijvoorbeeld kunnen worden gebruikt voor de implementatie van een IaaS-omgeving die voldoet aan de overheidsnormen van het NIST en gegevens van federale overheden bevat (Caballero, 2020, pp. 456-457; Tabel 2).

In het literatuuronderzoek zijn de veiligheidsaspecten wet- en regelgeving, beheersbaarheid van processen en systemen en gegevensbescherming specifiek belicht. Met betrekking tot deze aspecten blijkt uit het literatuuronderzoek dat het van belang is dat overheidsorganisaties op de hoogte zijn van de certificeringen die zij gebruiken en aan welke wet- en regelgeving zij moeten voldoen. Bij het gebruik van cloudgebaseerde informatiesystemen nemen overheidsorganisaties een risico in de beheersbaarheid van processen en systemen. Zij staan dan op een aantal onderdelen hun controle en beheersmogelijkheden af aan de cloud serviceprovider (Khan & Malluhi, 2010; Rashidi & Movah-hedinia, 2012). Om te bepalen onder welke voorwaarden een overheidsorganisatie bereid is om haar processen en systemen onder te brengen in de cloud is het noodzakelijk dat zij hier beleid voor formuleert. Dit beleid dient ook te beschrijven hoe de organisatie dit beleid op naleving gaat controleren (NCSC, 2012; Ferrin, Bligh & Kohles, 2007). De bescherming van gegevens in de cloud is een van de belangrijkste aspecten van clouddiensten (Ibiricu & van der Made, 2020). De toenemende verwevenheid van computersystemen en het koppelen van dataopslagsystemen maakt de gevoelige gegevens in systemen kwetsbaar. Daarnaast blijven organisaties zelf verantwoordelijk voor de beveiliging van gegevens, zelfs wanneer deze gegevens bij een cloud serviceprovider zijn ondergebracht (NCSC, 2012; Rîndaşu, 2018).

Een concreet antwoord op de vraag in welke mate cloud computing aantoonbaar invloed heeft op de vormgeving van de security architectuur van overheidsorganisaties is in de literatuur niet teruggevonden.

Het vervolgonderzoek heeft zich gericht op een eerste aanzet in het vaststellen van de invloed van cloud computing op de security architectuur van overheidsorganisaties. Een toename in kennis over dit onderwerp biedt overheidsorganisaties de mogelijkheid om hun security architectuur-

beslissingen beter te onderbouwen. Daarnaast draagt het onderzoek bij aan het vergroten van de theoretische kennis omtrent dit onderwerp.

Uit het vervolgonderzoek blijkt dat de caseorganisatie niet over een formeel vastgelegde security architectuur beschikt (ID147). Wel heeft zij een referentie architectuur, namelijk VeRA, welke volgens de Veiligheidsregio ICT-kwaliteitsnormen (IFV, 2021) het kader vormt voor de ICT-prestatie. De VeRA beschrijft de inrichting van de gewenste informatiehuishouding van Veiligheidsregio's en de aansluiting daarvan op de omgeving (IFV, 2021, p. 8; ID239). De organisatie beschikt over verschillende overheidsvoorschriften en -handreikingen die als hulpmiddelen kunnen worden gebruikt voor het vormgeven van haar security (ID69). Deze documenten worden voornamelijk ingezet voor inkooptrajecten van nieuwe IT-systemen (ID83). Uit het onderzoek komt naar voren dat er, ondanks de beschikbaarheid van deze middelen, onvoldoende duidelijkheid aanwezig is ten aanzien van beveiligingsniveaus en passende veiligheidsmaatregelen (ID31-32, 35). Het besef groeit dat er meer governance noodzakelijk is om de cloud security van de organisatie te borgen.[31] Om dit vorm te kunnen geven wordt er gewerkt aan het verhogen van het interne kennisniveau en worden er stappen gemaakt om meer te documenteren omtrent security beleid.[32]

Uit het onderzoek blijkt dat cloud computing invloed heeft op alle drie de veiligheidsaspecten die specifiek zijn belicht.[33] Verder blijkt er meer nadruk te liggen op het veiligheidsaspect beschikbaarheid van de clouddienst, vanwege informatiesystemen die voor het verlenen van spoedeisende hulp worden gebruikt. Daarnaast hebben respondenten aangegeven dat de organisatie vanwege haar publieke taak meer risico loopt op imagoschade bij datalekken. Dit is naast het veiligheidsaspect gegevensbescherming ook gerelateerd aan het veiligheidsaspect beheer van incidenten.

De organisatie ervaart dat zij, doordat zij een overheidsorganisatie is, moet voldoen aan aanvullende overheidsvoorschriften zoals de BIO, zwaardere eisen moet stellen aan leveranciers, meer te maken heeft met kritieke systemen en gevoelige gegevens, en dat zij bij datalekken meer risico loopt op imagoschade.[34] Een voordeel voor de organisatie is dat er, in het geval een datalek voorkomt, snel hulp voorhanden is (ID140).

5.2. Discussie

Uit de resultaten van zowel het literatuur- als het vervolgonderzoek blijkt dat er noodzaak is tot meer kennis ten aanzien van de invloed van cloud computing op de vormgeving van de security architectuur van overheidsorganisaties, aangezien deze beperkt aanwezig is en het onderwerp zeer actueel is.

De vervolgonderzoeksresultaten leveren informatie op over de invloed van cloud computing op de security van overheidsorganisaties. Omdat de caseorganisatie niet over een formeel vastgelegde security architectuur beschikt, kan niet concreet worden vastgesteld wat voor betekenis dit heeft voor de vormgeving van haar security architectuur (ID147). Wel is vastgesteld dat de organisatie over een referentie architectuur beschikt (ID239-240, 243). Het resultaat dat de overheids-organisatie over een sectorale referentie architectuur beschikt, met eigen specifieke normen en standaarden voor ICT-producten en -diensten (ID238), sluit aan op wat door Herre (2020, p. 405) is aangegeven, namelijk: dat er sprake is van een gebrek aan standaardisatie tussen overheden en dat

[31] ID1, 4, 10, 62, 72-73, 75-76, 81, 92, 98, 133, 185
[32] ID20, 23, 42-43, 48, 77, 79-80, 93, 144, 183
[33] ID6, 12, 14, 46, 49, 53, 85-87, 100, 148-149, 151-154, 160, 163, 204, 244
[34] BIO 2020; ID25-26, 28-29, 67, 134, 137, 139

hun verscheidenheid aan eisen tot een beperkt hergebruik van bestaande cloud concepten en architecturen leidt.

Omdat de organisatie geen formele security architectuur heeft en het kennisniveau niet in alle veiligheidsaspecten even hoog is[35], maakt dit het lastig om vast te stellen in hoeverre zij aan de voorwaarden voldoet die Caballero (2020, p. 457, Tabel 2) noemt voor de meest geavanceerde en veilige cloudarchitecturen. Ook door gebrek aan documentatie, waaronder een dataclassificatie-beleid, is niet duidelijk wat voor beveiligingsniveaus door de organisatie worden gehanteerd en of genomen veiligheidsmaatregelen passend zijn.[36]

De resultaten van het literatuuronderzoek ten aanzien van de invloed van cloud computing op de veiligheidsaspecten wet- en regelgeving, beheersbaarheid van processen en systemen en gegevens-bescherming komen overeen met de resultaten uit het vervolgonderzoek. De organisatie ervaart inderdaad dat het migreren van gegevens en processen naar de cloud gevolgen heeft voor de mate waarin zij moet voldoen aan wet- en regelgeving.[37] Er wordt op dit gebied meer gevraagd van de organisatie en dit vertaalt zich door in wat zij van haar leveranciers eist.[38] Verder ervaart de organisatie in sterke mate dat zij door cloud computing op een aantal onderdelen haar controle en beheersmogelijkheden aan de cloud serviceproviders afstaat.[39] De organisatie ervaart dat het noodzakelijk is om beleid te formuleren waarin zij bepaalt onder welke voorwaarden zij bereid is om haar processen en systemen in de cloud onder te brengen.[40] Een tweede stap hierin is dat zij vastlegt hoe zij dit beleid op naleving gaat controleren. Hoewel het bewustzijn dat deze controle nodig is groeit, is er nog een verdere cultuuromslag nodig binnen de organisatie om hier verder op te acteren (ID70, 184). Gegevensbescherming wordt zeker als een van de belangrijkste aspecten van clouddiensten ervaren (ID12, 46, 148). Het veilig koppelen van dataopslagsystemen is belangrijk voor de organisatie, mede omdat zij met ketenpartners samenwerkt.[41] Het borgen van data security is belangrijk, ook – of misschien juist – als de data bij een cloud serviceprovider is ondergebracht.[42]

Uit zowel het literatuur- als het vervolgonderzoek blijkt dat het veiligheidsaspect wet- en regelgeving specifiek relevant is voor de overheidsorganisatie. De organisatie moet voldoen aan aanvullende overheidsvoorschriften zoals de BIO (2020), de GIBIT (2020) en de Veiligheidsregio ICT-kwaliteits-normen (IVF, 2021) en merkt dat leveranciers moeite kunnen hebben met de eisen die aan overeenkomsten worden gesteld.[43] Met betrekking tot de veiligheidsaspecten beheersbaarheid van processen en systemen en gegevensbescherming kan niet expliciet worden vastgesteld dat deze voor een publieke organisatie een andere relevantie bezitten dan voor een private organisatie. Wel kunnen de aanvullende eisen die aan overheidsorganisaties voor het veiligheidsaspect wet- en regelgeving worden gesteld de vormgeving van de andere aspecten beïnvloeden. Zo kunnen eisen in een Service Level Agreement bij een overheidsorganisatie door aanvullende overheidsvoorschriften mogelijk hoger zijn dan bij een private organisatie en kan hierdoor een grotere beheersbaarheid van processen en systemen worden afgedwongen. Hetzelfde kan gelden voor eisen die in verwerkers-overeenkomsten worden gesteld, in het kader van gegevensbescherming.

[35] ID31, 44, 47-48, 59, 61-62, 69, 80, 147, 183, 193
[36] ID19-20, 117, 147, 183
[37] ID14, 28, 49, 53, 69, 83, 85-87, 160, 163, 208, 210
[38] ID25-26, 28, 134, 137
[39] ID2, 13, 16-17, 36-37, 40, 54, 78-79, 91, 94, 157, 166
[40] ID55, 75, 81, 92, 133, 172, 185
[41] ID56, 101, 138, 145).
[42] ID25-26, 29, 67, 135-137, 139, 189-190, 192
[43] ID15, 25-26, 28, 134, 137

Uit het vervolgonderzoek is naar voren gekomen dat er voor de organisatie wat meer nadruk ligt op het veiligheidsaspect beschikbaarheid van de clouddienst, vanwege informatiesystemen die voor het verlenen van spoedeisende hulp worden gebruikt (ID139). Aangezien niet elke overheidsorganisatie spoedeisende hulp verleent zal dit punt niet in het algemeen voor overheidsorganisaties gelden. Verder hebben respondenten aangegeven dat de organisatie bij datalekken, vanwege haar publieke taak, meer risico loopt op imagoschade dan bij private organisaties het geval is (ID29, 67). Informatie ten aanzien van dit onderwerp is in de literatuur niet teruggevonden.

5.3. Aanbevelingen voor de praktijk

Bij het gebruik van cloudgebaseerde informatiesystemen nemen overheidsorganisaties een risico in de beheersbaarheid van processen en systemen. Zij staan dan op een aantal onderdelen hun controle en beheersmogelijkheden af aan cloud serviceproviders (Khan & Malluhi, 2010; Rashidi & Movahhedinia, 2012). Om te bepalen onder welke voorwaarden een overheidsorganisatie bereid is om haar processen en systemen onder te brengen in de cloud is het noodzakelijk dat zij hier beleid voor formuleert. Dit beleid dient ook te beschrijven hoe de organisatie dit beleid op naleving gaat controleren (NCSC, 2012; Ferrin, Bligh & Kohles, 2007).

Wanneer het security beleid binnen een overheidsorganisatie is vastgesteld kan een security architectuur, door middel van een set samenhangende modellen en principes, efficiënt en flexibel richting geven aan de invulling hiervan. Inzicht in de relatie tussen cloud computing, security en de veiligheidsaspecten die specifiek relevantie bezitten voor de organisatie biedt haar de mogelijkheid om security architectuur-beslissingen beter te onderbouwen.

5.4. Aanbevelingen voor verder onderzoek

Security architectuur

Uit het vervolgonderzoek is gebleken dat de caseorganisatie niet over een formeel vastgelegde security architectuur beschikt (ID147). Omdat dit onderzoek zich op één organisatie heeft gericht, is aanvullend onderzoek noodzakelijk om vast te stellen in hoeverre andere overheidsorganisaties hun security architectuur hebben vastgelegd en wat de invloed van cloud computing hierop is.

Referentie architectuur

Uit het vervolgonderzoek is gebleken dat de caseorganisatie over een sectorale referentie architectuur beschikt (ID69, 147; IFV, 2021, p. 8). De vraag is in hoeverre deze referentie architectuur een geschikt kader vormt voor een security architectuur en of hier verschillen in zitten met betrekking tot andere sectorale referentie architecturen.

Integratie voorschriften

Overheidsorganisaties hebben te maken met aanvullende voorschriften zoals de BIO (2020) en de GIBIT (2020). Een aanvulling op dit onderzoek zou kunnen zijn om verder te verkennen welke rol deze voorschriften innemen voor overheidsorganisaties en hoe dit zich vertaalt in hun security architectuur.

Invloed veiligheidsaspecten

Uit het onderzoek blijkt dat het veiligheidsaspect wet- en regelgeving specifiek relevant is voor overheidsorganisaties.[44] Verder is uit het vervolgonderzoek naar voren gekomen dat er voor de caseorganisatie wat meer nadruk ligt op het veiligheidsaspect beschikbaarheid van de clouddienst, vanwege informatiesystemen die voor het verlenen van spoedeisende hulp worden gebruikt (ID139). Daarnaast hebben de respondenten aangegeven dat de organisatie, vanwege haar publieke taak, meer risico loopt op imagoschade bij datalekken dan bij private organisaties het geval is (ID29, 67). Dit is naast het veiligheidsaspect gegevensbescherming ook gerelateerd aan het veiligheidsaspect beheer van incidenten.

Aanvullend onderzoek zou zich kunnen richten op het vaststellen of deze invloeden voor andere organisaties binnen dezelfde overheidssector ook gelden en welke invloed dit heeft op de vormgeving van hun security architectuur. Vervolgens kan dit ook nog worden vergeleken met organisaties uit andere overheidssectoren.

Private sector

Dit onderzoek richt zich op de invloed van cloud computing op de vormgeving van de security architectuur van overheidsorganisaties. Hetzelfde type onderzoek kan ook worden verricht bij organisaties binnen de private sector. Op deze wijze kan nog inzichtelijker worden gemaakt of er verschillen zijn tussen de publieke en private sector als het gaat om de invloed van cloud computing op de vormgeving van hun security architectuur.

5.5. Reflectie

In de eerste opzet van het vervolgonderzoek lag de focus op het onderzoeken van meerdere overheidsorganisaties. Gedurende het onderzoek bleek dat dit qua tijdsplanning een te brede scope was en is dit beperkt tot één overheidsorganisatie. Dit resulteert in een lage generaliseerbaarheid van de onderzoeksresultaten. De externe validiteit is verhoogd door de beschrijving van de onderzoeksvragen, het ontwerp, de context, bevindingen en resulterende interpretaties. Op deze wijze kan de kwaliteit van het onderzoeksontwerp worden beoordeeld.

Om de interne validiteit te verhogen hebben de respondenten voorafgaand aan de interviews een toelichting ontvangen over het doel van het onderzoek en wat er van hen werd verwacht. Dit bood hen de mogelijkheid om zich in het onderwerp te verdiepen en daarmee de vragen die zij kregen beter te kunnen plaatsen en mogelijk meer complete antwoorden te kunnen geven. De interviews zijn gehouden aan de hand van een protocol (zie Bijlage 3). De interviews zijn op semigestructureerde wijze afgenomen en na afloop snel getranscribeerd. Twee respondenten hebben documentatie aangeleverd over het onderwerp. Dit is gebruikt voor datatriangulatie.

Ten behoeve van de constructvaliditeit is grondig vooronderzoek verricht en is de afstudeerbegeleider gevraagd om feedback op de interviewvragen voordat deze zijn ingezet voor de interviews. De resultaten van de codering van de verzamelde gegevens en de belangrijkste tekstfragmenten zijn vermeld in Bijlagen 4 en 5. Aan het verslag zijn niet de gehele transcripten toegevoegd, om te voorkomen dat de informatie mogelijk te herleiden is naar de organisatie en/of respondenten en sommige informatie vertrouwelijk is.

[44] ID14, 28, 49, 53, 69, 83, 85-87, 160, 163, 208, 210

In de uitvoering van de interviews is gelet op consistentie in de omgevingsfactoren waarin de interviews werden afgenomen. Zo zijn de drie interviews, die op locatie zijn afgenomen, in exact dezelfde ruimte afgenomen en is er gekozen voor een omgeving die vertrouwd is en daarnaast zo min mogelijk afleiding geeft. De gegevens zijn zo objectief mogelijk verzameld. Ook is er gelet op samenhang in de wijze waarop gegevens zijn gecodeerd, geanalyseerd en geïnterpreteerd.

De respondenten zijn zowel schriftelijk als mondeling op hun rechten gewezen. Zij hebben mondeling aangegeven hier kennis van te hebben genomen en hebben hun toestemming gegeven voor deelname aan het onderzoek. De respondenten is toegezegd dat de resultaten anoniem zijn. Met twee respondenten heeft er na afloop van de interviews nog contact plaatsgevonden voor aanvullende informatie.

Tijdens het afnemen van de interviews was merkbaar dat de formulering van sommige vragen wat lang kon zijn en daardoor minder goed te onthouden voor de respondenten. Het kennisniveau van de respondenten speelde hier mogelijk ook een rol in. Gaandeweg is er door de onderzoeker een kort document opgesteld waarin wat informatie staat om sommige vragen makkelijk verder toe te kunnen lichten en bij vervolginterviews exact dezelfde aanvullende informatie aan te kunnen leveren voor de respondenten.

Gedurende de interviews bleek er moeilijker informatie te kunnen worden verzameld over het onderzoeksonderwerp dan gedacht. Specifieke vragen over het gebruik van een security architectuur en de bijbehorende veiligheidsaspecten konden niet of beperkt worden beantwoord. Mogelijk is er voorafgaand aan het onderzoek door de onderzoeker onvoldoende een inschatting gemaakt van het kennisniveau op het gebied van security architectuur binnen de caseorganisatie. In de organisatie is geen security architect werkzaam en applicatiebeheer wordt uitbesteed, waardoor de (technische) kennis intern vrij beperkt is (ID242).

Hoewel er geen direct antwoord op de onderzoeksvraag is gevonden, vormt het onderzoek een verkenning ten aanzien van cloud security in de context van een overheidsorganisatie. De verzamelde en geanalyseerde gegevens bieden informatie over de invloed van cloud computing op security aspecten van een overheidsorganisatie en vormen hiermee een eerste aanzet voor de vormgeving van security beleid en de ontwikkeling van een security architectuur.

Referenties

Ali, O., Shrestha, A., Chatfield, A., & Murray, P. (2020). Assessing information security risks in the cloud: A case study of Australian local government authorities. *Government Information Quarterly*, *37*(1), 101419. https://doi.org/10.1016/j.giq.2019.101419

Baheer, B. A., Lamas, D., & Sousa, S. (2020). A systematic literature review on existing digital government architectures: State-of-the-art, challenges, and prospects. *Administrative Sciences*, *10*(2), 25. https://doi.org/10.3390/admsci10020025

Bijlsma-Frankema, K. M., & Costa, A. C. (2005). Understanding the trust-control nexus. *International Sociology, 20*(3), 259–283. https://doi.org/10.1177/0268580905055477

BIO. (2020). *Baseline Informatiebeveiliging Overheid*. Geraadpleegd op: https://www.bio-overheid.nl/

Institute of Electrical and Electronics Engineers. (2000). *Recommended practice for architectural description of software-intensive systems* (Std 1471-2000). https://doi.org/10.1109/IEEESTD.2000.91944

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Brumă, L. M. (2020). Data Security methods in cloud computing. *Informatica Economica, 24*(1/2020), 48-60. https://doi.org/10.24818/issn14531305/24.1.2020.05

Caballero, A. (2020). Advanced security architecture for cloud computing. In J. R. Vacca (Ed.), *Cloud computing security: Foundations and challenges* (pp. 443-462) (2e ed.) [Kindle-editie]. Geraadpleegd op https://www. routledge.com/

Commission Nationale de l'Informatique et des Libertés. (2018). *Security of personal data.* Geraadpleegd op https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_

personnelle_gb_web.pdf

Corbin, J., & Strauss, A. (2014). *Basics of qualitative research: Techniques and procedures for developing grounded theory* (4e ed.). Geraadpleegd op https://us.sagepub.com/en-us/nam/home

Costa, A. C., & Bijlsma-Frankema, K. (2007). Trust and control interrelations: New perspectives on the trust—control nexus. *Group & Organization Management*, *32*(4), 392-406. https://doi.org/10.1177/1059601106293871

Dubois, A., & Gadde, L. (2002, juli). Systematic combining: An abductive approach to case research. *Journal of Business Research, 55*(7), 553-560. https://doi.org/10.1016/S0148-2963(00)00195-8

Eisenhardt, K. M. (1989). Building theories from case study research. *The Academy of Management Review, 14*(4), 532-550. https://doi.org/10.2307/258557

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. *Academy of Management Journal, 50*(1), 25-32. https://doi.org/10.5465/AMJ.2007.24160888

Fernandez, E. B., Monge, R., & Hashizume, K. (2016). Building a security reference architecture for cloud systems. *Requirements Engineering, 21*(2), 225-249. https://doi.org/10.1007/s00766-014-0218-7

Ferrin, D. L., Bligh, M. C., & Kohles, J. C. (2007). Can I trust you to trust me?: A theory of trust, monitoring, and cooperation in interpersonal and intergroup relationships. *Group & Organization Management, 32*(4), 465–499. https://doi.org/10.1177/1059601106293960

Gibbert, M., & Ruigrok, W. (2010). The what and how of case study rigor: Three strategies based on published work. *Organizational Research Methods, 13*(4), 710-737. https://doi.org/10.1177/1094428109351319

Gupta, S. (2020). Assuring compliance with government certification and accreditation regulations. In J. R. Vacca (Ed.), *Cloud computing security: Foundations and challenges* (pp. 386-394) (2e ed.) [Kindle-editie]. Geraadpleegd op https://www. routledge.com/

Hakim, C. (2000). *Research design: Successful designs for social and economic research* (2e ed.) [Kindle-editie]. Geraadpleegd op https://www. routledge.com/

Herre, T. (2020). Government certification, accreditation, regulations, and compliance risks. In J. R. Vacca (Ed.), *Cloud computing security: Foundations and challenges* (pp. 396, 405-406) (2e ed.) [Kindle-editie]. Geraadpleegd op https://www. routledge.com/

Hussain, S. A., Fatima, M., Saeed, A., Raza, I., & Shahzad, R. K. (2017). Multilevel classification of security concerns in cloud computing. *Applied Computing & Informatics, 13*(1), 57-65. https://doi.org/10.1016/j.aci.2016.03.001

Ibiricu, B., & van der Made, M. L. (2020). Ethics by design: A code of ethics for the digital age. *Records Management Journal, 30*(3), 395-414. https://doi.org/10.1108/RMJ-08-2019-0044

Instituut Fysieke Veiligheid (2021). *Veiligheidsregio ICT-kwaliteitsnormen*. Geraadpleegd op https://www.softwarecatalogusvr.nl/

Iorga, M., &. Karmel, A. (2020). Managing risk in the cloud. In J. R. Vacca (Ed.), *Cloud computing security: Foundations and challenges* (pp. 84-94) (2e ed.) [Kindle-editie]. Geraadpleegd op https://www. routledge.com/

Khan, K. M., & Malluhi, Q. (2010). Establishing trust in cloud computing. *IT professional*, *12*(5), 20-27. https://doi.org/10.1109/MITP.2010.128

Koo, J., Oh, S., Lee, S. H., & Kim, Y. (2020, februari). Security architecture for cloud-based command and control system in IoT environment. *Applied Sciences, 10*(3), 1035. https://doi.org/10.3390/app10031035

Kuner, C., Cate, F. H., Millard, C., Svantesson, D. J. B., & Lynskey, O. (2015). Risk management in data protection. *International Data Privacy Law, 5*(2), 95-98. https://doi.org/10.1093/idpl/ipv005

Mahmood, Z., & Hill, R. (Eds.). (2011). *Cloud computing for enterprise architectures*. Geraadpleegd op https://www.springer.com/gp

Mell, P. and Grance, T. (2011). *The NIST definition of cloud computing*. https://doi.org/10.6028/NIST.SP.800-145

Nationaal Cyber Security Centrum. (2012). *Whitepaper NCSC: Cloud computing & security.* Geraadpleegd op https://www.ncsc.nl/documenten/publicaties/2019/mei/01/cloudcomputing

Oosten, W. (2014). *Inleiding bestuurskunde* (5e ed.). Den Haag, Nederland: Boom.

Pohlmann, N. (2017). *The next step in it security after Snowden*. Geraadpleegd op https://norbert-pohlmann.com/app/uploads/2015/08/321-The-next-step-in-IT-security-after-Snowden-Prof.-Norbert-Pohlmann1.pdf

Powney, J., & Watts, M. (1987). *Interviewing in educational research.* https://doi.org/10.4324/9780429503740

Rashidi, A., & Movahhedinia, N. (2012). A model for user trust in cloud computing. *International Journal on Cloud Computing*, *2*(2), 1-8. Geraadpleegd op https://d1wqtxts1xzle7.cloudfront.net/38562388/33.pdf?1440480525=&response-content-disposition=inline%3B+filename%3DA_Model_for_User_Trust_in_Cloud_Computin.pdf&Expires=1620479133&Signature=dC0lzfDE8Og2decN-bdgvW27tIxSEh0Op~JIfJnRJ14 ~TVWFqyOgkYza6jUrDpiO6ivIv8pdvWSTOesQhed9tfTBbvfthgf5Y-RfJ92TBDr5zTqoEgm4MwUhQTyKOx02uIQ7OHuijTlX3LzjX-lNPfaLIay~bb7HvAvIdmk2gwnGeDuSABBzKvOnSU8gStPlxiljFWHCCHVCFwFNTW2L16bGUu1OdHKaCRLGbAvnZ-~D3Kejgn-otRBMQPnVA8ucdO8t3EWAU8G370Vi8wlWUzsGA7HZeUAAK3qNhIGxm15oVlrFD4TQRalY9wrM~v7JDk7QDSWCdzhcLaPT-ycITQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

Ridder, H., Hoon, C., & McCandless Baluch, A. (2014). Entering a dialogue: Positioning case study findings towards theory. *British Journal of Management, 25*(2), 373-387. https://doi.org/10.1111/1467-8551.12000

Rîndaşu, S. (2018). Information security challenges: Vulnerabilities brought by ERP applications and cloud platforms. *Audit Financiar, 16*(149), 131-139. https://doi.org/10.20869/AUDITF/2018/149/131

Ross, J.W., Weill, P., & Robertson, D. (2006). *Enterprise architecture as strategy: Creating a foundation for business execution.* Geraadpleegd op https://hbsp.harvard.edu/home/

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research methods for business students* (7e ed.). Harlow, Engeland: Pearson.

Sen, J. (2015). Security and privacy issues in cloud computing. In Information Resources Management Association (Ed.), *Cloud technology: concepts, methodologies, tools, and applications* (pp. 1585-1630). https://doi.org/10.4018/978-1-4666-6539-2.ch074

Shanks, G., Gloet, M., Asadi Someh, I., Frampton, K., & Tamm, T. (2018). Achieving benefits with enterprise architecture. *The Journal of Strategic Information Systems*, *27*(2), 139-156. https://doi.org/10.1016/j.jsis.2018.03.001

Tamm, T., Seddon, P. B., Shanks, G., Reynolds, P., & Frampton, K. M. (2015). How an Australian retailer enabled business transformation through enterprise architecture. *MIS Quarterly Executive*, *14*(4), 181-193. Geraadpleegd op https://aisel.aisnet.org/misqe/vol14/iss4/4

Vereniging van Universiteiten. (2014). *De Nederlandse gedragscode wetenschapsbeoefening: Principes van goed wetenschappelijk onderwijs en onderzoek.* Geraadpleegd op http://vsnu.nl/files/documenten/Domeinen/Onderzoek/Code_wetenschapsbeoefening_2004_%282014%29.pdf

Vereniging van Nederlandse Gemeenten, Informatiebeveiligingsdienst voor gemeenten. (2019). *Handreiking Inkoop Clouddiensten.* Geraadpleegd op https://www.informatiebeveiligingsdienst.nl/product/handreiking-inkoop-clouddiensten/

Vereniging van Nederlandse Gemeenten, Realisatie. (2021). *Gemeentelijke ICT-kwaliteitsnormen*. Geraadpleegd op https://www.vngrealisatie.nl/sites/default/files/2021-03/20210317%20-%20Gemeentelijke-ICT-kwaliteitsnormen-v2021-1_0.pdf

Vereniging van Nederlandse Gemeenten, Realisatie. (2020). *Gemeentelijke Inkoopvoorwaarden bij IT*. Geraadpleegd op https://www.vngrealisatie.nl/sites/default/files/2021-03/GIBIT-2020-Artikelen_0.pdf

Yin, R.K. (2018). *Case study research and applications: Design and methods* (6e ed.). Geraadpleegd op https://us.sagepub.com/en-us/nam/home

Bijlage 1: Query's voor het literatuuronderzoek

De query's zijn uitgevoerd in oktober/december 2020 en januari 2021.

Tabel 3 - Resultaten query 1: security architecture AND cloud computing AND government

Parameters	Aantal hits via https://bibliotheek.ou.nl/:
Geavanceerd zoeken Laatste 3 jaren Peer-reviewed publicaties	61
Verder toegepaste criteria:	
Aantal na scannen op titel	4
Aantal na lezen abstract	3
Aantal gelezen	3
Aantal gebruikt	1
Parameters	Aantal hits via https://scholar.google.nl/:
Sinds 2020	449
Verder toegepaste criteria:	
Aantal na scannen op titel	38
Aantal na lezen abstract	7
Aantal gelezen	7
Aantal gebruikt	2

Tabel 4 - Resultaten query 2: cloud security architecture AND government

Parameters	Aantal hits via https://bibliotheek.ou.nl/:
Geavanceerd zoeken Laatste 3 jaren Peer-reviewed publicaties	0
Geavanceerd zoeken Laatste 10 jaren Peer-reviewed publicaties	4
Verder toegepaste criteria:	
Aantal na scannen op titel	1
Aantal na lezen abstract	0
Aantal gelezen	0
Aantal gebruikt	0
Parameters	Aantal hits via https://scholar.google.nl/:
Sinds 2020	16
Verder toegepaste criteria:	
Aantal na scannen op titel	7
Aantal na lezen abstract	1
Aantal gelezen	1
Aantal gebruikt	1

Tabel 5 - Resultaten query 3: IT security architecture AND cloud computing AND government

Parameters	Aantal hits via https://bibliotheek.ou.nl/:
Geavanceerd zoeken Laatste 3 jaren Peer-reviewed publicaties	68
Verder toegepaste criteria:	
Aantal na scannen op titel	3
Aantal na lezen abstract	2
Aantal gelezen	1
Aantal gebruikt	1
Parameters	Aantal hits via https://scholar.google.nl/:
Sinds 2020	4
Sinds 2017	16
Verder toegepaste criteria:	
Aantal na scannen op titel	3
Aantal na lezen abstract	1
Aantal gelezen	1
Aantal gebruikt	1

Tabel 6 - Resultaten query 4: IT outsourcing AND government AND cloud security

Parameters	Aantal hits via https://bibliotheek.ou.nl/:
Geavanceerd zoeken Laatste 12 maanden Peer-reviewed publicaties	147
Verder toegepaste criteria:	
Aantal na scannen op titel	12
Aantal na lezen abstract	2
Aantal gelezen	1
Aantal gebruikt	0

Tabel 7 - Resultaten query 5: compliance AND cloud computing AND government

Parameters	Aantal hits via https://bibliotheek.ou.nl/:
Geavanceerd zoeken Laatste 12 maanden Peer-reviewed publicaties	440
Verder toegepaste criteria:	
Aantal na scannen op titel	11
Aantal na lezen abstract	4
Aantal gelezen	4
Aantal gebruikt	3

Bijlage 2: Informatie voor de respondenten

Basisgegevens

Tabel 8 - Basisgegevens

Opleiding	Open Universiteit, faculteit Bètawetenschappen Masteropleiding Business Process Management & IT
Naam student	Annet Schollaart
Onderzoeksonderwerp	Invloed van cloud computing op de security architectuur van overheids-organisaties

Wat wordt er gevraagd van jou als respondent?

- Deelname aan een individueel **interview van 60 minuten**.
- Het heeft de voorkeur om het interview **op locatie** (…) plaats te laten vinden; wanneer je hier een bezwaar tegen hebt kan het interview via Teams plaatsvinden.
- Toestemming voor een **opname van het interview**.
- Na het interview word je gevraagd of je **aanvullend documentatie** kunt aanleveren ten aanzien van het onderwerp binnen de context van de organisatie. Hiermee kunnen de interviewresultaten extra worden onderbouwd.

Wat is het doel van het interview?

Doel van het interview is om te achterhalen op welke wijze en in welke mate cloud computing invloed heeft op de vormgeving van de security architectuur van de organisatie. Om dit vast te kunnen stellen wordt besproken **welke wijzigingen er plaatsvinden in de securitybehoeften van de organisatie, wanneer zij de beslissing maakt om haar services en gegevens naar een cloudomgeving te migreren, en welke veiligheidsaspecten als gevolg hiervan in haar security architectuur worden geïmplementeerd**. Het gaat hier om het verkrijgen van een globaal beeld, zonder al te ver in te gaan op details.

Doel is om de kennis en ervaringen die jij specifiek hebt op het gebied van dit onderwerp binnen deze organisatie te inventariseren en deze informatie te bundelen met de gegevens die in de interviews met de andere respondenten worden verzameld.

Op de volgende pagina staat enige achtergrondinformatie vermeld over het onderwerp, zodat je je van tevoren alvast een beeld kunt vormen bij de inhoud van het interview.

Ethische aspecten

- Deelname aan het onderzoek is vrijwillig.
- Het staat je vrij om je op elk moment uit het onderzoek terug te trekken.
- Tijdens het interview ben je niet verplicht om te antwoorden op vragen.
- Gebruikte en verwerkte gegevens zijn niet direct te herleiden naar jou of naar de organisatie.
- De opname van het interview is enkel toegankelijk voor de onderzoeker.
- Na het onderzoek kan de opname worden vernietigd, als je dit wilt en hebt aangegeven.

- Gedurende het onderzoek wordt er gewerkt volgens de Wet Bescherming Persoonsgegevens (AVG) en de Nederlandse Gedragscode Wetenschapsbeoefening (Vereniging van Universiteiten, 2014).

Achtergrondinformatie

In het boek *Cloud Computing for Enterprise Architectures* van Mahmood en Hill (2011, p. 3) wordt **cloud computing** kortweg geïntroduceerd als een algemene term die betrekking heeft op het leveren van gehoste services via internet. Het National Institute of Standards and Technology (NIST) gaat uit van de volgende definitie:

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (Mell & Grance, 2011). (p. 2)

Enterprise Architectuur (EA) helpt een organisatie bij het ontwikkelen en verwoorden van een visie voor het gebruik van informatietechnologie (IT) om haar strategische bedrijfsprioriteiten te ondersteunen (Tamm, Seddon, Shanks, Reynolds & Frampton, 2015; Ross, Weill & Robertson, 2006, p. 9). Shanks, Gloet, Asadi Someh, Frampton en Tamm (2018) stellen het volgende: "Enterprise Architecture (EA) defines the current and desirable future states of an organization's processes, capabilities, application systems, data, and IT infrastructure and provides a roadmap for achieving this target from the current state". (p. 139)

EA vormt de basisarchitectuur voor een organisatie en kan subarchitecturen bevatten zoals een business architectuur, application architectuur, data architectuur, technical architectuur en een **security architectuur** (Mahmood & Hill, 2011, pp. 14, 198). Dit onderzoek beperkt zich in scope op het onderdeel security architectuur.

Security kent een aantal deelgebieden of aspecten, namelijk: naleving van wet- en regelgeving, beheersbaarheid van processen en systemen, gegevensbescherming, relatie tot de leverancier, beschikbaarheid van de clouddienst, beheer van gebruikers, beheer van incidenten, beheer van wijzigingen, back-up en recovery en transparantie (Nationaal Cyber Security Centrum, 2012). Dit onderzoek richt zich specifiek op de volgende drie **veiligheidsaspecten**:

1. naleving van wet- en regelgeving;
2. beheersbaarheid van processen en systemen;
3. gegevensbescherming.

Caballero (2020, p. 457) stelt dat de **meest geavanceerde en veilige cloudarchitecturen** in elk geval voorzien in de volgende zaken:

1. Veilige scheiding van tenant data en compute resources wordt in de hoogst mogelijke mate geïmplementeerd.
2. Service (assurance-)level agreements zijn in overeenstemming met het hoogste security-niveau dat intern is vastgesteld op basis van de classificatie van gegevens.
3. Security en compliancevereisten zijn gelijk aan of overtreffen de eisen die binnen de interne IT-organisatie worden aangehouden.
4. Beschikbaarheid en gegevensbescherming worden gemaximaliseerd met elk redelijk controlemechanisme dat in overeenstemming is met de gevoeligheid van de gegevens die moeten worden verwerkt.
5. Tenantbeheer en controle zijn vastgelegd in duidelijke en compromisloze methoden, met consequenties wanneer hier een afwijking in optreedt.

6. Het beheer en de controle van de cloud serviceprovider wordt geminimaliseerd en een intern team van de cloud customer heeft volledig inzicht in alle acties van de provider.

Referenties

Caballero, A. (2020). Advanced security architecture for cloud computing. In J. R. Vacca (Ed.), *Cloud computing security: Foundations and challenges* (pp. 443-462) (2e ed.) [Kindle-editie]. Geraadpleegd op https://www. routledge.com/

Mahmood, Z., & Hill, R. (Eds.). (2011). *Cloud computing for enterprise architectures*. Geraadpleegd op https://www.springer.com/gp

Mell, P. and Grance, T. (2011). *The NIST definition of cloud computing*. https://doi.org/10.6028/NIST .SP.800-145

Nationaal Cyber Security Centrum. (2012). *Whitepaper NCSC: Cloud computing & security.* Geraadpleegd op https://www.ncsc.nl/documenten/publicaties/2019/mei/01/cloudcomputing

Ross, J.W., Weill, P., & Robertson, D. (2006). *Enterprise architecture as strategy: Creating a foundation for business execution.* Geraadpleegd op https://hbsp.harvard.edu/home/

Shanks, G., Gloet, M., Asadi Someh, I., Frampton, K., & Tamm, T. (2018). Achieving benefits with enterprise architecture. *The Journal of Strategic Information Systems*, *27*(2), 139-156. https:// doi.org/10.1016/j.jsis.2018.03.001

Tamm, T., Seddon, P. B., Shanks, G., Reynolds, P., & Frampton, K. M. (2015). How an australian retailer enabled business transformation through enterprise architecture. *MIS Quarterly Executive*, *14*(4), 181-193. Geraadpleegd op https://aisel.aisnet.org/misqe/vol14/iss4/4

Vereniging van Universiteiten. (2014). *De Nederlandse gedragscode wetenschapsbeoefening: Principes van goed wetenschappelijk onderwijs en onderzoek.* Geraadpleegd op http://vsnu.nl/files /documenten/Domeinen/Onderzoek/Code_wetenschapsbeoefening_2004_%282014%29.pdf

Bijlage 3: Interviewprotocol

Interviewthema's

Algemene doelstelling van het onderzoek is om te verkennen wat de invloed van cloud computing is op de inrichting van de security architectuur van overheidsorganisaties. Op basis hiervan zijn de volgende thema's geformuleerd voor het interview:

Thema 1: Security architectuur

In welke mate er een security architectuur is vastgelegd binnen de organisatie en wat deze inhoudt.

Thema 2: Invloed cloud computing op de security architectuur

In welke mate en op welke wijze cloud computing invloed heeft op de vormgeving van de security architectuur van de organisatie.

Thema 3: Specifiek relevante veiligheidsaspecten bij cloud computing

Welke veiligheidsaspecten specifiek een rol spelen bij cloud computing, in het bijzonder de naleving van wet- en regelgeving, beheersbaarheid van processen en systemen en gegevensbescherming.

Thema 4: Invloed rol als overheidsorganisatie op security

In welke mate het invloed heeft op de (vormgeving van haar) security dat er hier sprake is van een overheidsorganisatie.

Thema 5: Informatiebehoefte t.a.v. cloud security

In welke mate de organisatie over voldoende informatie beschikt t.a.v. cloud security en er sprake is van een informatiebehoefte.

Voorbereiding

1. In overleg met een leidinggevende en een specialist op het gebied van security wordt vastgesteld welke werknemers geschikt zijn om te worden benaderd voor het onderzoek.
2. De potentiële respondenten worden benaderd en gevraagd of zij instemmen met deelname aan het onderzoek.
3. Bij toestemming voor deelname wordt er een afspraak gepland met de respondent en krijgt hij/zij informatie over het onderzoek aangeleverd zoals vermeld in Bijlage 2.

Interview

Introductie

4. Er vindt een check plaats of de respondent de aangeleverde informatie, waaronder de ethische aspecten, heeft doorgenomen, zich bewust is van zijn/haar rechten, en toestemming geeft voor de opname van het interview. De onderzoeker zorgt dat er een gedrukt en digitaal exemplaar van de informatie aanwezig is bij het interview.
5. De opname wordt gestart.
6. Het interview wordt gestart.

Vragen

7. De onderstaande vragen worden gesteld:

Tabel 9 - Interviewvragen

Thema 1: Security architectuur	
1	In welke mate is er een security architectuur vastgelegd binnen de organisatie?
2	Hoe zou je de security architectuur omschrijven; wat houdt deze in?
Thema 2: Invloed cloud computing op de security architectuur	
3	Als we kijken naar cloud computing en security, wat voor relatie zie je daartussen; hoe beïnvloedt cloud computing de security architectuur?
4	Welke onderdelen van cloud computing hebben specifiek invloed op de security architectuur?
Thema 3: Specifiek relevante veiligheidsaspecten bij cloud computing	
5	Als het gaat om veiligheidsaspecten en cloud computing; welke veiligheidsaspecten springen hierbij het meest in het oog, vormen de grootste uitdaging?
6	Wat maakt dat deze veiligheidsaspecten een uitdaging vormen?
7	Ik ben benieuwd naar wat je me kunt vertellen over drie verschillende veiligheidsaspecten in relatie tot cloud computing en security. De eerste is naleving van wet- en regelgeving; hoe beïnvloedt dit veiligheidsaspect de security bij cloud computing?
8	Het tweede veiligheidsaspect is de beheersbaarheid van de processen en systemen; wat is de invloed hiervan op de security bij cloud computing?
9	Als laatste dezelfde vraag ten aanzien van gegevensbescherming; welke invloed heeft dit aspect op de security bij cloud computing?
10	In de informatie die ik voorafgaand aan het interview heb aangeleverd worden 6 punten genoemd die onderdeel kunnen zijn van een security architectuur (Caballero, 2020, p. 457), ik pak ze er even bij. In welke mate herken je de punten die worden genoemd terug in de security architectuur van de organisatie?
Thema 4: Invloed rol als overheidsorganisatie op security	
11	Als we kijken naar het type organisatie waar we bij werken, een overheidsorganisatie, en security, wat voor relatie zie je daartussen; in hoeverre denk jij dat het feit dat het hier om een overheidsorganisatie gaat, invloed heeft op security?
12	Zijn er onderdelen van cloud computing specifiek relevant voor de security van publieke organisaties ten opzichte van de security van private organisaties?
13	Stel: er is een security breach. Welke invloed kan het feit, dat het hier om een overheidsorganisatie gaat, hebben op de gevolgen van de security breach?
Thema 5: Informatiebehoefte t.a.v. cloud security	
14	We komen nu bijna bij het einde van het interview. Ik wil het nog hebben over een eventuele informatiebehoefte binnen de organisatie ten aanzien van cloud security. De eerste vraag hierover is: in welke mate is er binnen de organisatie de kennis aanwezig om securitybehoeften rondom cloud computing in kaart te brengen en hierop te acteren en te anticiperen?
15	Voor welke onderdelen van cloud computing en security is er behoefte aan meer kennis?
16	Op welke wijze probeert de organisatie deze kennis te vergaren; zijn er bepaalde partijen die hierin een rol spelen of zouden kunnen spelen?
Overig	
17	Zijn er nog zaken die je ten opzichte van het onderzoeksonderwerp zou willen opmerken of die je nog mist in dit gesprek?

Slot

8. Het interview wordt afgerond en de respondent wordt bedankt voor zijn/haar deelname aan het onderzoek en de geleverde informatie.
9. De opname van het interview wordt gestopt.
10. Na afname van het interview wordt de respondent verzocht om eventuele documentatie t.a.v. het onderzoeksonderwerp aan te leveren.

Referentie

Caballero, A. (2020). Advanced security architecture for cloud computing. In J. R. Vacca (Ed.), *Cloud computing security: Foundations and challenges* (pp. 443-462) (2e ed.) [Kindle-editie]. Geraadpleegd op https://www. routledge.com/

Bijlage 4: Resultaten codering

Tabel 10 - Codes

Code	Aantal tekstfragmenten	Codegroepen
Advisering	10	Transparantie
Afhankelijkheid	6	Beheersbaarheid van processen en systemen
Application en Interface Security	6	Relatie tot de leverancier
Audit en Assurance	15	Beheersbaarheid van processen en systemen Beheer van incidenten
Baseline Informatiebeveiliging Overheid	28	Naleving van wet- en regelgeving Overheidsorganisatie
Betrouwbaarheid	5	Overheidsorganisatie
Beveiligingsniveau	8	Gegevensbescherming Beheer van wijzigingen
Bewustzijn	7	Beheersbaarheid van processen en systemen
Business Continuity Management	12	Relatie tot de leverancier Beschikbaarheid van de clouddienst Beheer van wijzigingen Back-up en recovery
Change management	14	Beheer van wijzigingen
Contractmanagement	19	Beheersbaarheid van processen en systemen Relatie tot de leverancier
Data Security	34	Gegevensbescherming Beheer van incidenten
Datacenter Security	4	Gegevensbescherming Beschikbaarheid van de clouddienst
Dataclassificatie	6	Gegevensbescherming
Endpoint Management	6	Gegevensbescherming Beheer van gebruikers Beheer van wijzigingen
Gemeentelijke Inkoop bij IT	4	Overheidsorganisatie
Governance	34	Beheersbaarheid van processen en systemen
Handreiking inkoop clouddiensten	2	Overheidsorganisatie
ICT-Richtlijnen en voorwaarden organisatie	6	Beheersbaarheid van processen en systemen
Identity en Access Management	9	Beheersbaarheid van processen en systemen Gegevensbescherming Beheer van gebruikers
Incident Management	11	Beschikbaarheid van de clouddienst Beheer van incidenten

Code	Aantal tekstfragmenten	Codegroepen
Infrastructure en Virtualization Security	14	Gegevensbescherming Relatie tot de leverancier Beschikbaarheid van de clouddienst Transparantie
Interoperability en Portability	2	Relatie tot de leverancier
Kennis	13	Beheersbaarheid van processen en systemen Beheer van wijzigingen Transparantie
Kritisch systeem	4	Beschikbaarheid van de clouddienst Overheidsorganisatie
Logging en Monitoring	9	Beheer van gebruikers Beheer van incidenten Beheer van wijzigingen
Organisatiecultuur	2	Beheersbaarheid van processen en systemen
Outsourcing	4	Beheersbaarheid van processen en systemen Transparantie
Overheidsorganisatie	18	Overheidsorganisatie
Privacywetgeving	16	Naleving van wet- en regelgeving Gegevensbescherming
Problem Management	5	Beheer van incidenten
Referentie architectuur	3	Overheidsorganisatie
Risicomanagement	13	Beheersbaarheid van processen en systemen Beheer van wijzigingen
Supply Chain Management	26	Beheersbaarheid van processen en systemen
Technisch applicatiebeheer	9	Beheersbaarheid van processen en systemen
Threat and Vulnerability Management	9	Transparantie
Transparantie	2	Transparantie
Vaardigheid	2	Beheersbaarheid van processen en systemen
Veiligheidsregio ICT-kwaliteitsnormen	2	Overheidsorganisatie
Vendor lock-in	2	Relatie tot de leverancier
Verantwoordelijkheid	10	Beheersbaarheid van processen en systemen Gegevensbescherming
Vertrouwen	10	Beheersbaarheid van processen en systemen Transparantie
Verwerkersovereenkomst	6	Naleving van wet- en regelgeving Gegevensbescherming

Code	Aantal tekstfragmenten	Codegroepen
Verwerkersovereenkomst organisatie	7	Naleving van wet- en regelgeving Gegevensbescherming
Wet- en regelgeving	9	Naleving van wet- en regelgeving Gegevensbescherming

Tabel 11 - Codegroepen

Codegroep	Aantal codes	Codes
Naleving van wet- en regelgeving	5	Baseline Informatiebeveiliging Overheid Privacywetgeving Verwerkersovereenkomst Verwerkersovereenkomst organisatie Wet- en regelgeving
Beheersbaarheid van processen en systemen	16	Afhankelijkheid Audit en Assurance Bewustzijn Contractmanagement Governance ICT-Richtlijnen en voorwaarden organisatie Identity en Access Management Kennis Organisatiecultuur Outsourcing Risicomanagement Supply Chain Management Technisch applicatiebeheer Vaardigheid Verantwoordelijkheid Vertrouwen
Gegevensbescherming	12	Beveiligingsniveau Data Security Datacenter Security Dataclassificatie Endpoint Management Identity en Access Management Infrastructure en Virtualization Security Privacywetgeving Verantwoordelijkheid Verwerkersovereenkomst Verwerkersovereenkomst organisatie Wet- en regelgeving

Codegroep	Aantal codes	Codes
Relatie tot de leverancier	6	Application en Interface Security Business Continuity Management Contractmanagement Infrastructure en Virtualization Security Interoperability en Portability Vendor lock-in
Beschikbaarheid van de clouddienst	5	Business Continuity Management Datacenter Security Incident Management Infrastructure en Virtualization Security Kritisch systeem
Beheer van gebruikers	3	Endpoint Management Identity en Access Management Logging en Monitoring
Beheer van incidenten	5	Audit en Assurance Data Security Incident Management Logging en Monitoring Problem Management
Beheer van wijzigingen	7	Beveiligingsniveau Business Continuity Management Change management Endpoint Management Kennis Logging en Monitoring Risicomanagement
Back-up en recovery	1	Business Continuity Management
Transparantie	7	Advisering Infrastructure en Virtualization Security Kennis Outsourcing Threat and Vulnerability Management Transparantie Vertrouwen
Overheidsorganisatie	8	Baseline Informatiebeveiliging Overheid Betrouwbaarheid Gemeentelijke Inkoop bij IT Handreiking inkoop clouddiensten Kritisch systeem Overheidsorganisatie Referentie architectuur Veiligheidsregio ICT-kwaliteitsnormen

Bijlage 5: Tekstfragmenten uit de interviews en documentatie

Tabel 12 - Tekstfragmenten

ID	Tekstfragment	Code
1	het is nu met name met natuurlijk het hele traject dat loopt, met het Microsoft Office 365 verhaal, dat we ons er bewust van worden dat dat toch een hele nieuwe wereld is die op ons afkomt en waarbij security echt een dingetje is	Bewustzijn
2	Ja, heel erg, denk ik. Een grote invloed. Ehm ja, hoe moet ik dat uitleggen, want je krijgt er opeens een heel domein erbij, waar je eigenlijk zelf niet de regie over hebt, waarbij je afhankelijk bent van hoe een partij z'n zaken regelt. En ja, misschien beseft niet iedereen dat, maar nu met het hele Office 365 verhaal, gooi je echt ons hele hebben en houwen bij meneer Microsoft neer.	Afhankelijkheid
3	Nou denk ik daarentegen dat meneer Microsoft wel de laatste is die daar niet goed mee omgaat, want op het moment dat het daar misgaat en het vertrouwen van de wereld in Microsoft in één keer naar beneden gaat, dan heeft Microsoft denk ik wel een héél groot probleem. Dus dat is dan eigenlijk weer de geruststelling en de bevestiging dat je het daarmee ook meteen goed geregeld hebt.	Vertrouwen
4	Maar we moeten ons wel bewust van zijn dat vooral daar nu de accenten liggen en de kunst is om alles, ja wat je nog zelf in de hand hebt, wat vanuit je eigen omgeving van invloed is daarop, hè, daar kan Microsoft niks aan doen, als wij allemaal gekke dingen doen en er daardoor gekke dingen gebeuren. Ja, dan is dat toch echt aan ons.	Verantwoordelijkheid
5	je zou bijna geneigd zijn om te zeggen van: jôh, zit al in de cloud, Microsoft heeft het hartstikke goed geregeld, zo, dat is een zorg minder. Maar dat is een valkuil, denk ik	Bewustzijn Verantwoordelijkheid
6	Ja, het delen van al je dingen in die grote buitenwereld en alles gaat over de internetlijntjes en ja, je mag ervan uitgaan dat dat hele veilige, point-to-point verbindingen zijn. Maar, eh ja, wat is de garantie dat daar niet routes en wegen worden gevolgd waarop ingebroken kan worden.	Data Security Infrastructure en Virtualization Security
7	Bij Microsoft heb ik daar absoluut geen twijfel over, maar ja, we hebben natuurlijk allerlei leveranciers die dan weer zelf hostingpartijen in de arm nemen waarvan ik ook allemaal niet weet wat voor partijen dat zijn. Ja, daar kunnen dan toch weer onverwachte gaten komen. Je vertrouwt er altijd maar op dat het professionele bedrijven zijn die beseffen dat als het één keer misgaat dat dat niet goed is voor de marketing et cetera, maar ja, je geeft het wel een beetje uit handen	Infrastructure en Virtualization Security
8	was er voorheen nog wel van dat die dan wilde dat dat ook één of twee keer per jaar echt werd aangetoond. Dat je bij wijze van spreken dan een audit zou laten doen bij zo'n partij. Dan denk ik van ja, dat kan toch niet, want dan ga je dus uit een soort wantrouwen, ga je dat dan allemaal op je nek halen?	Audit en Assurance Vertrouwen

ID	Tekstfragment	Code
9	Nee, je moet erop kunnen vertrouwen dat het goed geregeld is.	Supply Chain Management Threat and Vulnerability Management
10	Maar ja, ik herken dan aan de andere kant wel van, ja, totdat het misgaat en je met z'n allen moet concluderen: het was níet goed geregeld. Dan zijn wij als opdrachtgever de klos en wat hebben we eraan dat de partij dan zegt van: ja sorry, dat hebben we inderdaad niet goed gedaan. Dan zijn we wel de klos. Hoe kun je dat nu borgen?	Supply Chain Management Threat and Vulnerability Management Verantwoordelijkheid
11	Dat vind ik best wel een lastige en daar loop ik eigenlijk telkens met verwerkersovereenkomsten tegenaan, van ja, dat je dat allemaal zo goed mogelijk probeert af te spreken. Maar je merkt dat een hoop hostingpartijen toch ook weer met Amerikaanse bedrijven in zee zijn gegaan. Het zijn vaak partijen met een moederbedrijf in Amerika. Dus dan kunnen we hier zeggen tegen de Nederlandse vestiging van, we willen het niet, maar dan zeggen zij: ja, maar ja, dat hebben we niet in de hand.	Data Security Privacywetgeving Verwerkersovereenkomst
12	Dat de data veilig opgeslagen is.	Data Security
13	Je hebt het zelf niet meer in de hand. Je moet vertrouwen op andere partijen.	Afhankelijkheid Vertrouwen
14	het eerste waar ik dan aan denk ik het hele AVG-verhaal. Dat heeft ook natuurlijk ook heel veel met beveiliging te maken. Ehm, dat je op basis van de AVG wet- en regelgeving stringente afspraken maakt met al je hostingpartijen. Nou ja, iedereen die in cloud computing wat met jouw gegevens doet. Dat is van de afgelopen jaren wel echt een hele duidelijke. Daarvoor leefde dat wat minder en werd uiteindelijk alleen maar bij de wat grotere contracten, eh, was het dan een dingetje waar rekening mee gehouden wordt. Nu merk je bij elk peanut systeempje, wat dan ook, eh, zijn we daar heel erg op gebrand en getriggerd om rekening te houden met die wet- en regelgeving en dat het goed geregeld is.	Data Security Privacywetgeving Verwerkersovereenkomst
15	waarvan je ook merkt bij kleinere partijen, dat ze dat soms ook vervelend en lastig vinden omdat dat, ja, best wel impact heeft op wat we eigenlijk vragen en eisen en dat ze dan vaak een beetje zielig gaan doen van: ja, maar daar hebben we het geld niet voor en daar zijn we te klein voor. Ja, en dan komt bij een contractmanager de gewetensvraag van: wat ga ik de organisatie adviseren? Niet in zee gaan met die partij die juist hetgeen heeft wat we nodig hebben? Zeg het maar..	Contractmanagement Data Security Risicomanagement
16	heb je niet meer in de hand en kun je alleen maar op basis van afspraken proberen af te dwingen	Contractmanagement Technisch applicatiebeheer
17	Maar hoe het in het echie gaat.. hè, en je gaat er niet naast zitten. Dus het wordt in die zin een hele, ja, eigenlijk een soort virtuele vertrouwenskwestie.	Vertrouwen
18	dat is iets waar we echt best wel veel mee te maken hebben en wat we natuurlijk met z'n allen niet altijd helemaal beseffen. Alle camerabeelden en toestanden vallen daar ook onder en dat is nu nog niet helemaal goed geregeld	Data Security Privacywetgeving

ID	Tekstfragment	Code
19	geen hoogste securityniveau intern vastgesteld	Beveiligingsniveau
20	verhaal nog niet op papier staat. Dat is een stap die we nog gaan doen	Dataclassificatie
21	dat we minimaal van externe partijen hetzelfde vragen. Dat klopt wel	Governance Supply Chain Management
22	dat betekent dus ook weer dat je je heel bewust bent van: wat is de gevoeligheid van gegevens en wat zetten we ervoor in	Bewustzijn Dataclassificatie Risicomanagement
23	Dat je gewoon weet hoe het moet zijn en welke controlemechanismen je dus nodig hebt.	Kennis
24	hoe we ooit de dienstverlening aan zijn gegaan. Wat ik al zei, het zal voor onze organisatie een worst zijn hoe KPN dingen doet. Als wij maar goed kunnen werken, als het maar veilig gebeurt en we er verder geen last van hebben en dit suggereert een beetje dat je gewoon echt, nou ja, tot een bepaald detailniveau gewoon weet wat zij doen en hoe ze beheren	Outsourcing Supply Chain Management
25	een andere, en ik denk een grotere, verantwoordelijkheid dan een commerciële partij	Overheidsorganisatie
26	Wij doen en praten namens de overheid. We doen alles voor de burgers en integriteit moet echt hoog in het vaandel staan.	Overheidsorganisatie
27	dat een ministerie van VWS weet ik veel 5 miljard niet kan verantwoorden, dat is eventjes in het nieuws en dan gaan we weer verder, maar als gegevens op straat liggen en nou ja, noem maar op, dan is de ophef groter	Data Security Incident Management
28	echt die AVG-dingen. De privacy, beschermde persoonsgegevens: die dingen. Dat merk je zeker op het moment dat je met commerciële partijen dat soort afspraken moet maken: die vinden het allemaal lastig en onzin en 'wat maakt het nou uit dat die gegevens in Amerika staan'	Contractmanagement Data Security Overheidsorganisatie Privacywetgeving
29	Imagoschade. En zeker omdat je in de publieke sector zit komt dat heel hard aan. Een commercieel bedrijf kan gewoon drie keer sorry zeggen, pompt er een hoop geld in, koopt het af bij de mensen die gedupeerd zijn en gaat weer verder. Maar als het vertrouwen in een overheidsinstantie geschaad is, dat is heel moeilijk om dat weer terug te krijgen.	Betrouwbaarheid Incident Management Overheidsorganisatie
30	Kan natuurlijk altijd beter. Ik denk dat de hele transitie van Citrix naar moderne werkplekken ons daarin helpt.	Kennis
31	ik denk dat we op het gebied van security nog niet helemaal het goede beeld hebben van: wat hebben we nou werkelijk nodig en hoe ver moeten we gaan	Beveiligingsniveau Risicomanagement
32	We vragen overal hetzelfde, eigenlijk maximale veiligheid. Je merkt dat de markt dat ook lastig vindt, omdat dit niet altijd relevant is voor de dienst die ze verlenen en de gegevens die ze verwerken.	Beveiligingsniveau Contractmanagement
33	Dat leggen we nu vooral bij KPN neer, natuurlijk. KPN heeft dan haar partner, volgens mij is het zelfs KPN InSpark. Omdat InSpark erg tegen KPN aan schuurt, merk ik dat dat toch niet altijd de ideale partij is.	Advisering

ID	Tekstfragment	Code
34	onze softwarebroker, waar we zeker ook goed mee kunnen sparren. Maar dat spitst zich toe op de Microsoft licenties die we hebben en de bijbehorende security aspecten	Advisering
35	Op een wat hoger level, als het gaat om algemene beveiligingsniveaus, zou het misschien weleens goed zijn als we een partij hebben waar we, nou ja, goed mee kunnen schakelen en wat adviezen nog van kunnen krijgen. Voor hoe je security het beste kunt benaderen en hoe je dat nou uiteindelijk per partij goed kunt regelen.	Advisering Beveiligingsniveau Governance
36	Ik denk dat je invloed er anders op is, hè. Als je het on-premises had, had je vaak een eigen IT-afdeling, je had er meer invloed op, in je eigen beheer.	Technisch applicatiebeheer
37	je er wel invloed op uitoefenen, maar je bent heel erg afhankelijk van een Microsoft bijvoorbeeld. Die gaan echt niet alles aan passen omdat jij dat wil. Dus je kunt niet meer heel specifiek dingen beveiligen zoals jij dat zou willen of zien.	Afhankelijkheid
38	Nou zijn die organisaties natuurlijk ook zo groot dat die echt wel weten hoe het moet. En je moet natuurlijk vertrouwen hebben in zo'n organisatie, dat die ook nakomen wat ze beloven en doen. En eh, maar goed, daar heb je dan een contract voor.	Vertrouwen
39	Volgens mij is het uitgangspunt dat we zo veel mogelijk ontzorgt willen worden en voor het gemiddelde systeem dat wij gebruiken kan dat ook prima.	Outsourcing
40	alles bij één leverancier onderbrengen, dan ben je totaal afhankelijk van die ene leverancier	Vendor lock-in
41	Ik denk dat het vooral het idee is dat je iets niet meer in eigen beheer hebt.	Technisch applicatiebeheer
42	Procedures en afspraken zijn ook heel belangrijk. De leveranciersafspraken, dat dat gewoon echt knip en klaar helemaal duidelijk is. Kijk, het kan altijd fout gaan of er kan de verkeerde persoon zitten, ik noem maar wat. Maar dat het gewoon goed afgedekt is	Contractmanagement
43	dat je je interne procedures daar goed op aanpast. Zodat als er onverhoopt wat gebeurt, je daar heel snel op kan reageren	Problem Management
44	zolang je dat zelf niet helder hebt, dan kun je.. Maar ik denk dat een leverancier dat nu vaak nog beter weet dan dat we het zelf weten. Maar goed, het is iets gezamenlijks.	Kennis
45	Je moet je ook afvragen, denk ik, hoe ver ga je? Waar heiligt het doel zeg maar nog de middelen die je ervoor inzet. Want als je voor iedereen alles onmogelijk gaat maken is het ook bijna geen werkbare situatie meer.	Beveiligingsniveau Risicomanagement
46	Ik denk dat databeveiliging de grootste uitdaging is.	Data Security
47	Ik heb geen idee hoe makkelijk onze systemen gehackt kunnen worden, of die van de leveranciers dan vooral, hè. Ik heb geen flauw idee. Worden daar weleens testen op gedaan? Hebben we daar rapporten van? Ik zou het niet weten.	Threat and Vulnerability Management

ID	Tekstfragment	Code
48	hebben wij zelf überhaupt een soort A-viertje bij wijze van, met: waar moet je op beveiligingsgebied aan denken als je een applicatie gaat aanschaffen? Ik weet dat namelijk niet. Misschien is het er ergens, maar dan is het niet bekend genoeg. Ik denk dat de communicatie, helderheid binnen de organisatie, nog verbeterd kan worden	Bewustzijn
49	dat wij als organisatie heel erg onder invloed zijn van wet- en regelgeving. Als daar wat in veranderd kan dat invloed hebben op onze beveiliging, dan kun je ineens je systemen aan moeten passen	Change management Wet- en regelgeving
50	beiden. Voor onszelf ook. Want ja, stel dat er een datalek is? Of een medewerker heeft een USB-stick laten liggen en dat is op straat gekomen? Of er is een leverancier gehackt? Hoe ga je daarmee om? Hoe kun je dan zo snel en efficiënt mogelijk ervoor zorgen dat er actie ondernomen wordt om de gevolgen daarvan ongedaan te maken, voor zover dat mogelijk is? En welke acties zet je uit om ervoor te zorgen dat dat in het vervolg niet meer zal voorkomen?	Incident Management Problem Management Supply Chain Management
51	Incident Management: er is wat gebeurt en dat moet weer werken of ongedaan gemaakt worden	Incident Management
52	je Problem Management is eigenlijk van: hoe ga je nu een structurele oplossing bieden om het niet meer te laten voorkomen	Problem Management
53	als er nieuwe wet- en regelgeving komt zoals de AVG, ja dan heb je te maken met leveranciers die dat moeten gaan inregelen, daar ben je een soort afhankelijk van. Maar aan de andere kant, volgens mij is het onmogelijk dat een leverancier dat niet gaat inregelen, anders moet je op zoek gaan naar iets anders waarschijnlijk.	Change management Wet- en regelgeving
54	Als je gaat kijken naar het beheerproces in de zin van Incident Management, Problem Management of je change management, ja, dan is het dat je er vaker een andere partij bij nodig hebt.	Change management Incident Management Problem Management
55	je hebt met veel verschillende partijen te maken, dus je moet veel afstemmen	Governance Supply Chain Management
56	stel dat er koppelingen zijn tussen verschillende applicaties: wat doe je dan bij een datalek, heeft dat dan ook invloed op andere applicaties?	Application en interface security Incident Management
57	De vraag is of je als organisatie meer risico loopt wanneer je je processen en systemen minder zelf beheert. Vaak zijn het namelijk ook wel bedrijven die er heel bedreven in zijn.	Outsourcing Risicomanagement Technisch applicatiebeheer Vertrouwen
58	Volgens mij zitten wij bij KPN in een tenant met anderen. Er was een keertje een foutje met de inlogsite en toen konden we precies zien welke applicaties van andere leveranciers daar ook in zaten. Maar ik moet zeggen, ik weet niet wat de afspraken daaromheen zijn.	Infrastructure en Virtualization Security
59	Ik weet ook niet wat hier het hoogste securityniveau zou zijn.	Beveiligingsniveau
60	Is het optimaal hier? Dat denk ik niet.	Data Security

ID	Tekstfragment	Code
61	Ik denk niet dat we daar echt duidelijke afspraken over hebben nu.	Infrastructure en Virtualization Security
62	We hebben ons eigen proces nog niet helemaal op orde, denk ik.	Governance
63	Ik heb bij aanbestedingen gezeten en dan worden hier wel vragen over gesteld aan de leverancier. Bijvoorbeeld over hun beheer van incidenten, change management.	Change management Incident Management
64	De contractmanager ontvangt rapportages. En dan is het goed voor ons, volgens mij.	Contractmanagement Logging en Monitoring
65	Wat interessant zou kunnen zijn is als we bijvoorbeeld van leveranciers zouden horen van: zoveel cyberaanvallen zijn er geweest en dit is de top vijf, en dit zijn de maatregelen die genomen zijn. Dat zou me er meer gevoel bij geven. En dan zou ik niet hele technische details hoeven horen, maar dan weet je wel beter wat ze eraan doen.	Supply Chain Management Threat and Vulnerability Management
66	De gevoeligheid van het type gegevens bij een datalek maakt ook wel uit. Maar ik denk bij een overheidsorganisatie, dat dat voor de media wel smullen is, zeg maar, voor mensen om dat bekend te maken en daar achteraan te gaan.	Incident Management Overheidsorganisatie
67	Voor iedere organisatie gaat hier om imagoschade, denk ik. Maar bij een publieke organisatie ligt dat gevoeliger voor mensen.	Incident Management Overheidsorganisatie
68	Er zijn natuurlijk zat opties. Je hebt seminars, bedrijven die je dat heel goed uit kunnen leggen, leveranciers zelf, en KPN kan er ook genoeg in doen, wel een beetje in eigen straatje, maar eh.. Je kunt ook mensen inhuren die er wat meer kaas van hebben gegeten.	Advisering
69	We hebben natuurlijk wel de beleidsmatige structuur. We hebben de Baseline Informatiebeveiliging Overheid (BIO) die gehanteerd wordt. Dat kun je wel zien als een soort framework en daar hangen dan verschillende maatregelen, beleidstukken aan vast, ook de technische kant daarachter.	Baseline Informatiebeveiliging Overheid Governance
70	Deze organisatie is in de basis wel heel erg van het aanpakken en niet zozeer van het noteren.	Governance Organisatiecultuur
71	Waar we binnen de organisatie mee bezig zijn, zijn servers: waar draait het dan? Wat voor vorm van een server is het: is het in de cloud of on-premises? Wat voor regelingen maak je daarmee?	Datacenter security
72	regie en controle op maatregelen. We willen over ons eigen systeem kunnen zeggen: oké, dit is wat we hebben ingericht en dit zijn de maatregelen die we genomen hebben	Governance
73	Wat ik zelf een van de grootste uitdagingen vind is de monitoring en controle daarop.	Supply Chain Management
74	Je zou toch een bepaalde vorm van regie moeten behouden, maar je merkt dat je dat bij veel leveranciers toch wel echt uit handen geeft, dat je echt een vertrouwensband op gaat leggen en dat daarin, vanuit de oude gedachte van goed leverancierschap, mensen elkaar op de blauwe oogjes vertrouwen.	Governance Supply Chain Management Vertrouwen

ID	Tekstfragment	Code
75	met cloud computing kan dat eigenlijk echt niet meer, omdat je de controle niet uit kunt voeren. Leveranciers kunnen zeggen dat ze een heel goed back-upbeleid hebben, maar dat merk je pas op het moment dat je het nodig hebt om een back-up terug te zetten. En als het dan niet werkt, ja, dan merk je dat dus te laat.	Business Continuity Management Supply Chain Management
76	een omslag gemaakt in expertise, andere vaardigheden	Vaardigheid
77	Je hebt voor je eigen IT wat IT-vaardigheid nodig. Verder heb je IT-security, beleidssecurity, organisatorisch security. Het kan een beetje zoeken zijn van wat heb je dan precies nodig.	Governance Kennis
78	Je bent afhankelijker van de maatregelen die de leverancier neemt.	Governance Technisch applicatiebeheer
79	je eigen mogelijkheden zijn daarin beperkt en tegelijk moet je zien te begrijpen hoe zij het dan technisch hebben ingericht	Kennis
80	Zelf hoef je dus technisch minder in te richten, dus die kennis kan afzwakken daarin, alleen het stukje van: wat zie ik nou op zo'n omgeving en wat doe ik daarmee..	Kennis
81	veel meer leveranciersmanagement van: oké, wat gaan we erover afspreken, of jij mij een rapport stuurt of... Daar zit veel meer de kennis in	Contractmanagement Kennis
82	er zijn interne ICT-richtlijnen. Dat is best wel een uitgebreid document en is gericht op criteria waaraan systemen moeten voldoen. Dat wordt gebruikt bij aanbestedingen en moet strikt worden gevolgd. Als er afwijkingen zijn, dan moet dit in de aanbesteding worden benoemd	Governance
83	de Gemeentelijke Inkoopvoorwaarden bij IT (GIBIT). Hier staan richtlijnen in rondom informatieveiligheid en IT waaraan systemen moeten voldoen tijdens het inkooptraject	Governance
84	de bedoeling dat er vanuit Inkoop gekeken wordt of er een risicoanalyse moet worden uitgevoerd op het gebied van privacy en informatieveiligheid. Er is een basisrisicoanalyse, en als hieruit komt dat er een diepgaandere risicoanalyse moet gedaan worden, dan is dit de vervolgstap.	Contractmanagement Risicomanagement
85	Je hebt bepaalde certificeringen en normen waar je aan moet voldoen.	Wet- en regelgeving
86	regels rondom informatie-uitwisseling	Data Security Wet- en regelgeving
87	Sommige persoonsgegevens liggen extra gevoelig. De AVG is een belangrijke op het gebied van wet- en regelgeving.	Data Security Privacywetgeving
88	We merken wel dat het lastig kan zijn om vanuit leveranciers garanties te krijgen op dat gebied. Dat ze bijvoorbeeld zeggen: we hebben een leverancier en waar die een datacenter heeft staan maakt ons niet uit. Of: het datacenter staat nu in Taiwan, maar of dat over een jaar nog zo is weten we niet. Of dat partijen zes datacenters hebben en dan niet specifiek kunnen aangeven waar onze data beland. Dus zodoende is dat wel echt een lastig onderwerp.	Data Security Privacywetgeving Verwerkersovereenkomst

ID	Tekstfragment	Code
89	Wat je wel kunt aangeven is: we willen in ieder geval zeker weten dat het niet op deze plekken terechtkomt.	Data Security Privacywetgeving Verwerkersovereenkomst
90	Maar ja, soms blijft het lastig, want je hebt ook nog back-upomgevingen. Voor het geval er sprake is van uitval op de huidige omgevingen. En dan kun je geografisch weer op een andere locatie terechtkomen.	Data Security Privacywetgeving Verwerkersovereenkomst
91	Het eigen beheer wordt gewoon een stuk minder.	Technisch applicatiebeheer
92	Je rol verandert heel erg van beheersmatig naar regie.	Governance
93	je hebt er bepaalde kennis en vaardigheden voor nodig om de regie te kunnen voeren.	Governance Kennis Vaardigheid
94	Je verliest een bepaalde controle, je kunt niet in een organisatie kijken die jou deze diensten levert en waar deze een datacenter heeft staan.	Supply Chain Management Transparantie
95	eigenlijk audits houden, maar dat is prijzig	Audit en Assurance
96	Voor kritische systemen worden er wel jaarlijks pentesten uitgevoerd en daar krijgen we dan de uitslag van.	Kritisch systeem Threat and Vulnerability
97	Er is een beeld dat het outsourcen, en daarin ook een stukje cloud computing, dat dat eigenlijk werk wegneemt. Hè, we zetten onze omgeving over naar jullie toe, dus jullie kunnen onze omgeving beheren, op dat vlak hoeven wij niets meer te doen.	Bewustzijn Outsourcing
98	Het is heel anders. Dat stukje regie, ik blijf het af en toe een beetje herhalen, maar dat is heel moeilijk hoor, regie houden. Financiële overwegingen spelen hier ook een rol in. Elke change, elke verandering, of elke module die je erbij wilt, heeft ook weer een financiële impact. Dat allemaal in kaart houden is ook lastig. En al de wijzigingen in de systemen moeten ook bijgehouden worden.	Change management Governance
99	Cloud computing heeft invloed op de gegevensbescherming, op waar je data zich bevindt. En dat is niet enkel in je individuele systemen, en op welke server dit draait en welke locatie, maar ook koppelingen tussen systemen en welke informatie tussen systemen wordt overgeheveld.	Data Security
100	wie kan daar dan vervolgens bij, hoe is de toegang geregeld. Dat is echt essentieel	Identity en Access Management
101	Het is letten op een stukje integriteit van je gegevens. Je moet wel zeker weten dat dit bij koppelingen tussen systemen goed gaat.	Application en interface security Data Security
102	Je moet wel zeker weten dat dit bij koppelingen tussen systemen goed gaat. Daar is wederom ook weer duidelijkheid over nodig met leveranciers.	Contractmanagement Data Security
103	risicoanalyse op het gebied van gegevensbescherming is wel uitgebreider geworden door cloud computing	Data Security Risicomanagement

ID	Tekstfragment	Code
104	beschikbaarheid van gegevens ook heel belangrijk. Wat gebeurt er bij uitval? Is er dan een overdracht naar een ander datacenter? Wat voor afspraken liggen erover? Dat is nog essentiëler geworden	Business Continuity Management
105	Retentie daarin ook, hè. We hebben leveranciers af en toe die zeggen: nog een jaar nadat het contract verbroken is behouden we je gegevens. Dat vind ik een heel slecht idee. Dus daar moet je echt wel goed naar kijken wat daar voor afspraken liggen.	Contractmanagement Data Security
106	Je bent gewend om je eigen back-upbeleid te hebben voor je hele omgeving en het versplinterd gewoon heel erg op het moment dat je overgaat naar cloud computing.	Business Continuity Management
107	In bepaalde zaken wordt hier rekening mee gehouden, in bepaalde zaken ook niet. Je merkt dat dat niet altijd kan.	Infrastructure en Virtualization Security
108	Wat we bijvoorbeeld wel met een leverancier afspreken is van: stel, er vindt een aanval plaats op de omgeving, een DDoS-aanval bijvoorbeeld, dat je dan in elk geval back-up servers moet hebben om je systeem draaiende te kunnen houden.	Datacenter security
109	Bij één applicatie kan deze terugvallen op de testomgeving.	Business Continuity Management
110	Ja, op heel veel manieren zijn er scheidingen aangebracht.	Infrastructure en Virtualization Security
111	We zitten in de Citrix-omgeving in dezelfde omgeving, maar op verschillende servers.	Infrastructure en Virtualization Security
112	Leveranciers zitten ook op verschillende omgevingen, zodat ze niet zomaar bij bepaalde data kunnen.	Infrastructure en Virtualization Security
113	Er zal altijd de vraag gesteld worden of de leverancier bij de data kan en dat data niet gemengd moet kunnen worden met die van andere klanten. Dat wordt altijd uitgevraagd.	Infrastructure en Virtualization Security
114	We moeten onze data ook gemakkelijk kunnen overzetten, uit veiligheidsoverwegingen.	Interoperability en portability
115	Is het niet veilig, dan moeten we onze data snel weg kunnen halen. Ook als het gaat om data van verschillende systemen. Als 1 systeem niet veilig blijkt te zijn, moet de verbinding met andere systemen kunnen worden verbroken.	Business Continuity Management
116	De mogelijkheden hierin verschillen per leverancier. De maatregelen worden gebaseerd op risicomanagement, het gaat er niet per se om dat we dit in de hoogst mogelijke mate willen implementeren.	Business Continuity Management Infrastructure en Virtualization Security Risicomanagement
117	We kijken naar beschikbaarheid, integriteit en vertrouwelijkheid en uiteindelijk die classificatiemethodes, daar kijken we wel naar, maar strikte reglementen eromheen zijn er niet.	Dataclassificatie
118	We gaan niet per se voor het hoogste niveau qua beveiliging, hoe beschikbaar het systeem moet zijn hangt wel af van de informatie die daarin staat. Kritieke systemen moeten altijd beschikbaar zijn.	Beveiligingsniveau Business Continuity Management Kritisch systeem Risicomanagement

ID	Tekstfragment	Code
119	Data kan dus geclassificeerd worden op basis van beschikbaarheid, integriteit en vertrouwelijkheid. Integriteit gaat dan over juistheid, dat je je informatie actueel hebt, klopt de data wel echt? En de beschikbaarheid zit echt in de service level agreements: hoeveel service krijg je, waar houdt de servicedesk zich mee bezig? Wat betreft vertrouwelijkheid komt dit terug in een privacy overeenkomst of verwerkersovereenkomst.	Dataclassificatie
120	Dat is zo. Dingen als wachtwoordbeleid of toegankelijkheid, dat werkt gewoon hetzelfde. Wederom benadrukkend dat het ook wel afhangt van de applicatie.	Governance Supply Chain Management
121	Deels. Ja, op basis van dat we initieel een risicoanalyse uitvoeren. Controle hierop vindt heel weinig plaats.	Data Security
122	er worden vaak duidelijke afspraken gemaakt met leveranciers rondom beheer, hoe veranderingen worden gemaakt	Change management Contractmanagement Technisch applicatiebeheer
123	er is een wijzigingscommissie voor de grootste wijzingen. Daar is dus een methode in vastgelegd.	Change management
124	Het stukje consequenties als je hiervan afwijkt wordt gewoon weinig bekeken.	Change management
125	We hebben wel bepaalde rapportages, dus naar aanleiding van deze rapportages kun je wel een bespreking hebben.	Logging en Monitoring Supply Chain Management
126	het stukje Problem Management daarin is nog niet volledig ingericht. Wel voor bepaalde systemen, maar niet voor alle systemen	Problem Management
127	Logging is sowieso iets wat standaard meegenomen wordt.	Contractmanagement Logging en Monitoring
128	Dat wordt in de ICT-richtlijnen ook direct meegenomen. Dus daar zit wel een stukje waarop controle kan plaatsvinden.	Contractmanagement Logging en Monitoring
129	de logging van KPN, omdat alles via single sign-on gaat	Identity en Access Management Logging en Monitoring
130	Audits gebeuren nagenoeg niet.	Audit en Assurance
131	Er worden wel pentesten gedaan voor de kritieke systemen.	Kritisch systeem Threat and Vulnerability Management
132	Contractueel leggen we wel de mogelijkheid tot het uitvoeren van audits vast.	Audit en Assurance Contractmanagement
133	De eindverantwoordelijkheid zit echt bij je eigen organisatie, ook al voelen we dit niet altijd zo. Omdat het zo ver buiten je eigen organisatie ligt neemt het af en denk je: zij zullen het wel beter weten	Verantwoordelijkheid

ID	Tekstfragment	Code
134	Ik denk wel dat, doordat wij een overheidsorganisatie zijn, dat we wel al een startpunt hebben van wat specifiekere eisen die we stellen. Wij hebben meerdere leveranciers gehad, die zeiden van: jôh, jullie zijn wel heel streng richting ons. Misschien niet in die woorden, maar daar kwam het wel op neer. Maar het enige antwoord dat wij kunnen geven is simpelweg: wij hebben daar gewoon een functie in, we moeten wel. Je hebt toch een voorbeeldfunctie binnen het land.	Contractmanagement Overheidsorganisatie Verantwoordelijkheid
135	Er is een hele grote groep van inwoners die vertrouwd dat jij vertrouwelijk omgaat met informatie en dat jij het systeem zo hebt ingericht dat dat ook mogelijk is.	Betrouwbaarheid Data Security Overheidsorganisatie
136	Dat is een van de zaken waar dat groots speelt, dat zie je ook bij andere organisaties die gehackt zijn. Als dat een overheidsorganisatie is, is dat extra pijnlijk.	Data Security Overheidsorganisatie
137	als je het hebt over gevoelige en bijzondere persoonsgegevens, daar hebben wij wat meer mee te maken. Als overheidsorganisatie heb je wel een bepaalde vorm van een voorbeeldfunctie, je staat meer in de schijnwerpers als het fout gaat, en je moet je echt op een ander niveau verantwoorden, ook aan het Rijk	Data Security Overheidsorganisatie Privacywetgeving Verantwoordelijkheid
138	Ik denk wel dat een belangrijke is: het feit dat wij een overheidsorganisatie zijn maakt ook dat wij gekoppeld zitten en veel ketenpartners hebben die ook in de overheid zitten. En dat is gewoon een essentiële, ook vooral met cloud computing, waarbij je toch nog makkelijker hebt dat systemen aan elkaar gekoppeld worden.	Application en interface security Supply Chain Management
139	Wij hebben gedeelde systemen met andere overheidsorganisaties. Dus stel, er zou wat gebeuren, dan heeft dat wel invloed op andere instellingen. En niet dat dat belangrijker is dan bij bedrijven, maar wel hè, de informatie, en de noodzaak tot de beschikbaarheid van deze instanties ligt toch vaak wat hoger.	Kritisch systeem Overheidsorganisatie Supply Chain Management
140	Bij cloud computing worden externe onderzoeksbureaus en expertise ook steeds belangrijker. Het feit dat je een overheidsorganisatie bent kan het ook makkelijker maken, doordat je sneller andere instanties kan inschakelen die jou ondersteunen bij een incident. Je hebt gewoon best wel veel instanties die gemaakt zijn om de overheid te ondersteunen bij het ophogen van het informatiebeveiligingsniveau. Dat geeft ons steun op veel vlakken: richtlijnen voor allerlei zaken, maar ook bij incidenten. Het NCSC is daar een grote in. Je hebt het IBD, onderdeel van de VNG. Op het gebied van cloud computing kun je ontzettend veel advies krijgen.	Advisering Overheidsorganisatie
141	Als je kijkt naar de basisbehoefte en het aanschaffen van nieuwe systemen dan zitten die daar direct in. Dat is wel goed ingericht. Op het moment van aankoop en er vinden wijzigingen plaats dan hebben we daar een wijzigingscommissie voor. Ook daar zit enige controle op.	Change management

ID	Tekstfragment	Code
142	als de wijzigingscommissie in de praktijk wordt genegeerd en er een module wordt aangezet of verandering wordt doorgevoerd in het systeem, dan zal daar niet snel nogmaals een controle plaatsvinden.	Change management
143	in het extra's toevoegen kan security minder worden meegenomen. Dat gaat met cloud computing heel snel, je kunt snel wijzigingen doorvoeren en een leverancier kan dat voor je uitvoeren	Change management
144	hoeveel IT-kennis heb je nodig	Governance Kennis
145	in het bijzonder als het gaat om koppelingen en de beveiliging van technische koppelingen	Application en interface security Kennis
146	Nu we over zijn naar de cloudomgeving van Microsoft worden daar wel trainingen in genomen, omdat daar wel belangrijke onderwerpen liggen en zijn we ook aan het kijken van security technisch, wat kan daarvoor ontwikkeld worden? Wij hebben ook de licentie: de leveranciers, de broker partij. Voor bepaalde licenties hebben ze er ook trainingen bij. We hebben natuurlijk KPN die ons veel informeert over zaken. Die kunnen we ook wel aanspreken op het moment dat we echt specifieke kennis nodig hebben. Er zijn veel websites en producten beschikbaar. Het IBD is daar denk ik een heel goed voorbeeld van, die echt op de ontwikkelingen van de markt zit. Daar zit ook echt nog wel een stukje van de Rijksoverheid in, die producten levert zoals de GIBIT die je heel concreet kunt gebruiken. En dat is wel heel essentieel, denk ik. Er zijn zoveel onderdelen van cloud computing waar je aan moet denken, als daar zo producten voor worden aangeleverd behoud je dat overzicht.	Advisering
147	Dat heb ik nog niet gezien, een algemeen document.	Governance
148	Het is gericht op informatiebeveiliging, het voorkomen van een datalek. Heel terug naar de kern gebracht.	Data Security Governance
149	dat je ook geen buitenstaanders toegang geeft die geen rechten hebben	Governance Identity en Access Management
150	de hele ICT-omgeving zelf. De tweefactorauthenticatie, de werkbubbel op je telefoon. De telefoons worden ook weer ingenomen, dat was eerder niet echt het geval. Je kunt ze nu ook op afstand wissen. Riskant gebruik wordt gedetecteerd	Endpoint management Governance Identity en Access Management
151	Via de cloud loop je natuurlijk extra risico. Eerder hadden we alles op servers bij KPN gehost staan en hadden we daar een directe verbinding naar. Nu kun je vanuit de hele wereld inloggen. Dus je moet het ook wel gaan verbeteren.	Infrastructure en Virtualization Security

ID	Tekstfragment	Code
152	Met cloud computing geef je eigenlijk toegang aan iedereen die internet heeft, dus de beveiliging daarvan wordt veel belangrijker. Je wordt veel kwetsbaarder voor aanvallen van buitenaf, omdat iedereen je kunt aanvallen. Cloud computing kun je niet zonder adequate beveiliging doen. Anders komt alles zo op straat te liggen.	Infrastructure en Virtualization Security
153	Je moet bijvoorbeeld veel beter in de gaten houden dat gebruikers die uit dienst gaan geen toegang meer hebben. Vroeger kon je iemand simpelweg de toegang tot het fysieke gebouw ontzeggen, maar nu kan iemand nog steeds bij data als hij bijvoorbeeld zijn telefoon niet inlevert.	Identity en Access Management
154	Je maakt ook gebruik van een systeem dat veel meer bedrijven gebruiken. Dus als je als hacker geld wilt verdienen of de boel gaat versleutelen wordt het veel rendabeler om je te richten op een systeem wat heel veel bedrijven gebruiken, in plaats van op wat 1 organisatie gebruikt. Als je een zwak punt ontdekt, dan kun je duizenden bedrijven lastvallen en afpersen in plaats van maar één.	Threat and Vulnerability Management
155	De apparaten die mensen gebruiken. Mensen vinden het fijn om thuis hun eigen PC te gebruiken, dat kan dus niet meer. Je kunt alleen nog de webbased varianten gebruiken van applicaties.	Endpoint management
156	Updates draaien. Bij PC's en telefoons worden updates afgedwongen.	Endpoint management
157	Je draagt vertrouwen over aan je leveranciers. Je levert jezelf over aan de leverancier.	Vertrouwen
158	Er is een koppeling tussen Azure en een applicatie van personeelszaken. Als iemand uit de applicatie bij personeelszaken wordt gehaald, heeft deze persoon ook gelijk geen toegang meer tot andere applicaties. Met een BI-tool wordt er nog een extra controle gedaan. Daarmee wordt elke nacht gecheckt welke gebruikers actief staan in Azure en welke in de applicatie van personeelszaken; om te checken of dit overeenkomt. Eventuele verschillen worden in de ochtend gemeld.	Identity en Access Management
159	Je moet dingen doorzoekbaar maken en je kunt dingen niet zomaar weggooien. Dit valt onder de wet Openbaarheid van bestuur.	Data Security
160	Verder heb je privacywetgeving, waaronder het recht om vergeten te worden. Niet meer persoonlijke gegevens opslaan dan echt noodzakelijk is voor accounts in applicaties.	Privacywetgeving
161	We zijn afhankelijk van Microsoft, een Amerikaans bedrijf.	Privacywetgeving
162	Er zijn echter weinig alternatieven. Amazon is bijvoorbeeld ook een Amerikaans bedrijf.	Privacywetgeving
163	Bij aanbestedingen kunnen certificeringen een rol spelen, omdat applicaties moeten voldoen aan de geldende wet- en regelgeving.	Contractmanagement Wet- en regelgeving

ID	Tekstfragment	Code
164	Vendor lock-in is een risico. Eigenlijk heb je dat met Microsoft, want je maakt jezelf compleet afhankelijk. Maar ook bij andere applicaties.	Vendor lock-in
165	Cloud exit strategieën hebben niet echt de aandacht.	Business Continuity Management
166	Je bent met cloud computing erg afhankelijk van leveranciers.	Afhankelijkheid
167	Je kunt zelf dingen redelijk instellen, per app en type device	Endpoint management
168	je ziet bijvoorbeeld dat Microsoft regelmatig functies kan verwijderen of juist toevoegen, waar je helemaal niet op zit te wachten en dan móet je mee	Afhankelijkheid Vendor lock-in
169	KPN zit er ook wel bij natuurlijk, om mee te kijken. Die hebben de inrichting gedaan. Het is wel goed om een externe partij, in dit geval KPN, mee te laten kijken of je geen domme dingen doet.	Advisering
170	Dat is wel een probleem. Ze maken vrij makkelijk global admins aan. Af en toe zie ik dat. Eén keer ook een externe, zonder overleg.	Identity en Access Management Supply Chain Management
171	Een onafhankelijke, derde partij die het allemaal eens naloopt. Dat kan heel leerzaam zijn.	Advisering Supply Chain Management
172	je merkt dat er toch gewoon een soort van goed vertrouwen is in KPN. Dat vind ik lastig. Het blijft toch een zakelijke relatie: wij vragen, zij draaien. We moeten niet willen dat zij zaken doen op eigen initiatief, zonder dat wij ervan afweten.	Supply Chain Management Transparantie
173	Een combinatie van SaaS (Microsoft 365) en IaaS (Azure). Voor de meldkamer gaan we een hybride cloudoplossing aanbieden, namelijk: Citrix Virtual Apps en Desktops for Azure. Deze oplossing biedt de mogelijkheid om samen te werken met een andere organisatie, waarbij onze IT-netwerken zoveel mogelijk gescheiden worden gehouden. Dat is veiliger.	Infrastructure en Virtualization Security
174	Die scheiding is beter geworden nu we zijn overgestapt naar de Modern Workplace. Als KNP wat fout deed in de gedeelde omgeving bij Citrix zag je bijvoorbeeld in één keer de printers van heel andere organisaties. Je blijft echter ook hierin afhankelijk van hoe de leverancier dit doet. Voor zover ik weet wordt hier niet expliciet aandacht aan besteed vanuit onze organisatie.	Infrastructure en Virtualization Security
175	Daar doen we ons best voor, om dat goed te doen. Aandachtspunt is wel dat je nu met de migratie vanaf de netwerkschijf naar SharePoint/Teams heel veel data hebt waarvan je niet exact weet wat het is. En dat wordt in één keer gekopieerd en iedereen kan daar gewoon in grasduinen binnen een afdeling. Dat wordt overgezet per afdeling. Ik weet niet of er gevoelige zaken tussen zitten die er eigenlijk niet hadden moeten zijn. Maar het is te veel om na te kijken, dus je moet erop vertrouwen dat mensen dat goed hebben opgeslagen.	Data Security Dataclassificatie

ID	Tekstfragment	Code
176	Dat is wel vastgelegd, qua rollen wie wat doet. Maar je ziet dat daar af en toe dingen in misgaan. We merken afwijkingen wel gauw op, via controles. Maar dat zou strakker georganiseerd moeten zijn, zodat het niet meer voorkomt.	Change management
177	KPN zou niet meer zomaar een account moeten kunnen aanmaken. We moeten in het algemeen niet zomaar iemand global admin rechten kunnen geven.	Change management
178	Alles wat je doet, en wat KPN doet, wordt gelogd.	Logging en Monitoring
179	Audits lijken mij heel goed, omdat je altijd dingen over het hoofd kunt zien. En je kunt ervan leren. Verder ook aantonen dat je niets raars doet; dat je verantwoordelijk en betrouwbaar bent.	Audit en Assurance Betrouwbaarheid Verantwoordelijkheid
180	Het lijkt me goed als de gehele security inrichting jaarlijks door een derde, onafhankelijke partij wordt nagelopen. Dan weten we waar we staan. Auditrapporten kunnen ook als bewijs dienen, onder andere richting je management. Dus we zouden meer kunnen doen op dit gebied.	Audit en Assurance Verantwoordelijkheid
181	Opdrachten worden niet altijd duidelijk geformuleerd.	Governance Supply Chain Management
182	Ze worden vaak niet SMART geformuleerd hier.	Governance Supply Chain Management
183	Ik denk dat we niet altijd helder hebben wat we precies willen vragen. En er is ook maar heel weinig vastgelegd binnen deze organisatie. Maar daar maken we nu wel meer stappen in.	Kennis Supply Chain Management
184	Er heerst heel erg een hands-on-mentaliteit. En mensen zijn gewend veel vrijheid te bezitten. Zaken vastleggen, vrijheden beperken: dat ligt gevoelig.	Governance Organisatiecultuur
185	we moeten qua IT en security echt strakkere richtlijnen hebben, er komen gewoon te veel risico's bij kijken	Governance Risicomanagement
186	Je hebt natuurlijk te maken met gegevens van burgers / organisaties die er niet vrijwillig voor kiezen om in je systemen te staan.	Wet- en regelgeving
187	Je legt als overheidsorganisatie dingen vast vanuit een wettelijke taak. En dan vind ik eigenlijk dat je daar extra zorgvuldig mee om moet gaan; dat je betrouwbaar moet zijn.	Betrouwbaarheid Overheidsorganisatie
188	daarnaast word je ook nog door ze betaald, via belastinggeld. Dus dan moet je je zaken gewoon netjes regelen	Betrouwbaarheid Overheidsorganisatie
189	Je raakt veel vertrouwen kwijt.	Vertrouwen
190	Een datalek bij een overheidsorganisatie kan extra smeuïg zijn, denk ik.	Incident Management Overheidsorganisatie
191	voor slachtoffers doorgaans niet mogelijk om in zo'n situatie te zeggen van: ik stap over naar een andere organisatie, want hier heb ik geen vertrouwen meer in	Afhankelijkheid Vertrouwen
192	extra verwijten, omdat je als overheidsorganisatie toch een publiek taak hebt	Overheidsorganisatie Verantwoordelijkheid
193	Er worden hier stappen in gemaakt. Maar ik denk dat we nog steeds veel op KPN leunen op dit vlak. We hebben nog meer kennis nodig zelf.	Kennis

ID	Tekstfragment	Code
194	Ik denk vooral op het gebied van de inrichting van security	Governance Kennis
195	Je merkt wel dat als je het opbrengt dat je er dan wel veel ondersteuning bij krijgt. Microsoft en KPN spelen hier een rol in. Dus de leveranciers.	Advisering
196	Je kunt natuurlijk wel bij een vergelijkbare overheidsorganisatie gaan kijken. Een derde partij die een audit uitvoert kan hierin ook van betekenis zijn.	Advisering
197	Verwerker heeft geen zeggenschap over de ter beschikking gestelde persoonsgegevens.	Data Security Privacywetgeving Verwerkersovereenkomst organisatie
198	Verwerker werkt op verzoek van Verwerkingsverantwoordelijke te allen tijde mee aan een gegevensbeschermingseffect-beoordeling (PIA).	Audit en Assurance Data Security Verwerkersovereenkomst organisatie
199	Personen in dienst van, dan wel werkzaam ten behoeve van Verwerker, evenals Verwerker zelf, zijn verplicht tot geheimhouding met betrekking tot de persoonsgegevens waarvan zij kennis kunnen nemen, behoudens voor zover een bij, of krachtens de wet gegeven voorschrift tot verstrekking verplicht. De medewerkers van Verwerker tekenen hiertoe een geheimhoudingsverklaring. 5.2 Indien Verwerker op grond van een wettelijke verplichting gegevens dient te verstrekken, zal Verwerker de grondslag van het verzoek en de identiteit van de verzoeker verifiëren en zal Verwerker Verwerkingsverantwoordelijke onmiddellijk, voorafgaand aan de verstrekking, ter zake informeren. Tenzij wettelijke bepalingen dit verbieden.	Privacywetgeving
200	Verwerker houdt een gedetailleerd logboek bij van alle (vermoedens van) inbreuken op de beveiliging, evenals de maatregelen die in vervolg op dergelijke inbreuken zijn genomen	Data Security Incident Management Logging en Monitoring Verwerkersovereenkomst organisatie
201	Verwerkingsverantwoordelijke is te allen tijde gerechtigd de verwerking van persoonsgegevens te (doen) controleren.	Audit en Assurance Data Security Verwerkersovereenkomst organisatie
202	Verwerker blijft in deze gevallen te allen tijde aanspreekpunt en verantwoordelijk voor de naleving van de bepalingen uit deze verwerkersovereenkomst. Verwerker garandeert dat Paraaf Verwerker en Verwerkingsverantwoordelijke: pag. 4 (5) deze derden schriftelijk minimaal dezelfde plichten op zich nemen als tussen Verwerkingsverantwoordelijke en Verwerker zijn overeengekomen en zal Verwerkingsverantwoordelijke, op diens verzoek, inzage verschaffen in de overeenkomsten met deze derden waarin deze plichten zijn opgenomen.	Data Security Privacywetgeving Supply Chain Management Verwerkersovereenkomst organisatie

ID	Tekstfragment	Code
203	Verwerker informeert ogenblikkelijk Verwerkingsverantwoordelijke indien een faillissement dreigt dan wel surseance van betaling, zodat Verwerkingsverantwoordelijke tijdig kan beslissen de persoonsgegevens terug te vorderen alvorens faillissement wordt uitgesproken.	Business Continuity Management Data Security Verwerkersovereenkomst organisatie
204	De toereikendheid van de informatiebeveiliging blijkt uit: a. Certificering; b. Periodieke externe controles zoals audits of TPM's (bijv. ISAE3xxx SOC type II); c. Een Assurance rapport met conclusie over de bevindingen van de auditor; d. Eigen controles of eigen mededelingen.	Audit en Assurance Verwerkersovereenkomst organisatie
205	De Baseline Informatiebeveiliging Overheid (BIO) is geheel gestructureerd volgens NEN-ISO/IEC 27001:2017, bijlage A en NEN-ISO/IEC27002:2017. Het Forum Standaardisatie heeft deze normen opgenomen in de 'pas toe-of-leg uit'- lijst met verplichte standaarden voor de publieke sector, volgens het comply or explain principe. Dit betekent dat de overheid deze normen toepast tenzij er expliciet geformuleerde redenen zijn om dat niet te doen. De BIO beschrijft de invulling van de NEN-ISO/IEC 27001:2017 en de NEN-ISO/IEC 27002:2017 voor de overheid.	Baseline Informatiebeveiliging Overheid Overheidsorganisatie Wet- en regelgeving
206	Informatiebeveiliging vormt een belangrijk kwaliteitsaspect van de informatievoorziening van de overheid. Het beveiligen van informatie is echter geen eenmalige zaak, maar een proces waarbij steeds de Plan-Do-Check-Act cyclus wordt doorlopen. Het doorlopen van dit proces is een verantwoordelijkheid van het lijnmanagement. Om te voorkomen dat informatie en informatiesystemen te licht of te zwaar worden beveiligd, vormt risicomanagement een belangrijk onderdeel in dit proces.	Baseline Informatiebeveiliging Overheid Governance
207	Waar naleving (nog) niet volledig mogelijk is, dienen de bedrijfsonderdelen via een 'explain' de eventuele risico's inzichtelijk te maken aan hun ketenpartners.	Baseline Informatiebeveiliging Overheid Supply Chain Management
208	De BIO is van toepassing op de overheid. In verband hiermee is de BIO van toepassing op de volgende bestuursorganen: l Rijksdienst l Provincies l Waterschappen l Gemeentes Daarnaast wordt aanbevolen de BIO te verankeren in de taakomschrijving van de overige overheidsorganisaties en organisaties waarmee de overheid publiek-privaat samenwerkt en private samenwerkingen waarbij de overheid de enige aandeelhouder is.	Baseline Informatiebeveiliging Overheid Overheidsorganisatie

ID	Tekstfragment	Code
209	De overheid past risicomanagement toe om tot de juiste beveiliging van informatie en informatiesystemen te komen binnen de context van de bedrijfsdoelstellingen. Risicomanagement is het inzichtelijk en systematisch inventariseren, beoordelen en – door het treffen van maatregelen – beheersbaar maken van risico's en kansen, die het bereiken van de doelstellingen van de organisatie bedreigen dan wel bevorderen, op een zodanige wijze dat verantwoording kan worden afgelegd over de gemaakte keuzes.	Baseline Informatiebeveiliging Overheid Risicomanagement
210	De overheid volgt de standaarden die op de 'pas toe of leg uit'-lijst van het Forum Standaardisatie (hierna het Forum) staan. De BIO is gebaseerd op de NEN-ISO/IEC 27002:2017 en vanuit de BIO wordt verwezen naar de NEN-ISO/IEC 27001:2017, beide standaarden staan op de 'pas toe of leg uit'-lijst van het Forum.	Baseline Informatiebeveiliging Overheid Wet- en regelgeving
211	Om risicomanagement hanteerbaar en efficiënt te houden, kiest de BIO voor een diepgang van de uitwerking van het risicomanagement die proportioneel is aan de te beschermen belangen in combinatie met relevante dreigingen.	Baseline Informatiebeveiliging Overheid Risicomanagement
212	Daarom onderscheidt de BIO drie basisbeveiligingsniveaus (BBN's). Voor BBN1 ligt de nadruk op 'wat mag minimaal verwacht worden?'. Voor BBN2 ligt de nadruk op de bescherming van de meest voorkomende categorieën informatie volgens het principe 'valt de maatregel onder goed huisvaderschap; toont deze beveiliging de betrouwbare overheid?'. BBN3 is van toepassing op gerubriceerde informatie Departementaal Vertrouwelijk dan wel vergelijkbaar vertrouwelijk bij andere overheidslagen, waarbij weerstand tegen statelijke actoren of vergelijkbare dreigers nodig is.	Baseline Informatiebeveiliging Overheid Beveiligingsniveau
213	De keuze voor een BBN wordt gemaakt door de proceseigenaar en is gebaseerd op risicomanagement. De BIO gaat vergezeld van een methode van risicoafweging, de BBN-toets.	Baseline Informatiebeveiliging Overheid Governance Risicomanagement
214	De organisatie dient te beschikken over een registratie van overheidsmaatregelen waaraan niet of nog niet geheel kan worden voldaan. Dit zijn explains volgens het 'comply or explain' principe. Daarbij worden tevens de daaruit voortvloeiende risico's aangegeven.	Baseline Informatiebeveiliging Overheid Governance Wet- en regelgeving

ID	Tekstfragment	Code
215	In het geval dat een organisatie informatie aan ketenpartners toevertrouwt, blijft deze organisatie er verantwoordelijk voor dat ketenpartners de toevertrouwde informatie zorgvuldig beschermen. De organisatie moet daarom aansluitvoorwaarden eisen of stellen aan de leverende of afnemende partij. Tevens moet de organisatie leveringsgaranties bieden aan de afnemende partij. De organisatie moet hiervoor inzichtelijk hebben van welke informatiesystemen en -infrastructuren zij afhankelijk is, welke afhankelijk zijn van haar en hoe de governance van beide hierop is ingericht.	Application en interface security Baseline Informatiebeveiliging Overheid Governance Supply Chain Management Verantwoordelijkheid
216	Periodiek leggen alle dienstenleveranciers verantwoording af via een Statement of Compliance (of deel-ICV; met toepasselijke reikwijdte) aan de opdrachtgever bij de overheid.	Audit en Assurance Baseline Informatiebeveiliging Overheid Supply Chain Management
217	5 Informatiebeveiligingsbeleid	Baseline Informatiebeveiliging Overheid Governance
218	Er is een informatiebeveiligingsbeleid opgesteld door de organisatie. Dit beleid is vastgesteld door de leiding van de organisatie en bevat ten minste de volgende punten: a. De strategische uitgangspunten en randvoorwaarden die de organisatie hanteert voor informatiebeveiliging en in het bijzonder de inbedding in en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid. b. De organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden. c. De toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers. d. De gemeenschappelijke betrouwbaarheidseisen en normen die op de organisatie van toepassing zijn. e. De frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd. f. De bevordering van het beveiligingsbewustzijn.	Baseline Informatiebeveiliging Overheid Governance
219	7 Veilig personeel	Baseline Informatiebeveiliging Overheid Bewustzijn
220	8 Beheer van bedrijfsmiddelen	Baseline Informatiebeveiliging Overheid Bewustzijn Dataclassificatie Endpoint management

ID	Tekstfragment	Code
221	9 Toegangsbeveiliging	Baseline Informatiebeveiliging Overheid Endpoint management Identity en Access Management
222	Er is een actueel mandaatregister of er zijn functieprofielen waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten.	Baseline Informatiebeveiliging Overheid Change management
223	11 Fysieke beveiliging en beveiliging van de omgeving	Baseline Informatiebeveiliging Overheid Datacenter security
224	De restore procedure wordt minimaal jaarlijks getest of na een grote wijziging om de goede werking te waarborgen als deze in noodgevallen uitgevoerd moet worden.	Baseline Informatiebeveiliging Overheid Business Continuity Management
225	Gebeurtenissen registreren Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	Baseline Informatiebeveiliging Overheid Logging en Monitoring
226	In de inkoopcontracten worden expliciet prestatie-indicatoren en de bijbehorende verantwoordingsrapportages opgenomen.	Audit en Assurance Baseline Informatiebeveiliging Overheid Contractmanagement
227	Leveranciers moeten hun keten van toeleveranciers bekendmaken en transparant zijn over de maatregelen die zij genomen hebben om de aan hun opgelegde eisen ook door te vertalen naar hun toeleveranciers.	Baseline Informatiebeveiliging Overheid Data Security Verwerkersovereenkomst
228	Jaarlijks wordt de prestatie van leveranciers op het gebied van informatiebeveiliging beoordeeld op vooraf vastgestelde prestatie-indicatoren, zoals in het contract opgenomen is.	Audit en Assurance Baseline Informatiebeveiliging Overheid
229	Er is een vastgesteld auditplan waarin jaarlijks keuzes worden gemaakt voor welke systemen welk soort beveiligingsaudits worden uitgevoerd.	Audit en Assurance Baseline Informatiebeveiliging Overheid
230	In de P&C-cyclus wordt gerapporteerd over informatiebeveiliging, resulterend in een jaarlijks af te geven In Control Verklaring (ICV) over de informatiebeveiliging. Indien voldoende herkenbaar kan de ICV voor informatiebeveiliging onderdeel zijn van de reguliere, generieke verantwoording.	Baseline Informatiebeveiliging Overheid Governance

ID	Tekstfragment	Code
231	Informatiesystemen worden jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses of penetratietesten.	Baseline Informatiebeveiliging Overheid Threat and Vulnerability Management
232	Beheerafspraken dienen in een Service Level Agreement (SLA) te worden vastgelegd dat onderdeel uitmaakt van de overeenkomst.	Contractmanagement Handreiking Inkoop Clouddiensten Technisch applicatiebeheer
233	CSA Cloud Controls Matrix De Cloud Controls Matrix (CCM) van de Cloud Security Alliance (CSA), is een framework van cloud-specifieke beveiligingsmaat-regelen, gekoppeld aan toonaangevende normen, best practices en voorschriften. CCM biedt organisaties de benodigde structuur, detail en duidelijkheid met betrekking tot informatiebeveiliging gericht op cloudcomputing. CCM wordt momenteel beschouwd als de-facto standaard voor cloud security assurance en compliance.	Handreiking Inkoop Clouddiensten Governance
234	Leverancier zal periodiek aan Opdrachtgever rapport uitbrengen over de nakoming door hem van de overeengekomen Service Levels, waaronder in ieder geval wordt verstaan de Beschikbaarheid van de ICT Prestatie en het niveau van de diensten, waaronder het Onderhoud van de ICT Prestatie alsmede het geplande Innovatief Onderhoud. De inhoud en frequentie van deze rapportage is nader omschreven in de SLA.	Audit en Assurance Contractmanagement Gemeentelijke Inkoop bij IT
235	Opdrachtgever is gerechtigd de naleving door Leverancier van de wezenlijke verplichtingen uit hoofde van de Overeenkomst, de GIBIT 2020 en de daarmee samenhangende overeenkomsten (SLA, verwerkersovereenkomst, etc.), alsmede de juistheid van toegezonden facturen, binnen een redelijke termijn door een onafhankelijke ter zake deskundige aan geheimhouding gebonden derde te laten controleren.	Audit en Assurance Gemeentelijke Inkoop bij IT
236	Op eerste verzoek van Opdrachtgever zullen Partijen een exit-plan opstellen	Business Continuity Management Gemeentelijke Inkoop bij IT
237	Gelet op de grote afhankelijkheid van Leverancier alsmede het continuïteitsrisico bij incidenten en calamiteiten (zoals faillissement) die er bij Hosting bestaat, verklaart Leverancier zich reeds nu voor alsdan bereid aanvullende afspraken met Opdrachtgever te maken teneinde voornoemde risico's te verkleinen.	Business Continuity Management Gemeentelijke Inkoop bij IT

ID	Tekstfragment	Code
238	In november 2020 is door de VNG een bijgewerkte versie van de Gemeentelijke Inkoopvoorwaarden bij IT(GIBIT) vastgesteld. De GIBIT is een set uniforme en gestandaardiseerde inkoopvoorwaarden die gemeenten en gemeentelijke samenwerkingsverbanden kunnen gebruiken bij de verwerving van ICT-producten of -diensten. Een nadere specificatie van het toepassensgebied van de GIBIT is beschreven in de toelichting bij de voorwaarden. De GIBIT is tevens geadopteerd door andere decentrale overheden zoals GGD'en, GHOR-bureaus en Veiligheidsregio's. Op deze organisaties zijn andere sectorale referentie architecturen van toepassing met eigen specifieke normen en standaarden voor ICT-producten en diensten. Om die reden zijn bij die organisaties niet de Gemeentelijke ICT- kwaliteitsnormen van toepassing, maar de ICT-kwaliteitsnormen behorend bij de betreffende sector.	Referentie architectuur Veiligheidsregio ICT-kwaliteitsnormen
239	Voor de ICT Prestatie geldt de Veiligheidsregio Referentie Architectuur (VeRA) als kader. Deze sectorale referentie architectuur beschrijft de inrichting van de gewenste informatiehuishouding van Veiligheidsregio's en de aansluiting daarvan op de omgeving. De informatiehuishouding bestaat onder meer uit referentiecomponenten en applicatie- functionaliteit waarmee de gegevens kunnen worden opgeslagen, geraadpleegd en processen kunnen worden ondersteund.	Referentie architectuur Veiligheidsregio ICT-kwaliteitsnormen
240	Nr. Standaard/norm Bronnen/referenties A1 De ICT Prestatie dient op de VeRA referentiecomponenten geplot te worden. Voor die referentiecomponenten die geraakt worden dient de ICT Prestatie tenminste de bij de referentie-component(en) gespecificeerde functionaliteit te bieden. VeRA referentiecomponenten: veraonline.nl/index.php/ Overzicht_referentiecomponenten A2 Voor de ICT Prestatie is de VeRA kader stellend. De ICT Prestatie voldoet aan de visie en principes uit de VeRA.	Referentie architectuur Veiligheidsregio ICT-kwaliteitsnormen
241	Veiligheidsregio's maken gebruik van systemen van meerdere leveranciers. Ze willen voor een efficiënte uitvoering en dienstverlening informatie delen en werken in ketens samen met andere (overheids-)partijen. Gevolg is dat Veiligheidsregio's in staat moeten zijn om gegevens tussen verschillende systemen uit te kunnen wisselen. Goede, veilige en betrouwbare koppelingen zijn hiervoor noodzakelijk.	Application and interface security Interoperability en Portability Veiligheidsregio ICT-kwaliteitsnormen
242	Binnen de organisatie is het uitgangspunt dat applicatiebeheer een taak van de leverancier van de applicatie is, omdat dit over het algemeen applicatie-specifieke technische kennis vereist.	ICT-Richtlijnen en voorwaarden organisatie Technisch applicatiebeheer

ID	Tekstfragment	Code
243	Het systeem is modulair van opzet: componenten zijn afzonderlijk van elkaar te gebruiken.	ICT-Richtlijnen en voorwaarden organisatie Referentie architectuur
244	Het systeem wordt gehost op een locatie die valt onder Europese wetgeving	ICT-Richtlijnen en voorwaarden organisatie Privacywetgeving
245	Er worden met regelmaat kwetsbaarheden scans uitgevoerd op de aangeboden omgeving. Indien uit deze test aandachtspunten naar voren komen, zullen er direct maatregelen worden getroffen om deze aandachtspunten op te lossen.	ICT-Richtlijnen en voorwaarden organisatie Supply Chain Management Threat and Vulnerability Management
246	De leverancier heeft geen toegang tot de organisatie-gegevens binnen het systeem, tenzij hiervoor akkoord is gegeven door de organisatie.	ICT-Richtlijnen en voorwaarden organisatie Identity en Access Management
247	Er vindt op alle activiteiten van zowel de organisatie als de leverancier logging plaats. Deze logging kan door de leverancier op ieder gevraagd moment geleverd worden ten behoeve van interne rapportages.	ICT-Richtlijnen en voorwaarden organisatie Logging en Monitoring