# Zorgeloos informatiebeveiliging realiseren in de ziekenhuizen van Nederland

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

# Een verkennend onderzoek naar de auditlast binnen ziekenhuizen in Nederland met een focus op informatiebeveiliging.

mazars

**In opdracht van**

Kennisgroep ICT & Zorg van NOREA

Met begeleiding en ondersteuning van Mazars

**Uitgevoerd door**

Emine Arslan HBO-Bedrijfskunde (Hogeschool Windesheim Zwolle)

Lisa de Haan HBO-Finance & Control (Hogeschool van Amsterdam)

**Periode**

7 februari 2022 tot en met 3 juni 2022

# Voorwoord

De Kennisgroep ICT & Zorg van de Nederlandse Orde van Register EDP Auditors (NOREA) presenteert in dit rapport de resultaten van een verkennend onderzoek naar de auditlast binnen ziekenhuizen in Nederland met de focus op informatiebeveiliging.

Aanleiding voor het doen van onderzoek is de observatie vanuit onze beroepsgroep dat ziekenhuizen zich geplaatst zien voor een toenemend aantal verplichtingen om zich te laten auditen. Deze verplichtingen vloeien voort uit wet- en regelgeving, het ziekenhuis moet aantonen dat het zijn 'licence to operate' waarmaakt. Ze vloeien echter ook voort uit incidenten.

Een goed voorbeeld daarvan is de NVZ Gedragslijn die zijn oorsprong kent in het incident dat zich heeft voorgedaan bij het Hagaziekenhuis. In 2018 hebben een aantal medewerkers van het Hagaziekenhuis zonder toestemming het medisch dossier van bekende realityster Samantha de Jong, ook bekend als Barbie, bekeken.

Hoogleraar Pauline Meurs observeert: "bij elk incident worden er regels en verantwoordingsmechanismen bedacht om herhaling te voorkomen. En hoe meer verantwoording je vraagt, hoe minder vertrouwen je oogst." (Het Financiële Dagblad, 2 juli 2022)

Wij observeren een groeiend spectrum aan accreditaties, certificeringen, keuringen en controles bij ziekenhuizen zowel in aantal, in de breedte, in de diepte maar ook in tijd en geld.

Met dit onderzoek willen we inzicht verkrijgen in:
1. de aard en de omvang van de auditlast waarvoor ziekenhuizen zich geplaatst zien;
2. de vraag voor en door wie de audits worden uitgevoerd en waarom, daarmee kan tevens worden bepaald hoeveel (verschillende) partijen hiermee bezig zijn
3. de vraag of er overlap is tussen audits en zo ja, of het efficiënter kan
4. het geven van aanbevelingen om de auditlast terug te dringen, kosten en tijd te besparen en meer efficiency te behalen.

Een gemiddeld ziekenhuis heeft al snel te maken met 50-60 verschillende audits op diverse terreinen. Dit is te veel om op alle vier bovengenoemde vragen een antwoord te krijgen.

Vanuit NOREA lag het daarom voor de hand om de focus te leggen op de auditlast rond informatiebeveiliging. Het onderzoek is uitgevoerd door twee stagiaires onder begeleiding van een klankbordgroep bestaande uit leden van de Kennisgroep ICT & Zorg.

Beide stagiaires hebben uitstekend werk verricht. De Kennisgroep spreekt graag haar waardering uit voor hun inzet. Onze dank gaat ook uit naar Mazars IT Audit & Advisory, zij hebben de dagelijkse aansturing en begeleiding van deze stagiaires verzorgd.

Aan het onderzoek hebben medewerkers van verschillende ziekenhuizen bijgedragen alsmede een aantal experts, daarvoor onze dank!

De Kennisgroep ICT & Zorg hoopt met dit onderzoek een bijdrage te leveren aan het terugdringen aan de auditlast in de zorg. "Regeldruk en controledrang die zorgverleners nu zo frustreert, moet op de schop". (Pauline Meurs)

Kennisgroep ICT & Zorg NOREA

Klankbordgroep Onderzoek Auditlast Ziekenhuizen

Nico Huizing, Jan Hoogstra, Gert-Jan Gerrits, Michiel Hopstaken

# Samenvatting

Een verkennend onderzoek naar de **auditlast** binnen ziekenhuizen in Nederland met een focus op informatiebeveiliging.

Naar aanleiding van de stijgende auditlast in ziekenhuizen heeft de Kennisgroep ICT & Zorg van NOREA een verkennend onderzoek geïnitieerd naar de auditlast die zich bevindt binnen de informatiebeveiliging van ziekenhuizen. Dit onderzoek wordt uitgevoerd middels twee scriptieonderzoeken die samengebracht zijn in dit rapport. Het eerste onderzoek focust zich op de organisatorische knelpunten die voortkomen uit het auditproces voor de NEN 7510. Het tweede onderzoek focust zich op de overlap tussen andere normenkaders in relatie tot de NEN 7510.

De auditlast binnen de informatiebeveiliging is onderzocht via een vragenlijst voor de Chief Information Security Officers (CISO's (en soortgelijke informatiebeveiliging gerelateerde functies)). Deze vragenlijst is verstuurd naar de gehele populatie van het onderzoek, de 71 ziekenhuizen in Nederland. Via een database zijn 103 personen geselecteerd om deel te nemen aan de vragenlijst. De vragenlijst is ingevuld door 9 personen. Daarnaast zijn er vier verdiepende gesprekken gevoerd met ziekenhuizen en zijn er zes experts gesproken.

Uit het onderzoek komt voort dat de auditlast in de informatiebeveiliging als **hoog** wordt ervaren door ziekenhuizen. Ziekenhuizen hebben moeite met het houden van een gezonde balans tussen het primair verlenen van zorg en het besteden van aandacht aan secundaire zaken als informatiebeveiliging. Daarnaast vindt er een beperkte vertegenwoordiging van informatiebeveiliging plaats in de lijnorganisatie van ziekenhuizen. Dit maakt het lastig om informatiebeveiliging te implementeren in alle lagen van de organisatie. Ook geven ziekenhuizen aan het frustrerend te vinden dat er een verschil zit in de toetsing tussen auditors om zekerheid te kunnen verlenen. Dit levert de ziekenhuizen extra werk op. Daarbovenop leidt dit ook tot frictie tussen de auditor en het ziekenhuis. Er ontbreekt wederzijdse begrip. Dit gaat gepaard met de aanwezigheid van een bepaalde (werk)cultuur binnen ziekenhuizen, waarbij (medisch) personeel een zekere mate van terughoudendheid toont. Daarbovenop blijkt de NEN 7510 overlap te hebben met de normenkaders: Horizontaal Toezicht, E-health, NVZ-gedragslijn, VIPP-audits, DigiD audits, ISO 27001 en de Jaarrekening controle. Al deze constateringen dragen bij aan de lage mate van bewustzijn die aanwezig is in ziekenhuizen omtrent informatiebeveiliging.

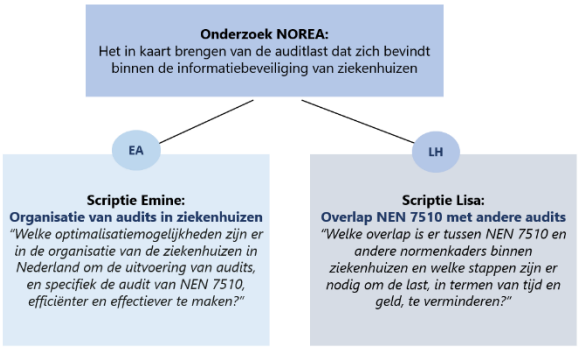
Deze constateringen leiden tot de volgende aanbevelingen:

- Meer vertegenwoordiging van informatiebeveiliging in de lijnorganisatie van een ziekenhuis;
- Informatiebeveiliging behandelen als continu proces in plaats van losstaand onderdeel;
- Duidelijke communicatie en meer interactie tussen auditor en ziekenhuis;
- Verantwoordingstool van personeel afstemmen op de gebruiker;
- Samenwerking opzoeken met andere ziekenhuizen;
- Verhogen van het bewustzijn en de bewustwording van personeel in het ziekenhuis omtrent informatiebeveiliging;
- Een voorbeeld nemen van het KIK-V model om te implementeren;
- Opzetten van een integraal control framework.

# Inhoudsopgave

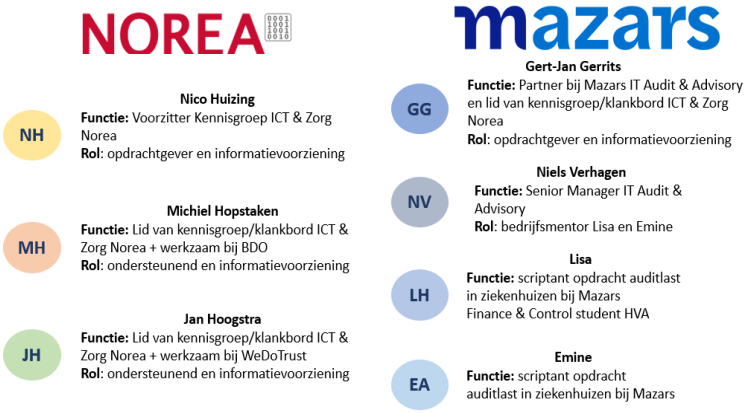
# Introductie en opbouw rapport

Dit onderzoek is uitgevoerd door twee studenten (hierna te noemen: auteurs) waarbij uiteindelijk twee scripties zijn opgeleverd. Deze scripties zijn vervolgens via dit rapport samengevoegd tot één rapport voor de opdrachtgever. De scheiding tussen de scripties wordt hiernaast weergegeven.




Figuur 1 scheiding scripties

Door de kennisgroep ICT & Zorg is het initiatief genomen om onderzoek te doen naar de auditlast[1] in ziekenhuizen binnen Nederland. Vanuit de kennisgroep een klankbordgroep gevormd waarmee wekelijks is vergaderd. Tijdens deze vergaderingen hebben de leden uit de klankbordgroep een ondersteunende rol gehad voor de auteurs van dit rapport. De auteurs van dit rapport zijn primair begeleid vanuit Mazars[2]. De samenstelling van de klankbordgroep wordt hiernaast weergegeven.




Figuur 2 samenstelling klankbordgroep

# Leeswijzer

Dit rapport bestaat allereerst uit een gedeelte Aanleiding. In dit hoofdstuk wordt achtergrondinformatie weergegeven over de aanleiding van dit onderzoek. Vervolgens komt het hoofdstuk Onderzoeksopzet aan bod. In dit hoofdstuk wordt er aandacht besteedt aan de manier waarop het onderzoek is verricht en wordt de verantwoording van de opgedane data weergegeven. Daaropvolgend worden de ondervonden knelpunten en aanbevelingen allereerst weergegeven in figuur 3. In deze figuur is te zien met welke data de knelpunten en aanbevelingen tot stand zijn gekomen. Aansluitend, worden de knelpunten en aanbevelingen toegelicht in het hoofdstuk Conclusies en aanbevelingen.

[1] Onder auditlast wordt verstaan: Een last in termen van tijd en geld die ziekenhuizen intern maar ook extern besteden aan het uitvoeren van audits. Audits is alles wat te maken heeft met certificeringen, accreditaties en keuringen, die wettelijk of via andere regelgeving wordt opgelegd binnen zo'n ziekenhuis.

[2] Het publiekrechtelijk karakter van NOREA is niet geschikt om stagiaires onder te brengen en te faciliteren. Mazars is bereid gevonden de auteurs een stagecontract te bieden en primair te begeleiden.

# 1. Aanleiding

Ziekenhuizen hebben steeds meer te maken met certificeringen, accreditaties en keuringen, die wettelijk of via andere regelgeving wordt opgelegd (verzamelnaam: audits). Hier besteden ziekenhuizen intern, maar ook extern veel tijd en geld aan. Aan de hand van een interview [3]met Nico Huizing (lid klankbordgroep) is gebleken dat de afgelopen jaren deze regelingen zijn toegenomen in aantal en in omvang. Dit resulteert in een hogere belasting (in tijd én geld) én complexiteit binnen de ziekenhuizen om aan deze eisen te kunnen voldoen. NOREA heeft dit ook bevestigd gekregen naar aanleiding van gesprekken die hebben plaatsgevonden met professionals binnen een aantal ziekenhuizen. Uit deze gesprekken bleek dat het personeel de audits als zeer belastend ervaart. Er wordt vermoed dat er bepaalde dubbeltellingen aanwezig zijn, waardoor bepaalde auditactiviteiten meerdere keren worden uitgevoerd. Er worden veel verschillende audits uitgevoerd door en voor diverse partijen. Het regelproces rondom het uitvoeren van audits lijkt in ziekenhuizen niet goed geregeld te zijn.

Ook komt het voor dat nieuwe audits voortvloeien uit incidenten bij één ziekenhuis en vervolgens gevolgen hebben voor alle ziekenhuizen. Een goed voorbeeld daarvan is de NVZ Gedragslijn die zijn oorsprong kent in het incident dat zich heeft voorgedaan bij het Hagaziekenhuis. In 2018 hebben een aantal medewerkers van het Hagaziekenhuis zonder toestemming het medisch dossier van bekende realityster Samantha de Jong, ook bekend als Barbie, bekeken. De Autoriteit Persoonsgegevens (AP) heeft hier een flinke boete voor uitgedeeld. Na overleg met de AP heeft de NVZ het initiatief genomen een NVZ Gedragslijn in het leven te roepen aan de hand waarvan de ziekenhuizen zouden moeten kunnen aantonen voldoende 'in control' te zijn, zodat een incident als in het Hagaziekenhuis zich niet (meer) zou kunnen voordoen.

Niet alleen incidenten zorgen voor meer audits maar ook de audits zelf worden zwaarder, blijkt uit gesprekken met bestuurders van zorginstellingen. Dit alles bij elkaar is aanleiding geweest voor dit onderzoek.

Het vermoeden is dat dit probleem zich naast ziekenhuizen ook voordoet bij andere zorgaanbieders. Hierbij kan gedacht worden aan de GGZ-instellingen, verplegings- en verzorgingshuizen en revalidatiecentra. In verband met de grootte van het onderzoek zal dit rapport zich beperken tot de auditlast die wordt ervaren in Nederlandse ziekenhuizen.

Kortom, de auditlast in ziekenhuizen neemt dus alsmaar toe en ook de toegevoegde waarde van de audits wordt in twijfel getrokken. De opdrachtgever wil via dit onderzoek verkennend onderzoek voeren naar de auditlast die zich bevindt binnen de ziekenhuizen in Nederland. Het is onmogelijk gebleken het onderzoek te richten op alle audits die ziekenhuizen dienen uit te (laten) voeren. Vanuit de specifieke rol van NOREA is gekozen het onderzoek in eerste instantie te richten op informatiebeveiliging.

Ook als gevolg van het toenemende belang en relevantie van informatiebeveiliging in ziekenhuizen, focust dit onderzoek zich op de organisatie van audits omtrent informatiebeveiliging in ziekenhuizen en de overlap tussen normenkaders binnen de informatiebeveiliging in ziekenhuizen.

[3] Dit gesprek heeft plaatsgevonden als "aftrap" voor dit onderzoek. Tijdens dit gesprek is de opdracht nader vormgegeven.

# 2. Onderzoeksopzet

Aan het begin van het afstudeertraject is er samen met de opdrachtgever afgestemd op welke wijze het onderzoeksproces zou plaatsvinden. Dit zou gebeuren op basis van actieve deelname van vier pilot ziekenhuizen die door de opdrachtgever hierop waren voorbereid. De oorspronkelijke opzet was om in gesprek te gaan op basis van deskresearch naar relevante informatie omtrent audits per ziekenhuis. De ziekenhuizen zouden vooraf geïnformeerd worden over het ontstane beeld en de geformuleerde vragen. De gesprekken dienden de basis te zijn voor het opstellen van een breed uit te zetten enquête.

Echter, is het onderzoeksproces niet verlopen zoals hierboven is beschreven. In de elfde kalenderweek van 2022 is er een inventariserend gesprek gevoerd met één van de pilot-ziekenhuizen. De overige drie pilot-ziekenhuizen stelden het gesprek voortdurend uit, lieten niet meer van zich horen of trokken zich terug uit het onderzoek met de reden dat het te veel moeite zou kosten. Er is besloten om de vragenlijst op te stellen op basis van het eerste gesprek met een ziekenhuis en input vanuit de opdrachtgever. De responses uit deze vragenlijst zijn geanalyseerd op kruisverbanden en terugkerende sleutelvariabelen. Daarnaast zijn er ook interviews gehouden met drie andere niet-pilot ziekenhuizen. Deze gesprekken hebben bijgedragen aan het opdoen van informatie voor dit onderzoek vanuit het perspectief van een ziekenhuis. Verder zijn er ook zes experts gesproken die allen werkzaam zijn op het gebied van informatiebeveiliging rondom ziekenhuizen. De interviews zijn uitgewerkt tot transcripten, deze zijn vervolgens gelabeld en samengevat in codetabellen.

### 2.1 De vragenlijst

De vragenlijst is opgesteld aan de hand van de hoofddoelstelling: een beeld vormen over de auditlast in ziekenhuizen.

De opbouw van de vragenlijst wordt hieronder schematisch weergegeven.

| Onderwerp | Korte toelichting | Soorten vragen | Vragen |
|---|---|---|---|
| Organisatie | Soort ziekenhuis, aanwezigheid CISO | Gesloten | 1 t/m 2 |
| Informatiebeveiliging in het ziekenhuis | Inzicht krijgen in de manier waarop informatiebeveiliging is georganiseerd | Gesloten, open vragen voor toelichting en vraag met een schaal | 3 t/m 16 |
| NEN 7510 | Status van de NEN 7510 | Gesloten | 17 |
| Organisatie van audits in ziekenhuizen | Inzicht krijgen in de organisatie van audits omtrent informatiebeveiliging | Gesloten en open vragen voor toelichting | 18 t/m 25 |
| Algemene indruk auditlast | Inzicht krijgen in de ontwikkeling van de auditlast over de afgelopen jaren heen | Gesloten en open vraag voor toelichting | 26 en 27 |

Tabel 1 opbouw vragenlijst

Vervolgens is er afgestemd met de opdrachtgever op welke manier de vragenlijst uitgestuurd zou worden naar de respondenten. De voornaamste doelgroep van de vragenlijst zijn de CISO's binnen

ziekenhuizen. Hetzelfde geldt voor de functies die goed zicht hebben op de informatiebeveiliging in ziekenhuizen. Helaas, bestaat er geen lijst met alle CISO's of soortgelijke functies in Nederland bij ziekenhuizen. De vragenlijst is uitgezonden via LinkedIn.

Via de HR-afdeling van Mazars is er een targetlijst opgesteld met daarbij relevante personen die geselecteerd zijn op basis van een aantal zoekfilters. Aan de hand van deze targetlijst is er een selectie gemaakt met personen die benaderd kunnen worden via de Inmail functie van LinkedIn.

De HR-afdeling heeft een search uitgevoerd op LinkedIn met de volgende zoekfilters: CISO, Information Security, Functionaris Gegevensbescherming, ICT, Gezondheidssector en informatiebeveiliging. Deze search heeft uiteindelijk meer dan 250 resultaten opgeleverd. Deze resultaten zijn vervolgens één voor één verwerkt in een Excel-overzicht. Vervolgens is er een legenda opgesteld om een verdeling te kunnen maken over de personen die benaderd zullen worden.

De gemaakte legenda wordt hieronder schematisch weergegeven.

| Categorie | |
|---|---|
| Rood | Geen doelgroep |
| Groen | Wel relevante functie/ wel relevant ziekenhuis |
| Oranje | Geen relevante functie/ wel relevant ziekenhuis |
| Blauw | Wel relevante functie/ geen relevant ziekenhuis |
| Paars | Geen relevante functie/ geen relevant ziekenhuis |

Tabel 2 Legenda proces definiëren populatie

In dit Excel-overzicht is ook een lijst gemaakt met het aantal ziekenhuizen in Nederland. In totaal zijn er 71 ziekenhuizen aanwezig in Nederland (Wikipedia-bijdragers, 2022). Deze groep ziekenhuizen vormen de populatie van dit onderzoek. Tijdens het definiëren van de populatie is het dan ook een randvoorwaarde geweest om alle ziekenhuizen de mogelijkheid te bieden om deel te nemen aan de vragenlijst.

Het selecteren van de juiste personen is op de volgende wijze gebeurd. In eerste instantie zijn de 250+ personen gemarkeerd met een rode of groene kleur. De rode personen konden vervolgens buiten beschouwing gelaten worden, omdat de organisatie niet tot een ziekenhuis behoorde. De groene personen zijn vervolgens verdeeld onder de 71 ziekenhuizen. De ziekenhuizen die geen groene persoon hadden, hebben een oranje persoon toegekend gekregen totdat de limiet van 100 personen is bereikt. Dit komt door de limiet van het aantal Inmails (50 per persoon) dat verstuurd kan worden via LinkedIn. De overige personen zijn vervolgens weer onderverdeeld in de kleuren: blauw en paars. Deze kleuren geven "geen relevant ziekenhuis" aan, omdat de limiet van 100 personen is bereikt en door de toegepaste selectiemethode alle ziekenhuizen zijn vertegenwoordigd door minimaal één persoon. Dit betekent dat er tijdens het markeren van de personen rekening is gehouden met het gegeven dat er ten minste naar één persoon van elk ziekenhuis een Inmail met de vragenlijst is verstuurd. Daarnaast is de vragenlijst anoniem ingevuld. Met het doel om het toegankelijker te maken voor personen om de vragenlijst in te vullen i.v.m. de gevoelige informatie die gegeven kan worden.

Op deze manier zijn er 103[4] groene en oranje personen geselecteerd die de mogelijkheid hebben gekregen om deel te nemen aan het invullen van de vragenlijst. Bij het bericht naar de oranje personen is er het verzoek gedaan om de vragenlijst naar de juiste persoon binnen het ziekenhuis te sturen indien zij deze niet konden invullen[5].

| Aantal groene personen | Aantal oranje personen | Totale personen |
|---|---|---|
| 87 | 16 | 103 |

Tabel 3 verdeling geselecteerde personen

Zie bijlage C voor een totaaloverzicht van het aantal ziekenhuizen met daarbij de aantal benaderde personen per ziekenhuis in verhouding tot de populatie.

Tussentijds is er een reminder gestuurd naar de respondenten met het verzoek om de vragenlijst alsnog in te vullen. De vragenlijst heeft uiteindelijk 9[6] responses opgeleverd van de 103 personen die geselecteerd waren. Dit levert een responspercentage van 8,7% op. Er is onderling met de opdrachtgever gekeken naar de datakwaliteit van de responses. Tijdens deze sessies is door de opdrachtgever geconcludeerd dat de verzamelde data in orde is. Tijdens het sturen van de reminderberichten is er ook gevraagd naar de reden waarom er gekozen wordt om niet deel te nemen aan het onderzoek. Hier is door zeven personen de volgende antwoorden op gegeven:

| | | | | |
|---|---|---|---|---|
| Geen interesse 3x | Burn-out 1x | Functie elders 1x | Geen tijd 1x | Gevoelige info 1x |

### 2.2 Verdiepende gesprekken met ziekenhuizen

In verband met de “lage” respons is er aanvullend data opgehaald om de antwoorden uit de vragenlijst te valideren. Hiertoe zijn een aantal aanvullende en verdiepende gesprekken gevoerd.

In totaal is er met vier ziekenhuizen gesproken. Hieronder wordt de functie van de personen die gesproken zijn weergegeven.

| Kalenderweek | Functie persoon |
|---|---|
| 9 | Klinisch projectmanager |
| 11 | Interne auditor |
| 14 | Klinisch chemicus |
| 18 | CISO en Kwaliteitsfunctionaris servicecentrum Informatie- en Medische Technologie |

Tabel 4 overzicht gesprekken ziekenhuizen

[4] In verband met het feit dat 3 respondenten op een andere manier zijn benaderd dan via LinkedIn (wegens: 1 x benaderd via al beschikbare e-mail, 2 x indirect bericht via andere LinkedIn lid omdat bericht ontvangen uitstond voor deze persoon) is er de mogelijkheid ontstaan om nog 3 oranje personen te benaderen via LinkedIn.

[5] Zie bijlage B voor het verstuurde bericht aan de groene en oranje respondenten.

[6] Uiteindelijk zijn er tien responses ontvangen. Echter, heeft één respons alleen de eerste vraag beantwoord.

### 2.3 Expertinterviews

In totaal is er met zes verschillende personen gesproken. Hieronder wordt de functie van de personen die gesproken zijn weergegeven.

| Kalenderweek | (Voornaamste) Functie persoon |
|---|---|
| 16 | IT-auditor |
| 16 | IT-auditor |
| 16 | IT-auditor |
| 16 | IT-auditor |
| 18 | Privacy- en security adviseur |
| 16 | Docent en IT-auditor |

Tabel 5 overzicht gesprekken experts

Middels deze gesprekken is het perspectief van de externe auditor van een ziekenhuis naar voren gekomen en geven de constateringen en aanbevelingen hierdoor een realistisch beeld van de werkelijkheid weer.

### 2.4 Afweging van de onderzoeksresultaten

Allereerst speelt de lage respons vanuit de vragenlijst een belangrijke rol in de representativiteit van de onderzoeksresultaten. Dit betekent dan ook dat de onderzoeksresultaten niet representatief zijn voor de gehele populatie. Hierdoor is bewust gekozen om de knelpunten “constateringen” te noemen. Daarnaast is de vragenlijst ook anoniem ingevuld, waardoor niet achterhaald kan worden welke ziekenhuizen er hebben gereageerd. Het kan namelijk voorkomen dat meerdere personen per ziekenhuis gereageerd hebben op de vragenlijst. Er is namelijk de afweging gemaakt om meerdere personen per ziekenhuis, zowel personen met een relevante als een niet relevante functie, te benaderen zodat er respons geleverd zou worden op de vragenlijst. Dit wordt ook aangeduid in bijlage A. Dit kan een scheve verhouding geven in de mate waarop de populatie vertegenwoordigd is in het onderzoek.

Daarnaast sluiten de functies van de personen die gesproken zijn tijdens de gesprekken met ziekenhuizen niet aan op de doelgroep van het onderzoek. Zij dragen wel bij aan het creëren van een breder kijkveld omtrent auditlast in ziekenhuizen.

Om het probleem vanuit verschillende invalshoeken te kunnen beschouwen is gebruik gemaakt van triangulatie. Ook zijn de gevoerde gesprekken zover dat mogelijk is geweest op dezelfde manier aangepakt. Dit verhoogt de interne validiteit van de onderzoeksresultaten. Er is een bepaalde systematiek in de analyse van de resultaten aangebracht. Bij de kwalitatieve data is dit het coderen van transcripten geweest. De data uit de vragenlijst is geanalyseerd op kruisverbanden en sleutelwoorden die terugkerend voorkomen in de antwoorden. De kruisverbanden worden met dezelfde kleur aangeduid en de sleutelwoorden zijn onderstreept en dikgedrukt weergegeven.

De resultaten uit de vragenlijst zijn vervolgens gevalideerd tijdens een gesprek met een ziekenhuis. Vanuit de functieachtergrond van de gesprekspartners konden zij een goed oordeel geven over de juistheid van de constateringen.

Verder is er ook nauw contact onderhouden met de opdrachtgever en de klankbordgroep om tussentijdse de opgehaalde data te bespreken op inhoudelijke kwaliteit. Op deze manier zijn de eisen vanuit de opdrachtgever, de doelstelling van het onderzoek en de inhoudelijke kwaliteit van de data voortdurend aan bod gekomen.

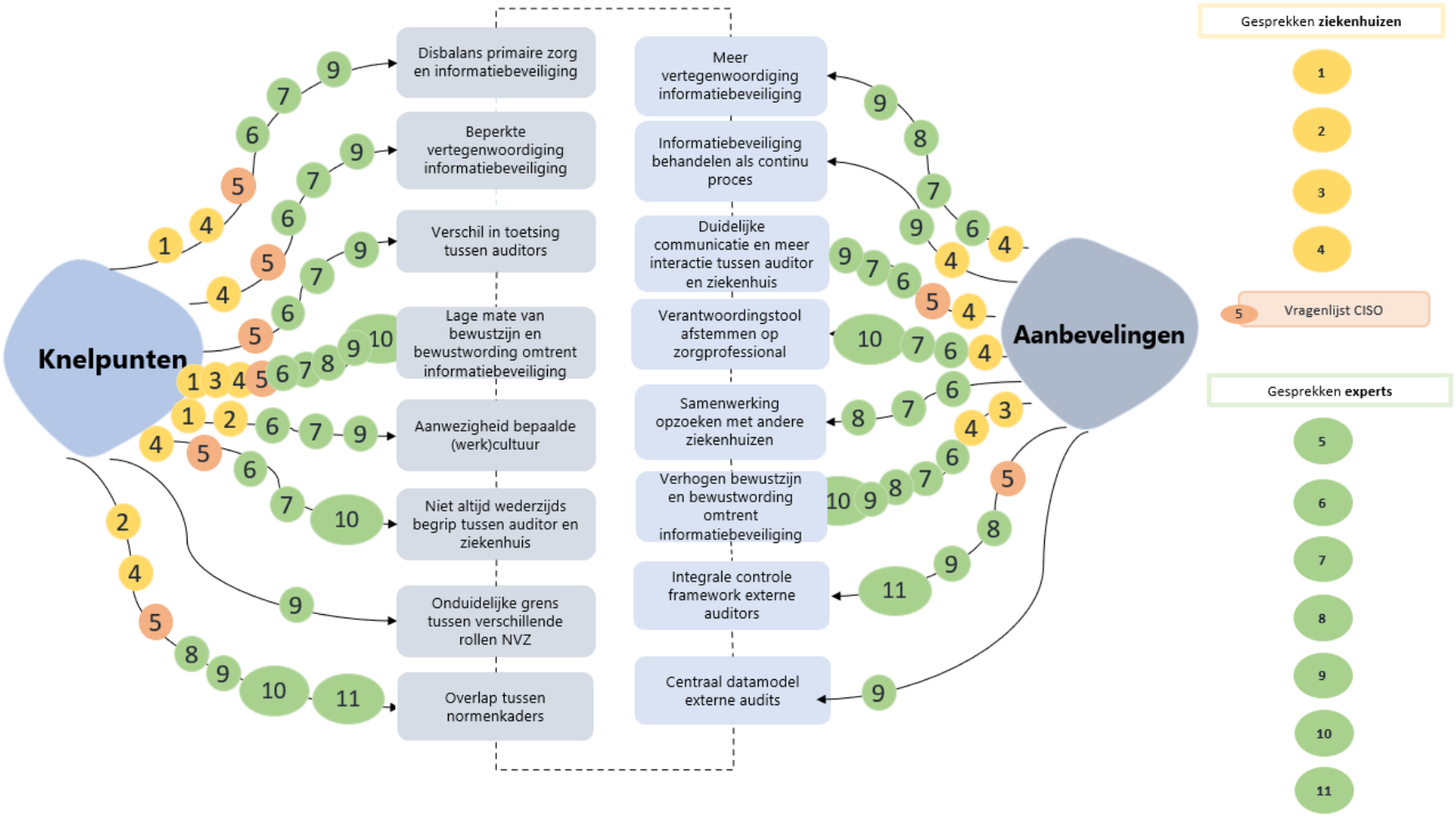
### 2.4.1 Betrouwbaarheid

De betrouwbaarheid van dit onderzoek is verhoogd door middel van het gebruikmaken van methodetriangulatie. Er is op verschillende manieren data verzamelt om te kijken of de verkregen resultaten in overeenstemming zijn met elkaar. Echter, zal het onderzoek niet tot dezelfde resultaten leiden bij herhaling van de vragenlijst i.v.m. het menselijk aspect dat hierbij meespeelt. De stemming, tijdstip en andere zaken hebben een grote invloed op de antwoorden die worden gegeven. Omdat dit onderzoek in samenwerkingsverband is uitgevoerd en er een vorm van het vier-ogenprincipe is toegepast.

### 2.4.2 Validiteit

Met de anonimiteit van de vragenlijst is proberen te voorkomen dat respondenten sociaal wenselijk antwoorden. Toch zal dit wel in een bepaalde mate gespeeld hebben. De lage respons uit de vragenlijst heeft effect op de externe validiteit. Het geeft geen goede afspiegeling van de populatie weer en maakt de resultaten beperkt generaliseerbaar. De validiteit is geprobeerd te versterken middels de gesprekken met ziekenhuizen en experts.

In onderstaand figuur worden de geconstateerde knelpunten en aanbevelingen in samenhang met de opgedane date weergegeven. Elk knelpunt en aanbeveling komen, zoals in het schema te zien is, voort uit data afkomstig uit gesprekken en een vragenlijst (zie rechterkolom 1 tot en met 11). Naast deze data hebben de input van de opdrachtgever en de eigen inbreng van de auteurs er vervolgens voor gezorgd dat een knelpunt en aanbeveling verder is uitgewerkt.




Figuur 3 de knelpunten en aanbevelingen in samenhang met elkaar

# 3. Constateringen

Uit de verzamelde data (zie figuur 3) is gebleken dat het auditproces voor de NEN 7510 op het moment van het uitvoeren van het onderzoek niet effectief en efficiënt is. Dit vloeit voort uit de onderstaande constateringen.

### 3.1 Moeite met balans tussen primair zorg verlenen en aandacht besteden aan informatiebeveiliging

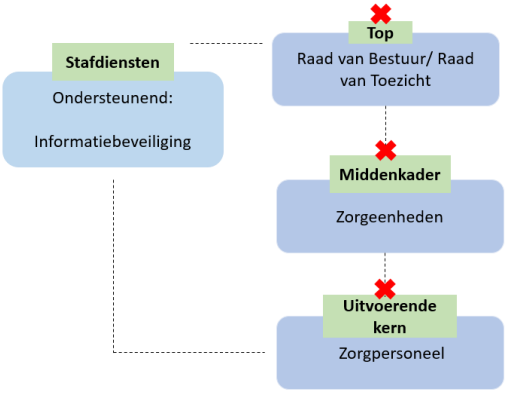
Ziekenhuizen vinden het lastig om de balans te houden tussen het primair leveren van zorg en het geven van prioriteit aan secundaire zaken zoals informatiebeveiliging.

Doordat ziekenhuizen dus primair gefocust zijn op het leveren van zorg en daarbij geen winst(oogmerk) hebben, is het lastig om tijd en middelen te besteden aan audits. Vooral het uitvoerig en gedetailleerd bezig gaan met audits vormt een uitdaging voor ziekenhuizen.

### 3.2 Beperkte vertegenwoordiging van informatiebeveiliging binnen ziekenhuizen

De CISO (en soortgelijke functies) worden geplaatst in de stafdiensten van een ziekenhuis. Hierdoor ontstaat er een beperkt kijkveld op wat er speelt binnen het ziekenhuis. Daarnaast wordt de rol van een CISO vaak gecombineerd met een andere soortgelijke rol. Dit resulteert in minder prioriteitsverlening aan de kerntaken van een CISO.

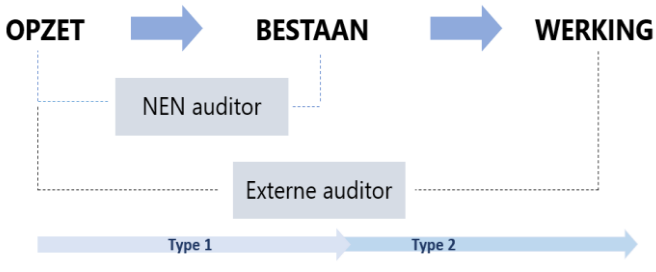
Uit de vragenlijst komt onder andere naar voren dat bij een centrale regie van het auditproces er slecht zicht is op de gemaakte kosten (in termen van tijd en geld) m.b.t. de auditwerkzaamheden. Terwijl ziekenhuizen met een centrale en decentrale regie aangeven goed zicht te hebben op de gemaakte kosten.




Figuur 4 visuele weergave positie informatiebeveiliging in ziekenhuis

### 3.3 Verschil in toetsing tussen auditors om zekerheid te kunnen verlenen

De NEN 7510 is een type 1 audit. Er wordt één keer vastgesteld of het ziekenhuis voldoet aan de gestelde eisen. Als het ziekenhuis voldoet aan de eisen wordt er een certificaat verleent die geldig is voor drie jaar. Een externe auditor wil niet steunen op de NEN 7510 en stelt daarom aanvullende eisen aan het ziekenhuis. Bij de toetsing van de NEN 7510 wordt de effectieve werking niet getoetst. De externe auditor wil alleen zekerheid verlenen als de effectieve werking van de NEN 7510 ook getoetst wordt. Het NEN 7510 certificaat is dus drie jaar geldig terwijl de externe auditor eigenlijk niet wil/kan steunen op een certificaat dat drie jaar geldig is. De auditor wil/kan dat niet, omdat er ten eerste geen tussentijdse meetmomenten plaatsvinden als het certificaat al is verleend. Ten tweede wil de externe auditor dat niet, omdat de effectieve werking van de NEN 7510 niet wordt getoetst (zie figuur 5). Ten derde ziet het NEN 7510 certificaat uitsluitend toe op de opzet en/of werking van het Information Security Management System (ISMS). Dat is slechts een deel van het complex aan procedures en maatregelen die in het kader van




Figuur 5 type audit met toetsingskader auditor

informatiebeveiliging een rol spelen. Bij gebruikers is lang niet altijd deze beperkte scope van een NEN 7510 certificaat duidelijk.

### 3.4 Lage mate van bewustzijn en bewustwording omtrent informatiebeveiliging

Uit de vragenlijst en expertinterviews komt bij het merendeel naar voren dat ziekenhuizen vanuit compliance gedachten gemotiveerd zijn om te voldoen aan een juiste informatiebeveiliging. Bij het vragen naar de achterliggende beweegreden om bezig te gaan met informatiebeveiliging is de sleutelvariabele "het moeten voldoen aan wettelijke kaders" teruggekomen. Meerdere ziekenhuizen geven aan dat zij informatiebeveiliging gerelateerde taken uitvoeren, omdat het moet op basis van de wet- en regelgeving. Hieruit kan geconstateerd worden dat de motivatie van ziekenhuizen grotendeels gefocust is op de toezichthouder en niet primair op het willen beschermen van de patiënt.

Het gemiddelde cijfer dat gegeven wordt door de respondenten aan de mate van prioriteitstelling omtrent informatiebeveiliging binnen het ziekenhuis is een 7.9. Dit zou betekenen dat de mate van bewustzijn goed in orde moet zijn binnen ziekenhuizen. Daarentegen komt uit gesprekken met ziekenhuizen en de gesprekken met experts weer naar voren dat de mate van bewustzijn nog te laag is. Dit verschil kan verklaard worden met het gegeven dat de vragenlijst is ingevuld door respondenten met een informatiebeveiliging gerelateerde functie. De mate van bewustzijn en bewustwording komt bij deze groep personen voort uit de uit te voeren taken. De expertsinterviews met externe onafhankelijke IT-auditors geven daarentegen perspectief van een buitenstaander weer die zicht heeft op alle lagen van het ziekenhuis.

### 3.5 Aanwezigheid bepaalde (werk)cultuur

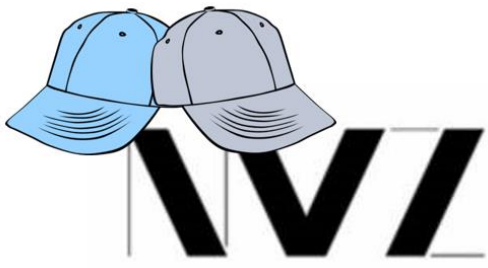
Uit expertinterviews en verdiepende gesprekken met ziekenhuizen komt voort dat (medisch) personeel een bepaalde manier van werken heeft ontwikkeld waarbij er beperkte flexibiliteit aanwezig is om dingen anders aan te pakken. Er is een bepaalde mate van terughoudendheid aanwezig. Dit resulteert in een (werk)cultuur waarbij het lastig is om bepaalde (gedrags-)veranderingen aan te brengen.

### 3.6 Niet altijd wederzijdse begrip tussen auditor en ziekenhuis

Dat een externe auditor niet wil steunen op de NEN 7510 levert de ziekenhuizen veel frustratie op. Er wordt vaak niet ingezien waarom een externe auditor aanvullende eisen stelt. Er ontbreekt wederzijds begrip.

### 3.7 Onduidelijke grens tussen verschillende rollen NVZ

De NVZ is de belangenvereniging van Nederlandse ziekenhuizen.[7] De NVZ wordt bestuurd door bestuursleden. Deze bestuursleden bevinden zich ook in de Raad van Bestuur van een bepaald ziekenhuis. Dit betekent dat een bestuurslid een dubbele rol heeft. Enerzijds is deze persoon bestuurslid bij de NVZ, die collectief de belangen van alle aangesloten ziekenhuizen behartigt. Anderzijds bevindt deze persoon zich in de eigen Raad van Bestuur van een ziekenhuis. In de praktijk kan dit tot fricties leiden. Waarbij er in eerste instantie in collectieve zin ingestemd wordt met iets, levert dat verhindering op zodra het terecht komt op het "eigen bordje". De NVZ Gedragslijn is een voorbeeld dat




Figuur 6 foto om dubbele rol van NVZ aan te tonen

[7] De academische ziekenhuizen zitten aangesloten bij de Nederlandse Federatie van Universitair Medisch Centra (NFU).

veel genoemd werd in interviews en komt ook in de vragenlijst meerdere keren terug.

Daarbij houdt de NVZ ook toezicht op de naleving van deze gedragslijn. De NVZ vervult de rol van een belangenorganisatie, maar is daarbij ook een toezichthouder. Wat in sommige aspecten tegenstrijdig kan zijn.

### 3.8 Overlap tussen normenkaders

De NEN 7510 kent overlappen met een aantal normenkaders. Dit zijn de volgende normenkaders:

- Horizontaal Toezicht
- E-health
- NVZ-gedragslijn
- VIPP-audits
- DigiD audits
- ISO 27001
- Audit van de jaarrekening

De normenkaders overlappen niet allen op dezelfde punten, maar veel van de overlappen gaan over dezelfde onderwerpen: Logging, monitoring, authenticatie, autorisatie en bewustwording.

#### 3.8.1 Tijdsbesteding en kosten

In de vragenlijst werd er een vraag gesteld over het inzicht in de lasten (in tijd en geld) van auditwerkzaamheden op het gebied van informatiebeveiliging. In de tabel hieronder worden de resultaten weergegeven.

| Respondenten | Tijdsbesteding per jaar | Kosten per jaar |
|---|---|---|
| Respondent 1 | 100 uur, wellicht meer. | Onbekend |
| Respondent 2 | 6.600 uur voor verschillende afdelingen. (40*5) + (40*10) + (40*150, dit is 5% van 3000) | 2,25 miljoen euro (750.000 + 1.500.000) |
| Respondent 3 | Onbekend | Onbekend |
| Respondent 4 | 60 uur, aan interne audits (40*1,5) | Certificering kost 45.000 euro in het eerste jaar, oplopende kosten van een consultant van 1.200 euro per dag. |
| Respondent 5 | 120 uur aan interne audits (8*15) | Onbekend |
| Respondent 6 | 180 uur aan interne audits incl. Horizontaal Toezicht. (40*4,5) | 5.000 á 6.000 euro. |
| Respondent 7 | Beperkt, onbekend | Onbekend |
| Respondent 8 | Zichtbare toename, onbekend | Zichtbare toename, onbekend. |
| Respondent 9 | Tussen de 120 en 240 uur, gemiddeld 180 uur. (4,5* 40) | Onbekend |

Om bovenstaande lasten te verminderen, moeten de volgende veranderingen worden doorgevoerd in een ziekenhuis:

- Het aanreiken van documentatie moet minder tijd kosten.
- Er moeten integrale audits plaatsvinden.
- Er moet een betere afstemming en coördinatie komen tussen de interne auditor en de externe auditors.
- Evidence moet hergebruikt worden voor andere audits en niet dubbel getoetst worden.
- Er moet een integraal control framework worden gecreëerd die helpt om dubbeltellingen te voorkomen.

Een constatering van de grote verschillen is dat een UMC veel verschilt ten opzichte van een algemeen ziekenhuis. Daarnaast ontbreken er ook veel gegevens, dit maakt het lastiger om een realistisch overzicht te schetsen.

### 3.8.2 Efficiency

In de vragenlijst is de vraag gesteld wat voor efficiency de respondenten denken te behalen (in termen van tijd en geld). Dit op het gebied betreft de afstemming van informatiebeveiliging. Dit is in de tabel hieronder weergegeven.

| Respondenten | Efficiency per jaar |
|---|---|
| Respondent 1 | 50% |
| Respondent 2 | 50% |
| Respondent 3 | Onbekend |
| Respondent 4 | 40 uur |
| Respondent 5 | Geen efficiency |
| Respondent 6 | 10-15% |
| Respondent 7 | Onbekend |
| Respondent 8 | Onbekend |
| Respondent 9 | 10-25% |

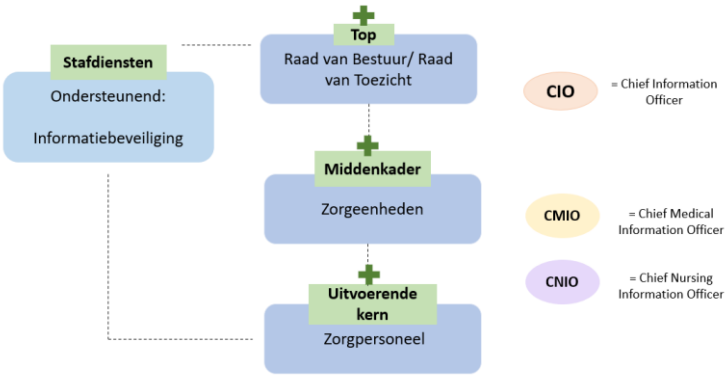
Dit betekent dat veel respondenten denken dat er wel efficiencyslagen te maken zijn, door o.a. overlappen beter in te delen en het auditproces beter te laten verlopen.

# 4. Aanbevelingen

De onderstaande aanbevelingen vloeien voort uit de hiervoor omschreven constateringen. Onderstaande aanbevelingen moeten in relatie met elkaar gezien worden en kunnen voor een optimaal resultaat niet opgepakt worden als losstaande aanbevelingen.

### 4.1 Informatiebeveiliging beter vertegenwoordigen in het ziekenhuis

Afhankelijk van de grootte van de organisatie zou(den) (er meer) informatiebeveiliging gerelateerde functies geïmplementeerd moeten worden in de lijnorganisatie. In figuur 7 wordt een voorbeeld weergegeven van zulke functies. In de afbeelding is te zien dat de Chief Information Officer, Chief Medical Information Officer en Chief Nursing Information Officer staan op volgorde van hun positie in de organisatiestructuur. De CIO bevindt zich aan top. Zowel de CMIO als de CNIO kunnen zich in het middenkader als in de uitvoerende kern bevinden.




Figuur 7 visuele weergave positie informatiebeveiliging met functies erbij

De CMIO en CNIO vormen het eerste aanspreekpunt voor medisch personeel en dragen bij aan de vertegenwoordiging van informatiebeveiliging binnen het primaire proces van een ziekenhuis, namelijk het verlenen van zorg. Mede dankzij de kennis die zij van beide werelden bezitten, zorg en informatiebeveiliging, vormen zij een belangrijke schakel binnen de organisatie.

Daarnaast is het ook belangrijk om de CISO (en soortgelijke functiepersonen) zichtbaar te maken in de organisatie. Medewerkers voldoende inlichten op de aanwezigheid van een CISO draagt bij aan de interactie tussen (medisch) personeel en de CISO. Op deze manier worden vragen vanuit de organisatie sneller gesteld aan de "bron", namelijk: de CISO.

### 4.2 Informatiebeveiliging behandelen als continu proces

Informatiebeveiliging wordt momenteel nog te vaak gezien als een incidenteel proces. Er wordt van audit naar audit gewerkt. Informatiebeveiliging zou juist behandeld moeten worden als een opzichzelfstaand proces waarbij verbetering steeds centraal staat. Het bewerkstelligen van dit proces zal meer interactie en initiatief van de CISO vergen. In de praktijk betekent dit ook dat de rol van de Raad van Bestuur minder gericht zal zijn op het verlenen van toestemming voor het uitvoeren van bepaalde werkzaamheden. De CISO zal op deze manier meer betrokken zijn bij de informatiebeveiliging in zijn geheel in plaats van van audit naar audit te werken. Doordat de CISO meer betrokken is bij het proces, kan hij of zij de Raad van Bestuur beter inlichten over dit proces en heeft de CISO een duidelijke set aan taken en bevoegdheden waarbinnen hij/zij kan handelen. Dit zal er weer voor zorgen dat de Raad van Bestuur meer inzicht krijgt in de informatiebeveiliging van het ziekenhuis. De Raad van Bestuur kan dan beter inspelen bij bijvoorbeeld besluiten die genomen worden over capaciteitsproblemen die zich eventueel voordoen binnen het proces van de informatiebeveiliging.

### 4.3 Duidelijke communicatie en meer interactie tussen auditor en ziekenhuis

Ziekenhuizen hebben graag een auditor die voldoende kennis en kunde bezit over de organisatie. Dit heeft namelijk een positief effect op de onderlinge communicatie en begripsvorming. Het inhoudelijk kunnen meepraten over wat er speelt in het ziekenhuis wordt dan ook benoemd als zeer belangrijk door de ziekenhuizen. De auditors benoemen dat zij de behoefte hebben om de uitvoerende kern van het ziekenhuis meer mee te nemen in de auditwerkzaamheden. In de huidige situatie is er meestal een vertegenwoordiger van het ziekenhuis aanwezig, maar lijkt dit niet voldoende te zijn om inhoudelijk mee te kunnen praten en zaken aan te kunnen tonen. Dit komt doordat de uitvoering van de beveiligingsmaatregelen belegd is bij de uitvoerende kern. Door een vertegenwoordiger en een uitvoerende medewerker aanwezig te hebben, wordt het auditproces voor beide partijen vergemakkelijkt.

### 4.4 Verantwoordingstool van personeel afstemmen op de gebruiker

De zorgprofessionals ervaren de tools waarmee zij verantwoording afleggen als zeer belastend. Uit interviews komt naar voren dat deze tools niet voldoende afgestemd worden op de zorgprofessional. Een voorbeeld van zo'n tool dat genoemd wordt, is ISMS. Deze tools worden vanuit het oogpunt van een kwaliteitsbeoordelaar, zoals een auditor, ingericht en niet vanuit een zorgprofessional die de tool uiteindelijk zal gebruiken om evidence te leveren. Hierdoor belemmert het de zorgprofessional in zijn dagelijkse werkzaamheden en wordt het ervaren als losstaande extra werkzaamheden. De zorgprofessional moet namelijk veel tijd en moeite steken om die extra werkzaamheden af te kunnen krijgen. Dat zorgt ervoor dat het lastig wordt voor de zorgprofessional om enerzijds de zorgtaken uit te voeren en anderzijds de verantwoording af te leggen in de tools. Door de tools beter in te richten op de eigen werkzaamheden van de zorgprofessional wordt de verantwoordingslast van de zorgprofessional verminderd. Om dat te bewerkstelligen is afstemming nodig met de zorgprofessional. Door meer te kijken naar de praktische haalbaarheid van de eisen die zo'n norm stelt en daar meer op te sturen, wordt het makkelijker voor een ziekenhuis om beter te kunnen voldoen aan een norm. Hier ligt wellicht ook een rol voor de auditor weggelegd. De auditor denkt in zo'n geval meer vanuit de organisatie zodat deze wel kan voldoen aan de gestelde eisen. Een belangrijke kanttekening hierbij is wel dat een auditor geen adviesfunctie mag vervullen indien deze een onafhankelijk oordeel moet leveren. Dit speelt voornamelijk bij audits die via een externe auditor uitgevoerd moeten worden. Bij interne audits heeft de auditor namelijk meer ruimte om ook eigen input te leveren.

Experiment Zinvolle Registratie (ZIRE), geïnitieerd door het NFU, is een voorbeeld om verantwoordingstools beter af te stemmen met het werk van zorgprofessionals. Dit project is gefocust op het verminderen van normen die veel registratielast opleveren en weinig patiënt risico's met zich dragen. Een voorbeeld is het noteren van bepaalde medische gegevens die geen toegevoegde waarde hebben voor zowel de patiënt als de behandelaar. Er wordt geëxperimenteerd met het loslaten van bepaalde registraties. De focus ligt meer op indicatoren die door verpleegkundigen en artsen zijn geselecteerd, omdat ze van toegevoegde waarde zijn voor patiënten en daadwerkelijk gebruikt worden voor kwaliteitsverbetering. De resultaten lijken tot nu toe veelbelovend te zijn (NFU Consortium Kwaliteit van Zorg, z.d.).

De ENSIA (Eenduidige Normatiek Single Information Audit) voor de Nederlandse gemeenten is een goed voorbeeld voor de ziekenhuizen. De aanpak van de ENSIA is erop gericht om in één keer verantwoording af te leggen over informatieveiligheid, gebaseerd op de normen die gelden volgens de Baseline Informatiebeveiliging Overheid (BIO) (*ENSIA Informatieveiligheid*, 2021). Dit zorgt ervoor dat zo'n verantwoordingstool minder last met zich meebrengt. Door dezelfde aanpak van de ENSIA toe te passen

in de ziekenhuizen zal de verantwoordingslast van de zorgprofessional aanzienlijk afnemen. De experts die zijn geïnterviewd kwamen opmerkelijk genoeg zelf[8] met de vergelijking om een soortgelijk initiatief te nemen als de ENSIA voor de ziekenhuizen.

### 4.5 Samenwerking opzoeken met andere ziekenhuizen

In de huidige situatie is er een bepaalde terughoudendheid aanwezig bij ziekenhuizen om samenwerking op te zoeken met andere ziekenhuizen. Dit terwijl er wel een mate van nieuwsgierigheid aanwezig is naar de werkwijze van andere ziekenhuizen m.b.t. bepaalde onderwerpen. Ziekenhuizen lijken de samenwerking alleen op te zoeken aan de hand van problemen die opdoen. Door meer "spontane" samenwerking op te zoeken ontstaat er kennisdeling en zal dit positief bijdragen aan de bedrijfsvoering van ziekenhuizen. Deze samenwerkingen zijn niet alleen formele samenwerkingen, maar focussen zich ook op operationele zaken die aan bod komen. Daarnaast lijkt er momenteel een ontwikkeling aan de gang te zijn waarbij ziekenhuiszorg steeds meer gecentraliseerd wordt. Dit heeft als gevolg dat ziekenhuizen met elkaar concurreren om de huidige positie in de markt te kunnen behouden. Terwijl ziekenhuizen in basis geen concurrenten van elkaar zouden moeten zijn, lijkt dit op dit moment wel te gebeuren.

### 4.6 Verhogen bewustzijn en bewustwording omtrent informatiebeveiliging

Een complex maar vaak terugkomend onderwerp is het bevorderen van de mate van bewustzijn van (medisch) personeel in ziekenhuizen. Men is op zoek naar manieren om dit te verhogen zonder dat er meer regels en verplichtingen opgelegd worden aan het personeel. Het opleggen van meer verplichtingen en regels zorgt namelijk voor een negatief effect op het personeel. Het implementeren van beveiligingsmaatregelen die zo min mogelijk impact hebben op de eindgebruikers en dus goed aansluiten binnen het werkproces, is dan ook een grote uitdaging. Hierbij zou dan ook gestreefd moeten worden naar een optimale veiligheid i.p.v. een ultieme veiligheid.

Ziekenhuizen zouden een vertaalslag moeten maken vanuit de motivatie van personeel om te werken binnen de zorg naar de bewustwording die daarbij komt kijken. Ziekenhuizen zouden zich daarbij moeten afvragen hoe zij het zorgpersoneel kunnen aanmoedigen om zorg te kunnen verlenen met de gewenste autonomie én daarbij ook binnen de kaders kunnen blijven van een veilige werkomgeving.

Een veel terugkomend antwoord is het herhalen van belangrijke zaken omtrent informatiebeveiliging. De kracht van herhaling moet niet onderschat worden. Ook het inzetten van multidisciplinaire teams kan bijdragen aan de bewustwording. Deze teams bestaan uit verschillende disciplines, zoals IT, zorg en kwaliteit. Op die manier wordt de onderlinge interactie en betrokkenheid ook bevorderd. Eerdergenoemde aanbevelingen dragen ook bij aan de bewustwording binnen ziekenhuizen, zoals de lokale aansturing via de CMIO en CNIO of lokale kwaliteitsfunctionarissen.

Het is lastig om een concreet antwoord te geven op de manier waarop de mate van bewustzijn kan worden verhoogd. Het vergt dan ook aanvullend onderzoek om de specifieke situaties van de ziekenhuizen nader te onderzoeken zodat daar concrete aanbevelingen uit voort kunnen komen.

Een mogelijke oorzaak van de lage mate van bewustzijn is wellicht te vinden in het curriculum van medische opleidingen die aangeboden worden. Hier kan verbetering in gebracht worden door studenten al redelijk vroeg in de loopbaan mee te nemen in informatiebeveiliging gerelateerde zaken

[8] Er is niet gevraagd tijdens het interview naar de ENSIA. De experts vertelden zelf uit eigen initiatief over de ENSIA en kwamen met het voorstel om een soortgelijke aanpak als de ENSIA te realiseren.

en de praktische werking ervan. Hier kan NOREA aan bijdragen door bijvoorbeeld vast onderdeel uit te maken van het curriculum van de medische opleidingen. Hierbij kan gedacht worden aan het geven van gastcolleges voor een bepaalde duur binnen een daarbij passend vak.

### 4.7 Opzetten van een integraal control framework

Door het grote aantal richtlijnen waaraan ziekenhuizen moeten voldoen, ondervinden ziekenhuizen een hoge auditlast. Bij het verkrijgen van o.a. het inzicht in de processen waarop deze richtlijnen van toepassing zijn, de betrokkenen en de risico's die gemoeid zijn met deze processen, kost het veel tijd om lijsten met alle controles die voortvloeien uit de normeringen te onderhouden. Om een beter inzicht hierin te verkrijgen, kan er een control framework worden gebruikt. Het control framework moet betrouwbaar zijn, maar voor eenieder ook zekerheid kunnen verlenen. Dat zijn niet alleen interne- en externe auditors, maar ook ziekenhuizen, belanghebbenden en financial auditors.

NOREA kan hierbij voor een deel helpen met het ontwikkelen van een integraal control framework, waarbij er dimensies worden toegepast in de aspecten: scope, diepgang, breedte en periodiciteit. Bij een norm dat gedetailleerd getoetst moet worden wordt er gebruik gemaakt van een 'narrow scope' en bij een andere norm wordt er een bredere scope worden gebruikt, maar hoeft dit niet gedetailleerd getoetst te worden en is de diepgang minder. Zo'n integraal control framework zou dat dus moeten omvatten, zodat elke auditor kan steunen op het oordeel. NOREA speelt hierbij een rol door te bewaken dat het integraal control framework vaktechnisch in orde is, en blijft.

In het control framework moet onder andere goed te zien zijn wat de processen, normen, overlap, functies en controls zijn. Als deze vijf aspecten veranderen, moet dit ook aangepast kunnen worden. Om dit te kunnen realiseren, moeten de processen, normen, overlap, functies en controls worden vastgelegd in het control framework en moeten deze worden verbonden met elkaar. Ook moeten de verschillende normeringen in het control framework zitten. Daarnaast kan er extra informatie worden toegevoegd, zoals verantwoordelijkheden en vervaldatums van certificeringen. Ook kan er een overzicht worden weergegeven wanneer er een audit wordt gedaan en wat er getoetst gaat worden, met aanduiding van de scope, diepgang, breedte, periodiciteit. De betrokken afdelingen staan hierbij ook vermeld. Op deze manier kan dit control framework een goede handreiking zijn op de voorbereiding van een audit. Er kunnen bijvoorbeeld herinneringen worden gestuurd voor taken aan desbetreffende personen zodat de deadlines worden gehaald. Vervolgens kan dit ook gemonitord worden. Gegevens uit het control framework moeten ook snel gedeeld kunnen worden aan auditors en betrokkenen. Uit het control framework kunnen databestanden uitgedraaid worden in Excel. Het voordeel van het control framework is dat het overlappen signaleert en dubbeltellingen minimaliseert. Daarnaast wordt er veel tijd bespaart bij het beheren van de IT-processen en werkt het control framework ook kostenbesparend.

Kortom, door een integraal control framework te gebruiken, levert dit de volgende voordelen op:

- Het control framework verleent eenieder zekerheid, zodat eenieder hierop kan steunen.
- Zoeken en aanreiken van documentatie kan snel, extra gevraagde documentatie kan snel aangereikt worden.
- Het control framework kan overlappende normen signaleren zodat de dubbeltellingen worden geminimaliseerd. Evidence wordt hergebruikt.
- Er wordt veel tijd bespaart bij het beheren van IT-processen.
- Het werkt kostenbesparend.

### 4.8 Een voorbeeld nemen van het KIK-V model om te implementeren

Om de overlap tussen partijen zoals DigiD, zorgverzekeraars, ministeries etc. te verminderen is het een idee om een datawarehouse te hebben waarbij alle auditobjecten en de uitvoering met uitkomsten en de testwerkzaamheden worden bewaard. Dan komt er een externe partij, die vervolgens zegt "Dat wil ik weten", en dan hoeft er alleen maar gecheckt te worden of die partij het daadwerkelijk wel mag weten. Dus je verzamelt alle informatie op één plek: in het datawarehouse.

Een voorbeeld waar dit al wordt uitgevoerd, is het KIK-V model, wat wordt gebruikt in de verpleeghuiszorg. Dit is een programma waarbij ketenpartijen samenwerken aan het stroomlijnen van de informatie-uitwisseling. Het doel van het KIK-V model is om te zorgen dat de uitwisseling van kwaliteitsinformatie beter verloopt. Hierbij moeten gegevens beter op elkaar worden afgestemd en moeten er gegevens worden hergebruikt. Dit zorgt o.a. voor een verlichting in de administratieve lasten van de ziekenhuizen en een betere kwaliteit. Hiervoor is er een samenwerking nodig met o.a. IGJ, NZA, ministerie van VWS, zorgaanbieders, zorgverzekeraars, NVZ en NFU en andere samenwerkende belanghebbenden.

Ook kan deze aanbeveling worden ingezet om dubbeltellingen te voorkomen, omdat het evidence ten eerste zal worden hergebruikt en ten tweede omdat de gegevensset die zal worden gedeeld aan de belanghebbenden hetzelfde zal zijn, omdat de belanghebbenden hierin samenwerken. Dit resulteert daarnaast in een betere kwaliteit van de gegevensset, omdat er van tevoren is bedacht door de belanghebbenden wat voor gegevens er moeten worden opgevraagd van de zorgaanbieders. Hierdoor gaat er minder tijd verloren aan het delen van gegevens die niet relevant zijn.

Als laatste vermindert dit de auditlast voor de ziekenhuizen, waarbij er dus minder tijd en geld verloren gaat, wat het probleem was van dit onderzoek.

Kortom, door een vergelijkbaar model zoals he KIK-V model te implementeren, bied dit de volgende voordelen:

- Administratieve lasten nemen af voor het ziekenhuis.
- Evidence wordt hergebruikt; voorkomen van overlappen.
- Betere kwaliteit van de gegevensset.
- Ziekenhuizen hoeven minder nawerk te doen.
- Betere afstemming tussen ketenpartijen en het ziekenhuis.
- Auditlast neemt af voor de ziekenhuizen.

### Rol van NOREA

Bovenstaande aanbevelingen staan allemaal in relatie met elkaar en leiden tot een verminderde auditlast in de ziekenhuizen.

De gesproken partijen vinden dat NOREA momenteel een heldere en duidelijke rol heeft. De directe rol die NOREA aan de hand van de organisatorische aanbevelingen kan aannemen is beperkt, omdat het veelal de interne organisatie van ziekenhuizen betreft. Wel zouden auditors een rol kunnen spelen in het verkleinen van de afstand tussen NOREA en het ziekenhuispersoneel door input op te halen vanuit ziekenhuizen en deze weer te leveren aan NOREA. Met die input kan NOREA de normenkaders die worden gehanteerd meer inrichten op de praktische haalbaarheid van de ziekenhuizen. Ook kan NOREA een rol spelen in het verzorgen van voorlichtingen op medische opleidingen, zodat dit een positief effect zal hebben op de mate van bewustzijn van het ziekenhuispersoneel.

Bovendien kan NOREA een rol spelen om de hoge auditlast aan te kaarten bij ketenpartijen en ziekenhuizen. Zo kunnen er vergaderingen plaatsvinden om een vergelijkbaar model te implementeren zoals het KIK-V model en om een integraal control framework op te zetten. Hiervoor is veel samenwerking nodig met belanghebbenden partijen, NOREA kan dit niet alleen.

Daarnaast wil NOREA dit onderzoek onder de aandacht brengen van de NVZ. De NVZ is op de hoogte van dit onderzoek en heeft haar nieuwsgierigheid over de resultaten ook uitgesproken. Aangezien de bestuurders van ziekenhuizen zich ook bevinden in het NVZ-bestuur is dit een belangrijk kanaal om de onderzoeksresultaten mee te delen zodat daar vervolgstappen uit voort kunnen komen.

## Bibliografie

Wikipedia-bijdragers. (2022, 29 april). *Lijst van Nederlandse ziekenhuizen*. Wikipedia. Geraadpleegd op 10 maart 2022, van https://nl.wikipedia.org/wiki/Lijst_van_Nederlandse_ziekenhuizen

Embargo geldt tot 5 september 2022 15:00 uur[i]

# 5. Bijlagen

## Bijlage **A**: Totale overzicht populatie met het aantal respondenten in verhouding tot de populatie

| Populatie<br>**Ziekenhuis** | **Totaal personen benaderd per ziekenhuis** | **Percentage aantal respondenten t.o.v. totale populatie** |
|---|---|---|
| Amsterdam UMC | 4 | 5,6% |
| Admiraal de Ruyterziekenhuis | 2 | 2,8% |
| Albert Schweitzer ziekenhuis | 1 | 1,4% |
| Alrijne ziekenhuis | 1 | 1,4% |
| Antoni van Leeuwenhoek ziekenhuis | 3 | 4,2% |
| Amphia ziekenhuis | 2 | 2,8% |
| Ziekenhuis Amstelland | 1 | 1,4% |
| St. Antonius Ziekenhuis | 1 | 1,4% |
| Bernhoven | 1 | 1,4% |
| Treant Zorggroep | 1 | 1,4% |
| BovenIJ Ziekenhuis | 1 | 1,4% |
| Bravis Ziekenhuis | 1 | 1,4% |
| Canisius-Wilhelmina ziekenhuis | 1 | 1,4% |
| Catharina Ziekenhuis | 1 | 1,4% |
| Deventer ziekenhuis | 1 | 1,4% |
| Diakonessenhuis | 1 | 1,4% |
| Dijklander ziekenhuis | 2 | 2,8% |
| Elkerliek Ziekenhuis | 2 | 2,8% |
| Erasmus MC | 2 | 2,8% |
| Flevoziekenhuis | 2 | 2,8% |
| Franciscus Gasthuis & Vlietland | 1 | 1,4% |

| | | |
|---|---|---|
| Ziekenhuis Gelderse Vallei | 2 | 2,8% |
| Gelre ziekenhuizen | 2 | 2,8% |
| Groene Hart ziekenhuis | 2 | 2,8% |
| HMC | 1 | 1,4% |
| IJsselland Ziekenhuis | 1 | 1,4% |
| Ikazia Ziekenhuis | 1 | 1,4% |
| Isala | 2 | 2,8% |
| Jeroen Bosch Ziekenhuis | 1 | 1,4% |
| Het LangeLand ziekenhuis | 1 | 1,4% |
| Laurentius Ziekenhuis | 1 | 1,4% |
| Leids Universitair Medisch Centrum | 2 | 2,8% |
| Maasstad Ziekenhuis | 3 | 4,2% |
| Maastricht UMC+ | 1 | 1,4% |
| Maasziekenhuis Pantein | 1 | 1,4% |
| Martini Ziekenhuis | 2 | 2,8% |
| Maxima MC | 1 | 1,4% |
| Meander Medisch Centrum | 2 | 2,8% |
| Medisch Centrum Leeuwarden | 1 | 1,4% |
| Noordwest Ziekenhuisgroep | 1 | 1,4% |
| Medisch Spectrum Twente | 1 | 1,4% |
| Nij Smellinghe | 1 | 1,4% |
| Ommelander Ziekenhuis Groningen | 1 | 1,4% |
| OLVG | 1 | 1,4% |
| Radboud UMC | 2 | 2,8% |
| Reinier de Graaf Gasthuis | 1 | 1,4% |
| Hagaziekenhuis | 2 | 2,8% |

| | | |
|---|---|---|
| Rijnstate | 1 | 1,4% |
| Rivas Zorggroep/ Beatrix Ziekenhuis | 1 | 1,4% |
| Ziekenhuis Rivierenland | 3 | 4,2% |
| Rode Kruis Ziekenhuis | 1 | 1,4% |
| Saxenburgh Medisch Centrum | 1 | 1,4% |
| Spijkenisse Medisch Centrum | 2 | 2,8% |
| St. Anna Zorggroep | 1 | 1,4% |
| St. Jans gasthuis | 1 | 1,4% |
| St Jansdal ziekenhuis | 1 | 1,4% |
| Slingeland ziekenhuis | 2 | 2,8% |
| Spaarne Gasthuis | 2 | 2,8% |
| Streekziekenhuis Koningin Beatrix | 1 | 1,4% |
| Tergooiziekenhuizen | 2 | 2,8% |
| Tjongerschans | 1 | 1,4% |
| Universitair Medisch Centrum Groningen | 3 | 4,2% |
| UMC Utrecht | 1 | 1,4% |
| Van Weel-Bethesda Ziekenhuis | 1 | 1,4% |
| VieCuri Medisch Centrum | 1 | 1,4% |
| Wilhelmina Ziekenhuis | 1 | 1,4% |
| Zaans Medisch Centrum | 1 | 1,4% |
| Ziekenhuis Groep Twente | 1 | 1,4% |
| ZorgSaam Ziekenhuis | 1 | 1,4% |
| Sint Antonius Ziekenhuis | 2 | 2,8% |
| Zuyderland Medisch Centrum | 2 | 2,8% |
| Totaal: **71** | Totaal: **103** | |

## Bijlage **B**: Het verstuurde bericht via LinkedIn

**De groene personen (kerndoelgroep)**

Beste,

Allereerst willen wij u alvast hartelijk danken voor uw deelname aan dit onderzoek. Wij zijn twee vierdejaarsstudenten in de richting Finance & Control en Bedrijfskunde aan de Hogeschool van Amsterdam en Hogeschool Windesheim. Momenteel voeren wij onze afstudeeronderzoeken uit bij Mazars binnen de afdeling IT Audit & Advisory. Voor ons afstuderen doen wij voor de NOREA (Nederlandse Orde van Register EDP-auditors) Kennisgroep ICT & Zorg onderzoek met als doel te achterhalen hoe het staat met de auditlast binnen ziekenhuizen. De scripties hebben een focus op informatiebeveiliging van ziekenhuizen in Nederland.

Om een beeld te vormen over de opzet, inrichting en auditlast in ziekenhuizen rondom het onderwerp informatiebeveiliging zouden wij u willen vragen om enkele vragen te beantwoorden. Deze resultaten zullen wij in het onderzoek en in onze scripties nader uitwerken.

De vragenlijst zal ongeveer 15 minuten van uw tijd in beslag nemen. U bent via LinkedIn geselecteerd op basis van uw relevante werkervaring. Er zal vertrouwelijk met uw gegevens worden omgegaan en de resultaten worden geheel anoniem verwerkt.

Mocht u nog vragen of opmerkingen hebben over de vragenlijst, neem dan contact op met Lisa of Emine via +3188 277 25 04/+3188 277 25 07 of lisa.dehaan@mazars.nl/emine.arslan@mazars.nl. Wij zullen uw vraag z.s.m. proberen te beantwoorden.

Nogmaals hartelijk dank voor uw deelname aan dit onderzoek. Graag verzoeken wij u de vragenlijst voor 14 april 2022 in te vullen.

[LINK] naar de vragenlijst: https://forms.office.com/r/bqNnt4cMm3

Met vriendelijke groet,

Lisa en Emine

Namens de Kennisgroep ICT & Zorg van NOREA

**De oranje personen (aanvullend doelgroep)**

Beste,

Allereerst willen wij u alvast hartelijk danken voor uw deelname aan dit onderzoek. Wij zijn twee vierdejaarsstudenten in de richting Finance & Control en Bedrijfskunde aan de Hogeschool van Amsterdam en Hogeschool Windesheim. Momenteel voeren wij onze afstudeeronderzoeken uit bij Mazars binnen de afdeling IT Audit & Advisory. Voor ons afstuderen doen wij voor de NOREA (Nederlandse Orde van Register EDP-auditors) Kennisgroep ICT & Zorg onderzoek met als doel te achterhalen hoe het staat met de auditlast binnen ziekenhuizen. De scripties hebben een focus op informatiebeveiliging van ziekenhuizen in Nederland.

Om een beeld te vormen over de opzet, inrichting en auditlast in ziekenhuizen rondom het onderwerp informatiebeveiliging zouden wij u willen vragen om enkele vragen te beantwoorden. Deze resultaten zullen wij in het onderzoek en in onze scripties nader uitwerken.

De vragenlijst zal ongeveer 15 minuten van uw tijd in beslag nemen. Er zal vertrouwelijk met uw gegevens worden omgegaan en de resultaten worden geheel anoniem verwerkt. Mocht u de vragen

niet kunnen beantwoorden, dan verzoeken wij u gelieve de vragenlijst door te sturen (link staat onderaan) naar de juiste persoon binnen de organisatie.

Mocht u nog vragen of opmerkingen hebben over de vragenlijst, neem dan contact op met Lisa of Emine via +3188 277 25 04/+3188 277 25 07 of lisa.dehaan@mazars.nl/emine.arslan@mazars.nl. Wij zullen uw vraag z.s.m. proberen te beantwoorden.

Nogmaals hartelijk dank voor uw deelname aan dit onderzoek. Graag verzoeken wij u de vragenlijst voor 14 april 2022 in te vullen.

[LINK] naar de vragenlijst: https://forms.office.com/r/bqNnt4cMm3

Met vriendelijke groet,

Lisa en Emine

Namens de Kennisgroep ICT & Zorg van NOREA

[i] Embargo geldt tot 5 september 2022, 15:00 uur.