SHIELD vzw

State of Cybersecurity in Belgian Hospitals

Samenvatting

Wim Bijnens
01/12/2025

Inhoudsopgave

1. Samenvatting

Dit rapport biedt een duidelijk en bruikbaar overzicht van de CyberFundamentals 2023 Basic-volwassenheid van Belgische ziekenhuizen. Uit de analyse blijkt dat de volwassenheid van de sector verbetert, maar nog steeds aanzienlijk onder de vereiste drempel voor april 2026 blijft. Slechts **23,8 %** van de Basic-controles voldoet aan het vereiste maturiteitsniveau van **2,50**, waarbij documentatie (gemiddeld **1,57**) ver achterblijft op implementatie (**2,18**).

Het domein dat de meeste aandacht vereist, is **Identificatie**. Dit weerspiegelt duidelijk fundamentele tekortkomingen op het gebied van activabeheer, risicobeoordeling en governance. De kloof tussen de beste en slechtste presteerders is aanzienlijk (**+1,21 punten**), wat wijst op ongelijke paraatheid binnen de sector. Met name psychiatrische ziekenhuizen vertonen de grootste structurele tekortkomingen.

Ziekenhuizen die daadwerkelijk gebruikmaken van onze **SHIELD Library** laten een sterke vooruitgang zien, met een verbetering van de documentatiescores van **2,31 naar 3,40**. Dit bevestigt dat gestandaardiseerde en sectorspecifieke sjablonen de volwassenheid versnellen, waarbij wel rekening moet worden gehouden met voldoende personeel en tijd.

Om aan de vereisten van april 2026 en 2027 te voldoen, moet de sector prioriteit geven aan versnelde documentatie-inspanningen, gerichte ondersteuning voor ziekenhuizen met onvoldoende middelen, volledige beoordelingsdekking, sterkere betrokkenheid van het management en vroegtijdige voorbereiding op de strengere volwassenheidsniveaus van 2027.

1.1.1. Sectorstatus

- 23,8% van de basiscontroles voldoet aan de normen
- Documentatie: 1,57 gemiddeld
- Implementatie: 2,18 gemiddeld
- Psychiatrische ziekenhuizen hebben de grootste achterstand

1.1.2. Kritieke verschillen

- “Identificatie” is het zwakste domein
- Grote kloof tussen instellingen aan de top en onderaan
- Belangrijk/essentieel (2027) ver onder de doelstelling

1.1.3. Wat werkt

- SHIELD Library verbetert documentatie snel (2,31 → 3,40)

1.1.4. Hoogste prioriteiten

1. Documentatie versnellen
2. Ondersteuning van ziekenhuizen met te weinig middelen
3. Beoordelingsdekking voltooien

4. betrokkenheid van leidinggevenden waarborgen
5. vroeg beginnen voor 2027

1.1.5. Beleidsmaatregelen

Ontwikkel een nationaal documentatieprogramma, monitoring van de volwassenheid, structurele financiële ondersteuning voor ISMS-personeel (Information Security Management System) en structuren voor peer-learning.

1.2. Huidige maturiteit: wat de cijfers laten zien

De huidige maturiteit van Belgische ziekenhuizen blijft ver onder de vereiste drempel voor april 2026. Slechts **23,8%** van alle beoordeelde basiscontroles voldoet aan de verplichte maturiteitsscore van **2,50**, terwijl **76,2%** daar niet aan voldoet. Dit betekent dat er weliswaar veel beveiligingspraktijken bestaan in operationele teams, maar dat deze niet consistent worden gedocumenteerd, geformaliseerd of ingebed in bestuursstructuren.

Over de 55 beoordeelde ziekenhuizen genomen is de gemiddelde volwassenheidsscore **1,57 voor documentatie** en **2,18 voor implementatie**, wat een structurele kloof tussen 'doen' en 'bewijzen' weerspiegelt.

In dit rapport wordt de term *documentatie* gebruikt in overeenstemming met de CyberFundamentals-terminologie zoals gedefinieerd door het Centrum voor Cybersecurity België. De praktische reikwijdte van documentatie gaat echter veel verder dan geschreven artefacten. Het omvat ook de definitie, acceptatie en instandhouding van processen, organisatorisch beleid, bestuursstructuren en de consistente integratie van deze elementen in de dagelijkse praktijk. Effectieve documentatie vereist daarom niet alleen het produceren van tekstuele materialen, maar ook het verankeren ervan in de organisatorische mentaliteit, ondersteund door geschikte tools, toewijzing van middelen en terugkerende onderhoudscycli. Het begrijpen van documentatie in deze bredere zin is essentieel voor een juiste interpretatie van de maturiteitskloof die in de sector wordt waargenomen.

Deze kloof is zichtbaar in de hele sector en geeft aan dat ziekenhuizen vaak vertrouwen op informele processen, ongedocumenteerde praktijken en teamspecifieke kennis. Als gevolg hiervan kan hun cyberbeveiligingsparaatheid niet worden aangetoond, gereproduceerd of gecontroleerd.

Het gebrek aan documentatie verhoogt de audit- en nalevingsrisico's aanzienlijk, vertraagt gecoördineerde sectorbrede verbeteringen en maakt duurzaam cyberbeveiligingsbeheer moeilijk. Aangezien documentatie een voorwaarde is voor herhaalbaarheid, verantwoordingsplicht en naleving, is deze kloof de belangrijkste reden waarom de meeste ziekenhuizen momenteel het risico lopen de maturiteitsdoelstelling van april 2026 niet te halen.

Deze resultaten bevestigen een systemisch patroon: sterke operationele teams zorgen ervoor dat veel controles in de praktijk worden geïmplementeerd, maar het ontbreken van gestructureerde documentatiekaders, toegewijd personeel en het alloceren van tijd

verhindert dat de maturiteitsniveaus in het vereiste tempo stijgen. Het aanpakken van dit documentatietekort is daarom cruciaal om de groei van de maturiteit in de Belgische ziekenhuissector te versnellen.

Verschillende ziekenhuizen in België beschikken al over een ISO/IEC 27001-certificering. Dit is niet in tegenspraak met de CyberFundamentals-resultaten die in dit rapport worden gepresenteerd. ISO 27001 evalueert of er een informatiebeveiligingsbeheersysteem is opgezet en continu wordt verbeterd , terwijl CyberFundamentals een strikt, controle-per-controle scoringsmodel met beperkte granulariteit hanteert. Een controle die als "2" wordt gescoord, kan in de praktijk dicht bij "3" liggen, maar wordt toch als niet-conform gerapporteerd totdat aan alle volwassenheidseisen is voldaan.

Als gevolg hiervan kunnen ziekenhuizen een functionerend ISMS hanteren en voldoen aan de ISO 27001-vereisten, terwijl ze toch lagere CyberFundamentals-scores krijgen, met name op het gebied van de volledigheid van de documentatie en de diepgang van het bewijsmateriaal. Het is essentieel om dit onderscheid te verduidelijken: CyberFundamentals doet geen afbreuk aan de bestaande volwassenheid van het bestuur, maar de beperkte scoringsmethode benadrukt de specifieke hiaten die moeten worden gedicht om de drempels van april 2026 en 2027 te halen.

1.3. Volwassenheid per CyFun-domein: Identificatie is het zwakste punt

Van de vijf CyFun-pijlers **is Identificatie veruit het slechtst presterende domein**, waarbij slechts **15,9%** van de ziekenhuizen de vereiste volwassenheidsscore van 2,50 haalt. Dit maakt Identificatie tot de belangrijkste structurele lacune in de sector. Figuur 4 (te vinden in het volledige rapport) illustreert hoe **Identificatie** consequent lager scoort dan Beschermen, Detecteren, Reageren en Herstellen in alle ziekenhuizen en regio's.

Het domein Identificeren omvat de fundamentele elementen van cyberbeveiligingsbeheer, waaronder **activabeheer, software- en gegevensinventarissen, risicobeoordeling, bestuursstructuren en gegevensclassificatie**. Deze componenten bepalen of een ziekenhuis weet *welke activa het bezit, welke risico's het loopt en wie verantwoordelijk is* voor het beheer ervan. Verschillende controles binnen dit domein, zoals ID.AM-2.1 (software-inventaris), ID.AM-3.1 (informatie-inventaris) en ID.RA-5.1 (risicobeoordeling), behoren tot de **laagst scorende controles in de hele basisset**, met nalevingsniveaus tussen 9% en 12%.

Zwakke punten in Identificatie hebben gevolgen voor de hele sector. Zonder een volledig overzicht van activa en risico's hebben ziekenhuizen moeite om prioriteiten te stellen voor beveiligingsmaatregelen, kunnen ze geen betrouwbare investeringsplannen maken en hebben ze moeite om te voldoen aan documentatie- en auditvereisten. Bovendien is Identificatie een voorwaarde voor een effectieve uitvoering van de domeinen Beschermen, Detecteren, Reageren en Herstellen. Bijvoorbeeld:

- zonder nauwkeurige inventarisaties van activa kunnen patching en kwetsbaarheidsbeheer niet volledig worden uitgevoerd

- zonder governance en rolomschrijvingen kan het beleid niet worden gehandhaafd
- zonder risicobeoordelingen kunnen ziekenhuizen geen prioriteiten stellen of hun behoefte aan middelen rechtvaardigen
- zonder gegevensclassificatie worden gegevensverliespreventie en netwerksegmentatie inconsistent

Omdat identificatie de basis vormt waarop alle andere cyberbeveiligingsmaatregelen zijn gebaseerd, vormt de zwakke volwassenheid ervan een **cruciaal strategisch risico** voor de sector en een belangrijke belemmering voor het bereiken van de naleving in april 2026 en 2027. Het versterken van identificatie moet daarom een topprioriteit zijn voor ziekenhuizen en beleidsmakers.

1.4. Regionale vergelijking: de volwassenheid verschilt per regio.

In de drie regio's verschillen de volwassenheidsniveaus aanzienlijk, maar ze vertonen allemaal hetzelfde structurele patroon: de implementatiescores zijn hoger dan de documentatiescores. Uit de resultaten blijkt dat Vlaanderen consequent de hoogste volwassenheid rapporteert, gevolgd door Wallonië, terwijl Brussel het verst verwijderd blijft van de doelstelling voor april 2026.

De regionale resultaten zijn als volgt:

- **Brussel:** 1,29 documentatie, 1,99 implementatie
- **Wallonië:** 1,49 documentatie, 2,04 implementatie
- **Vlaanderen:** 1,61 documentatie, 2,22 implementatie

Afgezet tegen de vereiste maturiteitsscore van 2,50 resulteert dit in documentatieverschillen van **1,21 in Brussel**, **1,01 in Wallonië** en **0,89 in Vlaanderen**, en in implementatieverschillen van respectievelijk **0,51, 0,46 en 0,28**.

Deze verschillen weerspiegelen verschillende onderliggende factoren. Ziekenhuizen in Vlaanderen hebben over het algemeen grotere of meer gespecialiseerde digitale en beveiligingsteams, meer volwassen bestuursstructuren en een hoger niveau van operationele standaardisatie binnen netwerken. Ziekenhuizen in Brussel hebben te maken met grotere structurele beperkingen, waaronder beperkte middelen en een grotere organisatorische complexiteit, waardoor hun capaciteit om processen te formaliseren en documentatie bij te houden beperkt is. Wallonië bevindt zich tussen deze twee profielen in, met een matige implementatiecapaciteit maar nog steeds aanzienlijke uitdagingen op het gebied van documentatie.

De regionale vergelijking bevestigt een sectorbreed patroon: de implementatie vordert, maar documentatie blijft de belangrijkste belemmering. De resultaten laten ook zien dat sommige regio's meer ondersteuning en hulp nodig hebben om hun achterstand in volwassenheid in te lopen. Als deze regionale verschillen niet worden aangepakt, kan dit

leiden tot ongelijke nalevingsgereedheid en inconsistente niveaus in weerbaarheid in het hele land.

Shield vzw I Kempische Steenweg 303/200 I 3500 Hasselt I info@shield-vzw.be

1.5. Volwassenheid per type ziekenhuis.

De volwassenheid van Belgische ziekenhuizen varieert aanzienlijk per type ziekenhuis, wat een weerspiegeling is van verschillen in personeelscapaciteit, bestuursstructuren en de beschikbaarheid van specifieke functies op het gebied van informatiebeveiliging. Zoals blijkt uit de figuren 7-9 (te vinden in het volledige rapport), bereiken algemene ziekenhuizen en universitaire ziekenhuizen consequent een hogere volwassenheid, terwijl psychiatrische ziekenhuizen op alle gebieden achterblijven, met name op het gebied van documentatie.

Algemene ziekenhuizen

Algemene ziekenhuizen scoren **1,66 op documentatie** en **2,23 op implementatie**. Hun hogere maturiteit kan grotendeels worden verklaard door grotere ICT- en beveiligingsteams, gestructureerde bestuursprocessen en meer geformaliseerde administratieve procedures. Deze ziekenhuizen zijn dan ook beter gepositioneerd om de maturiteitsdrempel van april 2026 te halen, op voorwaarde dat de documentatie-inspanningen worden opgevoerd.

Psychiatrische ziekenhuizen

Psychiatrische ziekenhuizen vertonen een aanzienlijk lagere maturiteit, met een score van **1,30 voor documentatie** en **2,04 voor implementatie**. Veel van deze ziekenhuizen werken met zeer beperkte ICT-personeelsbezetting, weinig of geen speciale beveiligingsfuncties en minder geformaliseerde bestuursstructuren. Dit resulteert in ontbrekende of onvolledige documentatie en beperkte capaciteit om processen te integreren. Zonder gerichte ondersteuning lopen psychiatrische ziekenhuizen het grootste risico om de doelstellingen voor 2026 en 2027 niet te halen.

Universitaire ziekenhuizen

Universitaire ziekenhuizen scoren **1,79 op documentatie** en **2,23 op implementatie**, waarmee ze beter presteren dan andere soorten ziekenhuizen, met name op het gebied van documentatiekwaliteit. Hun bredere governance-volwassenheid, grotere teams en meer gestandaardiseerde processen dragen bij aan deze betere prestaties. Op verschillende gebieden – met name reageren en herstellen – vormen ze een benchmark voor de sector.

Deze vergelijking laat een duidelijke structurele trend zien: volwassenheid hangt rechtstreeks samen met de beschikbare personeelsbezetting, governancecapaciteit en specifieke expertise op het gebied van informatiebeveiliging. Algemene en universitaire ziekenhuizen profiteren van sterkere governance- en operationele structuren, waardoor ze sneller in volwassenheid kunnen groeien. Psychiatrische ziekenhuizen hebben echter aanhoudende en gerichte sectorale ondersteuning nodig om structurele capaciteitsbeperkingen te overwinnen. Met deze verschillen moet rekening worden gehouden bij het vormgeven van de nationale strategie, financiering en nalevingsplanning.

1.6. De koplopers versus de volgers

De maturiteitskloof tussen de best en slechtst presterende ziekenhuizen is aanzienlijk en benadrukt een structurele kloof binnen de Belgische gezondheidszorgsector. Zoals blijkt uit figuren 7, 10 en 11 (te vinden in het volledige rapport), behalen de best presterende ziekenhuizen een totale maturiteitsscore van 2,64, terwijl de slechtst presterende ziekenhuizen gemiddeld slechts 1,43 scoren. Dit verschil van 1,21 punten weerspiegelt aanzienlijke verschillen in governance, middelen en het vermogen om cyberbeveiligingsprocessen te formaliseren.

Koplopers

De vijf best presterende ziekenhuizen, die allemaal in Vlaanderen zijn gevestigd, vertonen een hoge maturiteit op de meeste domeinen, ondersteund door goed ontwikkelde bestuursstructuren, specifieke middelen voor informatiebeveiliging en stabiele processen. Hun scores voor documentatie (**2,56**) en implementatie (**2,72**) tonen aan dat cyberbeveiliging zowel geformaliseerd als consistent uitgevoerd wordt. Ze blinken vooral uit in communicatie, responsplanning, beveiligingsmonitoring en informatiebeschermingsprocessen. Deze organisaties zijn structureel goed gepositioneerd om te voldoen aan de vereisten van april 2026 of deze te blijven naleven.

Volgers

De vijf ziekenhuizen met de laagste scores – zowel algemene als psychiatrische ziekenhuizen – scoren gemiddeld **1,07 voor documentatie**, waarbij verschillende categorieën het minimumniveau van **1,00** halen, wat wijst op afwezige of zeer onvolledige documentatie. De implementatiematuriteit blijft ook beperkt, met een score van **1,79**, en er zijn kritieke hiaten in responsplanning, herstelplanning en verbeteringen. Deze ziekenhuizen werken doorgaans met beperkte personeelscapaciteit, minder formeel bestuur en minimale toegewijde beveiligingsfuncties, wat hun vermogen om processen te formaliseren en consistente praktijken in te voeren belemmert.

Betekenis van de kloof

Deze kloof in volwassenheid bevestigt een **tweesporig cybersecuritylandschap** binnen de Belgische gezondheidszorg. Zonder gerichte ondersteuning is het onwaarschijnlijk dat de slechtst presterende ziekenhuizen – met name psychiatrische instellingen – de volwassenheidseisen voor 2026 of 2027 zullen halen. Als deze kloof niet wordt aangepakt, zal dit leiden tot een inconsistente nationale baseline voor cybersecurity, waardoor het systeemrisico toeneemt en de operationele continuïteit in de hele sector in gevaar komt.

1.7. Voordelen van de SHIELD-bibliotheek

De SHIELD Library (een vrij beschikbare open source-bibliotheek – **© 2025 Shield VZW – Licentie CC BY-NC-SA 4.0**) is een van de meest effectieve versnellers gebleken voor het verbeteren van de documentatievolwassenheid in de Belgische ziekenhuissector. Zoals blijkt uit figuren 12 en 13 (te vinden in het volledige rapport), hebben ziekenhuizen die de bibliotheek hebben geïmplementeerd een aanzienlijke verbetering van de documentatiekwaliteit gerealiseerd, met een stijging van de gemiddelde documentatiescores **van 2,31 naar 3,40** in ongeveer een jaar tijd. Deze verbetering toont aan dat gestructureerde, sectorspecifieke sjablonen de voortgang naar CyberFundamentals-compliance aanzienlijk kunnen versnellen.

De impact van de bibliotheek wordt voornamelijk bepaald door de uitgebreide en gestandaardiseerde reeks beleidsregels, processen, procedures en ondersteunende documenten, die volledig zijn afgestemd op ISO/IEC 27001:2022 en CyberFundamentals 2023. Omdat het materiaal openbaar beschikbaar is en is afgestemd op de ziekenhuisomgeving, kunnen instellingen het direct implementeren zonder dat ze zelf documentatie hoeven te ontwikkelen. Dit vermindert de administratieve werklast, verbetert de consistentie en stelt kleinere teams in staat om documentatie van hogere kwaliteit te leveren.

De bibliotheek is echter **geen kant-en-klare oplossing**. Voor een effectief gebruik zijn gekwalificeerd personeel, tijd en een sterke lokale betrokkenheid nodig om de sjablonen aan te passen, in de dagelijkse praktijk te integreren en up-to-date te houden. Sommige ziekenhuizen hebben een tragere implementatie doorlopen omdat de bibliotheek de lat hoger heeft gelegd: naarmate de documentatie verbeterde, werden de beoordelingen grondiger en kwamen hiaten in de uitvoering van processen aan het licht. Dit onderstreept het belang van het koppelen van documentatieverbetering aan gestructureerde implementatieondersteuning.

Over het algemeen vertegenwoordigt de SHIELD-bibliotheek een **schaalbare, op bewijs gebaseerde methode** om de volwassenheid in de hele sector te vergroten. Met voldoende personeel en betrokkenheid van het bestuur kan deze bibliotheek de documentatiekloof aanzienlijk verkleinen en ziekenhuizen helpen om te voldoen aan de volwassenheidseisen voor 2026 en 2027.

1.8. Prioriteiten voor april 2026 en 2027

Om te voldoen aan de CyberFundamentals Basic-vereisten van april 2026 en om ons voor te bereiden op de strengere belangrijke en essentiële controles in 2027, is gecoördineerde actie in de hele sector nodig. Uit de beoordelingen blijkt duidelijk dat de huidige maturiteitskloof niet kan worden gedicht zonder gerichte ondersteuning, betrokkenheid van het bestuur en versnelde documentatie-inspanningen. De volgende prioriteiten vormen de basis van de vereiste nationale verbeteringsstrategie.

Prioriteit 1 – versnel de documentatie door gestructureerde invoering van de SHIELD-bibliotheek

Documentatie blijft de grootste maturiteitskloof in de sector. Systematische invoering van de SHIELD Library, in combinatie met beschermde tijd en lokaal eigenaarschap, kan de documentatiescores in alle ziekenhuiscategorieën snel verhogen. Dit is essentieel om tegen april 2026 de basismaturiteitsdrempel van 2,50 te bereiken.

Prioriteit 2 – gerichte ondersteuning bieden aan ziekenhuizen met onvoldoende middelen en psychiatrische ziekenhuizen

Psychiatrische ziekenhuizen en kleinere instellingen kampen met structurele beperkingen op het gebied van middelen, waardoor onafhankelijke naleving onwaarschijnlijk is. Op maat gemaakte ondersteuning – via regionale expertisecentra, gedeelde beveiligingsmiddelen of gerichte financiering – zal nodig zijn om de maturiteitskloof te dichten en een tweesporenbeleid op het gebied van cyberbeveiliging te voorkomen.

Prioriteit 3 – voltooiing van de beoordelingsdekking in de hele sector

Verschillende ziekenhuisentiteiten zijn nog niet beoordeeld. Door het beoordelingsprogramma te voltooien, wordt ervoor gezorgd dat de volwassenheid consistent wordt gemeten en dat de nationale planning het volledige risicolandschap weerspiegelt. Dit is noodzakelijk voor evidence-based beleidsbeslissingen en gecoördineerde verbetering van de sector.

Prioriteit 4 – versterking van de betrokkenheid van het management en het voorzien van tijd

Ziekenhuizen met de hoogste scores blinken uit in sterke betrokkenheid van het management en toegewijd ISMS-personeel. Leidinggevenden moeten cyberbeveiliging als een strategisch domein beschouwen, tijd vrijwaren en toewijzen voor documentatie- en governanceactiviteiten en ervoor zorgen dat verbeteringen op het gebied van cyberbeveiliging in de hele organisatie worden geïntegreerd.

Prioriteit 5 – tijdig voorbereiden op de strengere volwassenheidseisen van 2027

De belangrijke en essentiële kernmaatregelen, waarvoor een minimumscore van 3,0 vereist is, scoren momenteel gemiddeld slechts **1,33 voor documentatie** en **1,90 voor implementatie**. Deze lage uitgangswaarden onderstrepen de noodzaak van vroegtijdige voorbereiding, gecoördineerde verbeteringsplanning en sectorbrede toewijzing van middelen. Wachten tot 2026 zou een onbeheersbare nalevingslast met zich meebrengen.

Samen benadrukken deze prioriteiten de noodzaak van een gestructureerde, met middelen ondersteunde en centraal gesteunde aanpak. Zonder versnelde documentatie, gerichte hulp voor kwetsbare segmenten en versterkte betrokkenheid van het management loopt een aanzienlijk deel van de sector het risico niet te voldoen aan de CyberFundamentals-vereisten voor zowel 2026 als 2027.

1.9. Beleidsaanbevelingen

De bevindingen voor alle ziekenhuiscategorieën, regio's en CyFun-domeinen maken duidelijk dat de volwassenheid van de sector zonder gecoördineerde beleidsmaatregelen niet in het vereiste tempo zal verbeteren. Om ziekenhuizen te helpen aan de vereisten van april 2026 en 2027 te voldoen, worden de volgende beleidsmaatregelen op nationaal en regionaal niveau aanbevolen.

1. Een sectorbreed documentatie- en governanceprogramma opzetten

Een uniform documentatiekader, gebaseerd op de SHIELD Library, moet formeel worden aangenomen als nationale norm. Dit programma moet ziekenhuizen begeleiden bij de implementatie van consistent beleid, processen en bestuursstructuren, ondersteund door duidelijke mijlpalen, sjablonen en richtlijnen.

2. Gerichte financiering en structurele ondersteuning bieden aan kleinere en psychiatrische ziekenhuizen

Psychiatrische ziekenhuizen en instellingen met onvoldoende middelen hebben specifieke financiële en operationele ondersteuning nodig om ISMS-capaciteit op te bouwen, gespecialiseerd personeel aan te nemen of te delen en documentatieprocessen in te voeren. Zonder dergelijke ondersteuning zullen er nalevingslacunes blijven bestaan en zal de sector uiteenvallen in verschillende maturiteitsniveaus.

Hoewel structurele financiering nodig is voor alle ziekenhuizen, hebben kleinere instellingen en psychiatrische ziekenhuizen aanvullende en gedifferentieerde ondersteuning nodig. Door hun beperkte personeelscapaciteit, organisatorische beperkingen en het ontbreken van specifieke beveiligingsfuncties is het onrealistisch om te verwachten dat zij zonder gerichte hulp de vereiste volwassenheid bereiken. Deze organisaties hebben te maken met een onevenredige last in verhouding tot hun beschikbare middelen en blijven daarom een prioritaire groep voor versterkte financiële en operationele ondersteuning binnen de nationale strategie.

In de praktijk blijft het gebrek aan structurele financiering echter niet beperkt tot kleinere of psychiatrische ziekenhuizen. Voor veel algemene ziekenhuizen blijft een ontoereikend toegewezen budget de belangrijkste belemmering om documentatie- en governanceprocessen op het vereiste volwassenheidsniveau te brengen. Door extra financiële middelen toe te wijzen aan *alle* ziekenhuizen zouden zij gespecialiseerd fulltime personeel kunnen aanwerven, zoals een documentatie- of compliance officer, wat essentieel is voor het bereiken van duurzame verbeteringen.

Bovendien zou het voor toekomstige beoordelingen waardevol zijn om te controleren of elk ziekenhuis formeel een verantwoordelijke persoon of team heeft aangewezen voor documentatie- en compliance taken. Dit zou kunnen dienen als een extra meetpunt in komende evaluatiecycli en zou de transparantie en verantwoordingsplicht in bestuursstructuren helpen versterken.

3. Een nationaal systeem voor het monitoren van de maturiteit implementeren met driemaandelijkse updates

Een gecentraliseerd dashboard moet volwassenheidsscores verzamelen, hiaten aan het licht brengen en de voortgang in alle ziekenhuizen bijhouden. Driemaandelijkse updates maken evidence-based planning, vroegtijdige identificatie van stagnatie en transparante rapportage aan bestuursorganen mogelijk.

4. Voer beoordelingen uit bij alle entiteiten om volledige nationale dekking te garanderen

Alle ziekenhuizen en relevante zorginstellingen moeten worden beoordeeld aan de hand van de standaard SHIELD-methodologie. Een uitgebreide dekking zorgt ervoor dat de volwassenheidsplanning het volledige risicolandschap weerspiegelt en voorkomt blinde vlekken in de nationale cyberbeveiligingsstrategie.

5. Gestructureerd peer-learning tussen goed en slecht presterende ziekenhuizen bevorderen

Ziekenhuizen met hoge prestaties tonen consequent maturiteitsbevorderende praktijken, zoals een sterke afstemming van het bestuur, robuuste documentatieprocessen en toegewijd cyberbeveiligingspersoneel. Een gestructureerd model voor peer-learning – via regionale werkgroepen, gedeelde middelen of thematische workshops – kan de volwassenheidsgroei in de hele sector versnellen.

Deze beleidsaanbevelingen zijn bedoeld om een gecoördineerde, consistente en rechtvaardige aanpak van cybervolwassenheid in Belgische ziekenhuizen te creëren. De implementatie ervan zal helpen om de documentatiekloof te dichten, kwetsbare instellingen te ondersteunen, de transparantie te verbeteren en ervoor te zorgen dat alle ziekenhuizen vooruitgang boeken in de richting van de CyberFundamentals-vereisten van april 2026 en 2027.

1.10. Conclusie

Uit de beoordelingen voor 2025 blijkt dat de Belgische ziekenhuissector vooruitgang boekt op het gebied van cyberbeveiligingsvolwassenheid, maar niet in het tempo dat nodig is om te voldoen aan de CyberFundamentals-drempels van april 2026 en 2027. Hoewel de implementatie in de meeste domeinen vordert, **blijft documentatie de belangrijkste belemmering**, met aanhoudende hiaten op het gebied van governance, activabeheer en risicobeoordeling.

Algemene en universitaire ziekenhuizen vertonen een sterkere ontwikkeling op het gebied van maturiteit, ondersteund door grotere teams en meer formele bestuursstructuren. Psychiatrische ziekenhuizen hebben echter te maken met structurele beperkingen waardoor ze zonder gerichte hulp een groot risico lopen om niet aan de eisen te voldoen. De aanzienlijke kloof tussen de best en slechtst presterende instellingen bevestigt dat er **sprake is van een ontwikkeling in twee snelheden**, die moet worden aangepakt om een consistente nationale basisnorm voor cyberweerbaarheid te handhaven.

De SHIELD Library is een effectieve versneller gebleken voor de volwassenheid van documentatie, maar het succes ervan hangt af van gekwalificeerd personeel, toegewezen tijd en een sterk engagement van het management. Om de maturiteitskloof te dichten, is het essentieel om het gebruik ervan uit te breiden, de governancecapaciteit te versterken en systematische ondersteuning te bieden aan ziekenhuizen met onvoldoende middelen.

Om te voldoen aan de basisvereisten voor 2026 en ons voor te bereiden op de strengere belangrijke en essentiële controles in 2027, is **gecoördineerde actie op nationaal niveau** nodig, waaronder gestructureerd bestuur, gerichte financiering, uitgebreide beoordelingsdekking en regelmatige monitoring van de volwassenheid. Met gerichte investeringen, sterk uitvoerend leiderschap en consistent gebruik van de SHIELD-methodologie kan de sector een stabiel en duurzaam niveau van cyberbeveiligingsvolwassenheid bereiken dat de gezondheidszorg, de veiligheid van patiënten en de veerkracht van de samenleving beschermt.