SHIELD vzw

State of Cybersecurity in Belgian Hospitals

Résumé

Wim Bijnens
01/12/2025

Table des matières

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

1. Résumé

Ce rapport offre un aperçu clair et utile de la maturité des hôpitaux belges au regard des CyberFundamentals 2023 Basic. L'analyse montre que la maturité du secteur s'améliore, mais reste encore bien en deçà du seuil requis pour avril 2026. Seuls **23,8 %** des contrôles Basic satisfont au niveau de maturité requis de **2,50**, la documentation (**1,57** en moyenne) étant loin derrière la mise en œuvre (**2,18**).

Le domaine qui nécessite le plus d'attention est **celui de l'identification**. Cela reflète clairement des lacunes fondamentales en matière de gestion des actifs, d'évaluation des risques et de gouvernance. L'écart entre les meilleurs et les moins bons résultats est considérable (**+1,21 point**), ce qui indique un niveau de préparation inégal au sein du secteur. Les hôpitaux psychiatriques, en particulier, présentent les lacunes structurelles les plus importantes.

Les hôpitaux qui utilisent effectivement notre **bibliothèque SHIELD** affichent des progrès importants, avec une amélioration des scores de documentation de **2,31 à 3,40**. Cela confirme que les modèles standardisés et spécifiques au secteur accélèrent la maturité, à condition de disposer de suffisamment de personnel et de temps.

Pour répondre aux exigences d'avril 2026 et 2027, le secteur doit donner la priorité à l'accélération des efforts de documentation, à un soutien ciblé aux hôpitaux disposant de ressources insuffisantes, à une couverture complète des évaluations, à un engagement plus fort de la direction et à une préparation précoce aux niveaux de maturité plus stricts de 2027.

1.1.1. Situation du secteur

- 23,8 % des contrôles de base sont conformes aux normes
- Documentation : 1,57 en moyenne
- Mise en œuvre : 2,18 en moyenne
- Les hôpitaux psychiatriques accusent le plus grand retard

1.1.2. Différences critiques

- L'« identification » est le domaine le plus faible
- Écart important entre les établissements en tête et ceux en queue de peloton
- Important/essentiel (2027) bien en deçà de l'objectif

1.1.3. Ce qui fonctionne

- SHIELD Library améliore rapidement la documentation (2,31 → 3,40)

1.1.4. Priorités absolues

1. Accélérer la documentation
2. Soutenir les hôpitaux disposant de ressources insuffisantes
3. Compléter la couverture de l'évaluation
4. Garantir l'implication des dirigeants

5. Commencer tôt avant 2027

1.1.5. Mesures politiques

Élaborer un programme national de documentation, de suivi de la maturité, de soutien financier structurel pour le personnel ISMS (Information Security Management System) et de structures d'apprentissage entre pairs.

1.2. Maturité actuelle : ce que révèlent les chiffres

La maturité actuelle des hôpitaux belges reste bien en deçà du seuil requis pour avril 2026. Seuls **23,8 %** de tous les contrôles de base évalués satisfont au score de maturité obligatoire de **2,50**, tandis que **76,2 %** ne le satisfont pas. Cela signifie que, bien qu'il existe de nombreuses pratiques de sécurité dans les équipes opérationnelles, celles-ci ne sont pas systématiquement documentées, formalisées ou intégrées dans les structures de gouvernance.

Sur les 55 hôpitaux évalués, le score moyen de maturité est de **1,57 pour la documentation** et de **2,18 pour la mise en œuvre**, ce qui reflète un écart structurel entre « faire » et « prouver ».

Dans le présent rapport, le terme *« documentation »* est utilisé conformément à la terminologie CyberFundamentals telle que définie par le Centre pour la cybersécurité Belgique. Cependant, la portée pratique de la documentation va bien au-delà des artefacts écrits. Elle comprend également la définition, l'acceptation et le maintien des processus, des politiques organisationnelles, des structures de gouvernance et l'intégration cohérente de ces éléments dans la pratique quotidienne. Une documentation efficace nécessite donc non seulement la production de documents textuels, mais aussi leur ancrage dans la mentalité organisationnelle, soutenu par des outils appropriés, l'allocation de ressources et des cycles de maintenance récurrents. Il est essentiel de comprendre la documentation dans ce sens plus large pour interpréter correctement le fossé de maturité observé dans le secteur.

Cette lacune est visible dans l'ensemble du secteur et montre que les hôpitaux s'appuient souvent sur des processus informels, des pratiques non documentées et des connaissances spécifiques à chaque équipe. En conséquence, leur niveau de préparation en matière de cybersécurité ne peut être démontré, reproduit ou contrôlé.

Le manque de documentation augmente considérablement les risques liés à l'audit et à la conformité, ralentit les améliorations coordonnées à l'échelle du secteur et rend difficile la gestion durable de la cybersécurité. La documentation étant une condition préalable à la répétabilité, à la responsabilité et à la conformité, cette lacune est la principale raison pour laquelle la plupart des hôpitaux risquent actuellement de ne pas atteindre l'objectif de maturité fixé pour avril 2026.

Ces résultats confirment une tendance systémique : des équipes opérationnelles solides veillent à la mise en œuvre de nombreux contrôles dans la pratique, mais l'absence de cadres de documentation structurés, de personnel dédié et de temps alloué à l' empêche

les niveaux de maturité d'augmenter au rythme requis. Il est donc essentiel de remédier à ce manque de documentation afin d'accélérer la croissance de la maturité dans le secteur hospitalier belge.

Plusieurs hôpitaux en Belgique ont déjà obtenu la certification ISO/IEC 27001. Cela ne contredit pas les résultats CyberFundamentals présentés dans ce rapport. La norme ISO 27001 évalue si un système de gestion de la sécurité de l'information a été mis en place et est amélioré en permanence , tandis que CyberFundamentals utilise un modèle de notation strict, contrôle par contrôle, avec une granularité limitée. Un contrôle noté « 2 » peut en réalité être proche de « 3 », mais il sera tout de même signalé comme non conforme jusqu'à ce que toutes les exigences de maturité soient satisfaites.

En conséquence, les hôpitaux peuvent mettre en œuvre un SMSI fonctionnel et se conformer aux exigences de la norme ISO 27001, tout en obtenant des scores CyberFundamentals plus faibles, notamment en ce qui concerne l'exhaustivité de la documentation et la profondeur des preuves. Il est essentiel de clarifier cette distinction : CyberFundamentals ne remet pas en cause la maturité actuelle de la gouvernance, mais la méthode de notation limitée met en évidence les lacunes spécifiques qui doivent être comblées pour franchir les seuils d'avril 2026 et 2027.

1.3. Maturité par domaine CyFun : l'identification est le point faible

Parmi les cinq piliers CyFun**, l'identification est de loin le domaine le moins performant**, avec seulement **15,9 %** des hôpitaux atteignant le score de maturité requis de 2,50. Cela fait de l'identification la principale lacune structurelle du secteur. La figure 4 (la figure se trouve dans le rapport complet) illustre comment **l'identification** obtient systématiquement des scores inférieurs à ceux de la protection, de la détection, de la réponse et de la récupération dans tous les hôpitaux et toutes les régions.

Le domaine Identification comprend les éléments fondamentaux de la gestion de la cybersécurité, notamment **la gestion des actifs, les inventaires de logiciels et de données, l'évaluation des risques, les structures de gouvernance et la classification des données**. Ces composantes déterminent si un hôpital sait *quels actifs il possède, quels risques il court et qui est responsable* de leur gestion. Plusieurs contrôles dans ce domaine, tels que ID.AM-2.1 (inventaire des logiciels), ID.AM-3.1 (inventaire des informations) et ID.RA-5.1 (évaluation des risques), font partie des **contrôles les moins bien notés de l'ensemble de base**, avec des niveaux de conformité compris entre 9 % et 12 %.

Les faiblesses en matière d'identification ont des conséquences pour l'ensemble du secteur. Sans une vue d'ensemble complète des actifs et des risques, les hôpitaux ont du mal à établir des priorités en matière de mesures de sécurité, ne peuvent pas élaborer de plans d'investissement fiables et ont du mal à se conformer aux exigences en matière de documentation et d'audit. De plus, l'identification est une condition préalable à la mise en œuvre efficace des domaines Protection, Détection, Réponse et Récupération. Par exemple :

- sans inventaire précis des actifs, le patching et la gestion des vulnérabilités ne peuvent être pleinement mis en œuvre
- sans gouvernance et sans définition des rôles, les politiques ne peuvent être appliquées
- sans évaluations des risques, les hôpitaux ne peuvent pas établir de priorités ni justifier leurs besoins en ressources
- sans classification des données, la prévention des pertes de données et la segmentation du réseau deviennent incohérentes

L'identification étant la base sur laquelle reposent toutes les autres mesures de cybersécurité, son faible niveau de maturité constitue un **risque stratégique crucial** pour le secteur et un obstacle majeur à la mise en conformité en avril 2026 et 2027. Le renforcement de l'identification doit donc être une priorité absolue pour les hôpitaux et les décideurs politiques.

1.4. Comparaison régionale : la maturité varie selon les régions.

Les niveaux de maturité varient considérablement entre les trois régions, mais elles présentent toutes le même schéma structurel : les scores de mise en œuvre sont supérieurs aux scores de documentation. Les résultats montrent que la Flandre affiche systématiquement le niveau de maturité le plus élevé, suivie de la Wallonie, tandis que Bruxelles reste la plus éloignée de l'objectif fixé pour avril 2026.

Les résultats régionaux sont les suivants :

- **Bruxelles :** 1,29 pour la documentation, 1,99 pour la mise en œuvre
- **Wallonie :** 1,49 documentation, 2,04 mise en œuvre
- **Flandre :** 1,61 documentation, 2,22 mise en œuvre

Par rapport au score de maturité requis de 2,50, cela se traduit par des écarts de documentation de **1,21 à Bruxelles**, **1,01 en Wallonie** et **0,89 en Flandre**, et par des écarts de mise en œuvre de respectivement **0,51, 0,46 et 0,28**.

Ces différences reflètent divers facteurs sous-jacents. Les hôpitaux de Flandre disposent généralement d'équipes numériques et de sécurité plus importantes ou plus spécialisées, de structures de gouvernance plus matures et d'un niveau plus élevé de normalisation opérationnelle au sein des réseaux. Les hôpitaux bruxellois sont confrontés à des contraintes structurelles plus importantes, notamment des ressources limitées et une plus grande complexité organisationnelle, ce qui limite leur capacité à formaliser les processus et à tenir à jour la documentation. La Wallonie se situe entre ces deux profils, avec une capacité de mise en œuvre modérée mais des défis encore importants en matière de documentation.

La comparaison régionale confirme une tendance à l'échelle du secteur : la mise en œuvre progresse, mais la documentation reste le principal obstacle. Les résultats montrent également que certaines régions ont besoin de plus de soutien et d'aide pour rattraper leur retard en matière de maturité. Si ces différences régionales ne sont pas comblées, cela pourrait entraîner à l' e des niveaux inégaux de conformité et de résilience dans tout le pays.

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

1.5. Maturité par type d'hôpital.

La maturité des hôpitaux belges varie considérablement selon le type d'hôpital, ce qui reflète les différences en matière de capacités en personnel, de structures administratives et de disponibilité de fonctions spécifiques dans le domaine de la sécurité de l'information. Comme le montrent les figures 7 à 9 (Les figures se trouvent dans le rapport complet), les hôpitaux généraux et universitaires atteignent systématiquement un niveau de maturité plus élevé, tandis que les hôpitaux psychiatriques sont à la traîne dans tous les domaines, en particulier en matière de documentation.

Hôpitaux généraux

Les hôpitaux généraux obtiennent un score de **1,66 en matière de documentation** et de **2,23 en matière de mise en œuvre**. Leur maturité plus élevée s'explique en grande partie par la taille plus importante de leurs équipes informatiques et de sécurité, leurs processus de gouvernance structurés et leurs procédures administratives plus formalisées. Ces hôpitaux sont donc mieux placés pour atteindre le seuil de maturité fixé pour avril 2026, à condition que les efforts en matière de documentation soient intensifiés.

Hôpitaux psychiatriques

Les hôpitaux psychiatriques affichent une maturité nettement inférieure, avec un score de **1,30 pour la documentation** et de **2,04 pour la mise en œuvre**. Beaucoup de ces hôpitaux fonctionnent avec un personnel informatique très limité, peu ou pas de fonctions de sécurité spécialisées et des structures administratives moins formalisées. Il en résulte une documentation manquante ou incomplète et une capacité limitée à intégrer les processus. Sans un soutien ciblé, les hôpitaux psychiatriques sont les plus exposés au risque de ne pas atteindre les objectifs fixés pour 2026 et 2027.

Hôpitaux universitaires

Les hôpitaux universitaires obtiennent une note de **1,79 pour la documentation** et **de 2,23 pour la mise en œuvre**, ce qui leur permet de surpasser les autres types d'hôpitaux, notamment en termes de qualité de la documentation. Leur maturité plus avancée en matière de gouvernance, leurs équipes plus importantes et leurs processus plus standardisés contribuent à ces meilleures performances. Dans plusieurs domaines, notamment la réactivité et la résilience, ils constituent une référence pour le secteur.

Cette comparaison révèle une tendance structurelle claire : la maturité est directement liée aux effectifs disponibles, à la capacité de gouvernance et à l'expertise spécifique en matière de sécurité de l'information. Les hôpitaux généraux et universitaires bénéficient de structures de gouvernance et opérationnelles plus solides, ce qui leur permet d'atteindre plus rapidement la maturité. Les hôpitaux psychiatriques ont toutefois besoin d'un soutien sectoriel continu et ciblé pour surmonter leurs contraintes structurelles en matière de capacités. Ces différences doivent être prises en compte dans l'élaboration de la stratégie nationale, du financement et de la planification de la conformité.

1.6. Les leaders et les suiveurs

L'écart de maturité entre les hôpitaux les plus performants et les moins performants est considérable et met en évidence un fossé structurel au sein du secteur belge des soins de santé. Comme le montrent les figures 7, 10 et 11 (Les figures se trouvent dans le rapport complet), les hôpitaux les plus performants obtiennent un score de maturité total de 2,64, tandis que les moins performants n'obtiennent en moyenne que 1,43. Cette différence de 1,21 point reflète des écarts considérables en matière de gouvernance, de ressources et de capacité à formaliser les processus de cybersécurité.

Les leaders

Les cinq hôpitaux les plus performants, tous situés en Flandre, affichent une maturité élevée dans la plupart des domaines, soutenue par des structures de gouvernance bien développées, des ressources spécifiques pour la sécurité de l'information et des processus stables. Leurs scores en matière de documentation (**2,56**) et de mise en œuvre (**2,72**) montrent que la cybersécurité est à la fois formalisée et appliquée de manière cohérente. Ils excellent particulièrement dans les domaines de la communication, de la planification des interventions, de la surveillance de la sécurité et des processus de protection des informations. Ces organisations sont structurellement bien placées pour se conformer aux exigences d'avril 2026 ou pour continuer à s'y conformer.

Suiveurs

Les cinq hôpitaux ayant obtenu les scores les plus faibles – hôpitaux généraux et psychiatriques confondus – obtiennent une note moyenne **de 1,07 pour la documentation**, plusieurs catégories atteignant le niveau minimum de **1,00**, ce qui indique une documentation absente ou très incomplète. La maturité de la mise en œuvre reste également limitée, avec un score de **1,79**, et il existe des lacunes critiques dans la planification des interventions, la planification de la reprise et les améliorations. Ces hôpitaux fonctionnent généralement avec des effectifs limités, une gouvernance moins formelle et des fonctions de sécurité minimales, ce qui entrave leur capacité à formaliser les processus et à mettre en place des pratiques cohérentes.

Signification de l'écart

Cet écart de maturité confirme l'existence d'un **paysage de cybersécurité à deux vitesses** au sein du secteur belge des soins de santé. Sans un soutien ciblé, il est peu probable que les hôpitaux les moins performants, en particulier les établissements psychiatriques, atteignent les exigences de maturité pour 2026 ou 2027. Si cet écart n'est pas comblé, il en résultera une base de référence nationale incohérente en matière de cybersécurité, ce qui augmentera le risque systémique et compromettra la continuité opérationnelle dans l'ensemble du secteur.

1.7. Avantages de la bibliothèque SHIELD

La bibliothèque SHIELD (une bibliothèque open source librement accessible – **© 2025 Shield VZW – Licence CC BY-NC-SA 4.0**) s'est avérée être l'un des accélérateurs les plus efficaces pour améliorer la maturité de la documentation dans le secteur hospitalier belge. Comme le montrent les figures 12 et 13 (Les figures se trouvent dans le rapport complet), les hôpitaux qui ont mis en œuvre la bibliothèque ont réalisé une amélioration significative de la qualité de la documentation, avec une augmentation des scores moyens de documentation **de 2,31 à 3,40** en environ un an. Cette amélioration montre que des modèles structurés et spécifiques au secteur peuvent accélérer considérablement la progression vers la conformité aux CyberFundamentals.

L'impact de la bibliothèque est principalement déterminé par l'ensemble complet et normalisé de politiques, de processus, de procédures et de documents d'accompagnement, qui sont entièrement alignés sur la norme ISO/IEC 27001:2022 et CyberFundamentals 2023. Comme le matériel est accessible au public et adapté à l'environnement hospitalier, les établissements peuvent le mettre en œuvre immédiatement sans avoir à développer leur propre documentation. Cela réduit la charge de travail administratif, améliore la cohérence et permet à des équipes plus petites de fournir une documentation de meilleure qualité.

Cependant, la bibliothèque **n'**est **pas une solution toute faite**. Pour une utilisation efficace, il faut du personnel qualifié, du temps et un engagement local fort afin d'adapter les modèles, de les intégrer dans la pratique quotidienne et de les maintenir à jour. Certains hôpitaux ont connu une mise en œuvre plus lente, car la bibliothèque a placé la barre plus haut : à mesure que la documentation s'améliorait, les évaluations sont devenues plus approfondies et ont mis en évidence des lacunes dans la mise en œuvre des processus. Cela souligne l'importance de lier l'amélioration de la documentation à un soutien structuré à la mise en œuvre.

Dans l'ensemble, la bibliothèque SHIELD représente une **méthode évolutive et fondée sur des preuves** pour accroître la maturité dans l'ensemble du secteur. Avec un personnel suffisant et l'engagement de la direction, cette bibliothèque peut réduire considérablement le déficit de documentation et aider les hôpitaux à satisfaire aux exigences de maturité pour 2026 et 2027.

1.8. Priorités pour avril 2026 et 2027

Pour répondre aux exigences de base de CyberFundamentals d'avril 2026 et nous préparer aux contrôles plus stricts et essentiels de 2027, une action coordonnée à l'échelle du secteur est nécessaire. Les évaluations montrent clairement que le fossé actuel en matière de maturité ne peut être comblé sans un soutien ciblé, l'engagement de la direction et des efforts accélérés en matière de documentation. Les priorités suivantes constituent la base de la stratégie nationale d'amélioration requise.

Priorité 1 – accélérer la documentation grâce à la mise en place structurée de la bibliothèque SHIELD

La documentation reste le principal écart de maturité dans le secteur. L'introduction systématique de la bibliothèque SHIELD, combinée à un temps protégé et à une appropriation locale, peut rapidement améliorer les scores de documentation dans toutes les catégories d'hôpitaux. Cela est essentiel pour atteindre le seuil de maturité de base de 2,50 d'ici avril 2026.

Priorité 2 – Offrir un soutien ciblé aux hôpitaux disposant de ressources insuffisantes et aux hôpitaux psychiatriques

Les hôpitaux psychiatriques et les petits établissements sont confrontés à des contraintes structurelles en matière de ressources, ce qui rend improbable leur conformité indépendante. Un soutien sur mesure – via des centres d'expertise régionaux, des ressources de sécurité partagées ou un financement ciblé – sera nécessaire pour combler le fossé de maturité et éviter une politique à deux vitesses en matière de cybersécurité.

Priorité 3 – Achèvement de la couverture de l'évaluation dans l'ensemble du secteur

Plusieurs entités hospitalières n'ont pas encore été évaluées. L'achèvement du programme d'évaluation permettra de garantir une mesure cohérente de la maturité et de refléter l'ensemble des risques dans la planification nationale. Cela est nécessaire pour prendre des décisions politiques fondées sur des données probantes et améliorer le secteur de manière coordonnée.

Priorité 4 – Renforcer l'engagement de la direction et prévoir du temps

Les hôpitaux les mieux classés se distinguent par un engagement fort de la direction et un personnel ISMS dévoué. Les dirigeants doivent considérer la cybersécurité comme un domaine stratégique, réserver et allouer du temps aux activités de documentation et de gouvernance, et veiller à ce que les améliorations en matière de cybersécurité soient intégrées dans l'ensemble de l'organisation.

Priorité n° 5 – se préparer en temps utile aux exigences de maturité plus strictes de 2027

Les mesures clés importantes et essentielles, pour lesquelles un score minimum de 3,0 est requis, n'obtiennent actuellement qu'une moyenne **de 1,33 pour la documentation** et **de 1,90 pour la mise en œuvre**. Ces faibles valeurs de départ soulignent la nécessité d'une préparation précoce, d'une planification coordonnée des améliorations et d'une allocation des ressources à l'échelle du secteur. Attendre 2026 entraînerait une charge de conformité ingérable.

Ensemble, ces priorités soulignent la nécessité d'une approche structurée, soutenue par des ressources et appuyée au niveau central. Sans une accélération de la documentation, une aide ciblée pour les segments vulnérables et un engagement accru de la direction, une partie importante du secteur risque de ne pas satisfaire aux exigences des CyberFundamentals pour 2026 et 2027.

1.9. Recommandations politiques

Les conclusions pour toutes les catégories d'hôpitaux, toutes les régions et tous les domaines CyFun montrent clairement que sans mesures politiques coordonnées, la maturité du secteur ne s'améliorera pas au rythme requis. Afin d'aider les hôpitaux à se conformer aux exigences d'avril 2026 et 2027, les mesures politiques suivantes sont recommandées au niveau national et régional.

1. Mettre en place un programme de documentation et de gouvernance à l'échelle du secteur

Un cadre de documentation uniforme, basé sur la bibliothèque SHIELD, doit être officiellement adopté comme norme nationale. Ce programme doit aider les hôpitaux à mettre en œuvre des politiques, des processus et des structures de gouvernance cohérents, soutenus par des étapes, des modèles et des lignes directrices clairs.

2. Fournir un financement ciblé et un soutien structurel aux petits hôpitaux et aux hôpitaux psychiatriques

Les hôpitaux psychiatriques et les établissements disposant de ressources insuffisantes ont besoin d'un soutien financier et opérationnel spécifique pour renforcer leurs capacités en matière de SMSI, recruter ou partager du personnel spécialisé et mettre en place des processus de documentation. Sans un tel soutien, des lacunes en matière de conformité persisteront et le secteur se fragmentera en différents niveaux de maturité.

Bien que tous les hôpitaux aient besoin d'un financement structurel, les établissements de petite taille et les hôpitaux psychiatriques ont besoin d'un soutien supplémentaire et différencié. En raison de leurs capacités limitées en termes de personnel, de leurs contraintes organisationnelles et de l'absence de fonctions de sécurité spécifiques, il est

irréaliste d'attendre d'eux qu'ils atteignent le niveau de maturité requis sans aide ciblée. Ces organisations doivent faire face à une charge disproportionnée par rapport à leurs ressources disponibles et restent donc un groupe prioritaire pour un soutien financier et opérationnel renforcé dans le cadre de la stratégie nationale.

Dans la pratique, cependant, le manque de financement structurel ne se limite pas aux petits hôpitaux ou aux hôpitaux psychiatriques. Pour de nombreux hôpitaux généraux, l'insuffisance du budget alloué reste le principal obstacle à l'atteinte du niveau de maturité requis en matière de processus de documentation et de gouvernance. L'octroi de ressources financières supplémentaires à *tous* les hôpitaux leur permettrait de recruter du personnel spécialisé à temps plein, tel qu'un responsable de la documentation ou de la conformité, ce qui est essentiel pour parvenir à des améliorations durables.

En outre, il serait utile, pour les évaluations futures, de vérifier si chaque hôpital a officiellement désigné une personne ou une équipe responsable des tâches de documentation et de conformité. Cela pourrait servir de critère supplémentaire dans les prochains cycles d'évaluation et contribuerait à renforcer la transparence et la responsabilité dans les structures de gouvernance.

3. Mettre en place un système national de suivi de la maturité avec des mises à jour trimestrielles

Un tableau de bord centralisé doit collecter les scores de maturité, mettre en évidence les lacunes et suivre les progrès réalisés dans tous les hôpitaux. Des mises à jour trimestrielles permettent une planification fondée sur des données probantes, une identification précoce des stagnations et des rapports transparents aux organes de gouvernance.

4. Réaliser des évaluations dans toutes les entités afin de garantir une couverture nationale complète

Tous les hôpitaux et établissements de soins concernés doivent être évalués selon la méthodologie SHIELD standard. Une couverture étendue garantit que la planification de la maturité reflète l'ensemble du paysage des risques et évite les angles morts dans la stratégie nationale de cybersécurité.

5. Promouvoir l'apprentissage structuré entre pairs entre les hôpitaux performants et ceux qui le sont moins

Les hôpitaux très performants font systématiquement preuve de pratiques favorisant la maturité, telles qu'une forte coordination de la gouvernance, des processus de documentation robustes et un personnel dédié à la cybersécurité. Un modèle structuré d'apprentissage entre pairs – via des groupes de travail régionaux, des ressources

partagées ou des ateliers thématiques – peut accélérer la croissance de la maturité dans l'ensemble du secteur.

Ces recommandations politiques visent à créer une approche coordonnée, cohérente et équitable de la cybermaturité dans les hôpitaux belges. Leur mise en œuvre contribuera à combler le déficit de documentation, à soutenir les établissements vulnérables, à améliorer la transparence et à garantir que tous les hôpitaux progressent vers les exigences CyberFundamentals d'avril 2026 et 2027.

1.10. Conclusion

Les évaluations pour 2025 montrent que le secteur hospitalier belge progresse en matière de maturité en matière de cybersécurité, mais pas au rythme nécessaire pour atteindre les seuils CyberFundamentals d'avril 2026 et 2027. Bien que la mise en œuvre progresse dans la plupart des domaines, **la documentation reste le principal obstacle**, avec des lacunes persistantes en matière de gouvernance, de gestion des actifs et d'évaluation des risques.

Les hôpitaux généraux et universitaires affichent une évolution plus forte en matière de maturité, soutenue par des équipes plus importantes et des structures de gouvernance plus formelles. Les hôpitaux psychiatriques sont toutefois confrontés à des contraintes structurelles qui, sans aide ciblée, les exposent à un risque élevé de non-conformité. L'écart considérable entre les établissements les plus performants et les moins performants confirme **l'existence d'une évolution à deux vitesses**, à laquelle il convient de remédier afin de maintenir une norme nationale de base cohérente en matière de cyber-résilience.

La bibliothèque SHIELD s'est avérée être un accélérateur efficace pour la maturité de la documentation, mais son succès dépend de la qualification du personnel, du temps qui y est consacré et d'un engagement fort de la direction. Pour combler le fossé en matière de maturité, il est essentiel d'étendre son utilisation, de renforcer les capacités de gouvernance et d'apporter un soutien systématique aux hôpitaux disposant de ressources insuffisantes.

Pour répondre aux exigences de base pour 2026 et nous préparer aux contrôles plus stricts et essentiels de 2027, **une action coordonnée au niveau national** est nécessaire, notamment une gouvernance structurée, un financement ciblé, une couverture d'évaluation étendue et un suivi régulier de la maturité. Grâce à des investissements ciblés, à un leadership exécutif fort et à une utilisation cohérente de la méthodologie SHIELD, le secteur peut atteindre un niveau stable et durable de maturité en matière de cybersécurité qui protège les soins de santé, la sécurité des patients et la résilience de la société.