



SHIELD vzw

State of cybersecurity in Belgian hospitals

Sector report on CyberFundamentals (CyFun)
2023 basic assessments

Wim Bijmens, David Saray
19/11/2025

Generative AI Statement: In the preparation of this document, GenAI LLM was used by SHIELD vzw as a writing and editing tool to improve the clarity, grammar, and consistency of the text. The tool was employed solely for linguistic support and was not used to generate, analyze, or interpret any substantive, technical, or other content. All substantive decisions, analyses, designs, conclusions, and any visualizations included in this document are the responsibility of SHIELD vzw.

1. Executive Summary

This report provides a clear and actionable overview of the CyberFundamentals 2023 Basic maturity of Belgian hospitals. The analysis shows that sector-wide maturity is improving, but remains significantly below the required threshold for April 2026. Only **23.8%** of the Basic controls meet the required maturity level of **2.50**, with documentation (average **1.57**) lagging far behind implementation (**2.18**).

The domain requiring the most attention is **Identify**. It clearly reflects foundational gaps in asset management, risk assessment and governance. The gap between the best and worst performers is substantial (**+1.21 points**), indicating unequal readiness across the sector. Psychiatric hospitals in particular show the largest structural deficits.

Hospitals that are actually using the **SHIELD Library** demonstrate strong progress, with documentation scores improving from **2.31 to 3.40**, confirming that standardized and sector-specific templates accelerate maturity growth—keeping in mind that sufficient staff and time must be made available.

To reach the April 2026 and 2027 requirements, the sector must prioritize accelerated documentation efforts, targeted support for under-resourced hospitals, full assessment coverage, stronger leadership involvement, and early preparation for the stricter 2027 maturity levels.

1.1.1. sector status

- 23.8% of basic controls compliant
- documentation: 1.57 average
- implementation: 2.18 average
- psychiatric hospitals have the largest gap

1.1.2. critical gaps

- identify domain weakest
- major gap between top and bottom institutions
- important/essential (2027) far below target

1.1.3. what works

- shield library improves documentation rapidly (2.31 → 3.40)

1.1.4. top priorities

1. accelerate documentation
2. support under-resourced hospitals
3. complete assessment coverage
4. ensure leadership involvement
5. start early for 2027

1.1.5. policy actions

Develop a national documentation program, maturity monitoring, structural financial support for ISMS (Information Security Management System) staff, and peer-learning structures.

1.2. Current maturity: what the numbers show

The current maturity level of Belgian hospitals remains well below the required threshold for April 2026. Only **23.8%** of all assessed Basic controls meet the mandatory maturity score of **2.50**, while **76.2%** fall short. This means that although many security practices exist in operational teams, they are not consistently documented, formalized, or embedded in governance structures.

Across the 55 hospitals assessed, the average maturity score is **1.57 for documentation** and **2.18 for implementation**, reflecting a structural gap between “doing” and “proving.”

In this report, the term *documentation* is used in line with the CyberFundamentals terminology defined by the CCB. However, the practical scope of documentation extends far beyond written artefacts. It also encompasses the definition, adoption and maintenance of processes, organisational policies, governance structures, and the consistent integration of these elements into day-to-day practice. Effective documentation therefore requires not only producing textual materials, but also embedding them into the organisational mindset, supported by appropriate tooling, resource allocation and recurring maintenance cycles. Understanding documentation in this broader sense is essential for correctly interpreting the maturity gap observed across the sector.

This gap is visible throughout the sector and indicates that hospitals often rely on informal processes, undocumented practices, and team-specific knowledge. As a result, their cybersecurity readiness cannot be demonstrated, reproduced, or audited.

The lack of documentation significantly increases audit and compliance risks, slowing down coordinated sector-wide improvements, and making sustained cybersecurity governance difficult. Because documentation is a prerequisite for repeatability, accountability and compliance, this gap is the main reason why most hospitals currently risk missing the April 2026 maturity target.

These results confirm a systemic pattern: strong operational teams ensure many controls are implemented in practice, but the absence of structured documentation frameworks, dedicated personnel and protected time keeps maturity levels from increasing at the required pace. Addressing this documentation deficit is therefore the single most important driver for accelerating maturity across the Belgian hospital sector.

Several hospitals in Belgium already hold an ISO/IEC 27001 certification. This does not contradict the CyberFundamentals results presented in this report. ISO 27001 evaluates

whether an Information Security Management System is established and continuously improved, while CyberFundamentals applies a strict, control-by-control scoring model with limited granularity. A control scored as “2” may in practice be close to “3”, yet it is still reported as non-compliant until the full maturity requirements are met.

As a result, hospitals can operate a functioning ISMS and meet ISO 27001 requirements while still receiving lower CyberFundamentals scores, particularly in documentation completeness and evidence depth. Clarifying this distinction is essential: CyberFundamentals does not invalidate existing governance maturity, but its narrow scoring method highlights the specific gaps that must be closed to reach the April 2026 and 2027 thresholds.

1.3. Maturity per CyFun domain: identify is the weakest

Across the five CyFun pillars, **Identify is by far the weakest-performing domain**, with only **15.9%** of hospitals reaching the required maturity score of 2.50. This makes Identify the most significant structural gap in the sector. Figure 4 illustrates how **Identify** consistently scores below Protect, Detect, Respond, and Recover across all hospitals and regions.

The Identify domain covers the foundational elements of cybersecurity governance, including **asset management, software and data inventories, risk assessment, governance structures and data classification**. These components determine whether a hospital knows *what assets it owns, what risks it faces and who is responsible* for managing them. Several controls within this domain—such as ID.AM-2.1 (software inventory), ID.AM-3.1 (information inventory), and ID.RA-5.1 (risk assessment)—are among the **lowest-scoring controls in the entire Basic set**, with compliance levels between 9% and 12%.

Weaknesses in Identify have sector-wide consequences. Without a complete overview of assets and risks, hospitals struggle to prioritise security measures, cannot reliably plan investments, and face challenges in meeting documentation and audit requirements. Additionally, Identify is a prerequisite for effective execution of the Protect, Detect, Respond, and Recover domains. For example:

- without accurate asset inventories, patching and vulnerability management cannot be fully executed
- without governance and role definitions, policies cannot be maintained
- without risk assessments, hospitals cannot set priorities or justify resource needs
- without data classification, data loss prevention and network segmentation become inconsistent

Because Identify is the foundation on which all other cybersecurity measures depend, its weak maturity is a **critical strategic risk** for the sector and a major barrier to achieving

April 2026 and 2027 compliance. Strengthening Identify should therefore be a top priority for hospitals and policymakers.

1.4. Regional comparison: maturity differs across regions.

Across the three regions, maturity levels differ noticeably, yet all show the same structural pattern: implementation scores are higher than documentation scores. The results show that Flanders consistently reports the highest maturity, followed by Wallonia, while Brussels remains the furthest from the April 2026 target.

Regional results are as follows:

- **Brussels:** 1.29 documentation, 1.99 implementation
- **Wallonia:** 1.49 documentation, 2.04 implementation
- **Flanders:** 1.61 documentation, 2.22 implementation

Measured against the required maturity score of 2.50, this translates into documentation gaps of **1.21 in Brussels**, **1.01 in Wallonia** and **0.89 in Flanders**, and implementation gaps of **0.51**, **0.46** and **0.28** respectively.

These differences reflect several underlying factors. Hospitals in Flanders generally have larger or more specialised digital and security teams, more mature governance structures and a higher level of operational standardisation across networks. Hospitals in Brussels face greater structural constraints, including resource limitations and higher organisational complexity, which limits their capacity to formalise processes and maintain documentation. Wallonia sits between these two profiles, with moderate implementation capability but still significant documentation challenges.

The regional comparison confirms a sector-wide pattern: implementation is progressing, but documentation remains the main barrier. The results also highlight that some regions will require stronger support and assistance to close their maturity gaps. If unaddressed, these regional disparities may lead to unequal compliance readiness and inconsistent resilience levels across the country.

1.5. Maturity by hospital type.

The maturity of Belgian hospitals varies significantly by hospital type, reflecting differences in staffing capacity, governance structures and the availability of dedicated information-security roles. As shown in figures 7–9, general hospitals and university hospitals consistently achieve higher maturity, while psychiatric hospitals lag behind across all domains, particularly in documentation.

General hospitals

General hospitals score **1.66 on documentation** and **2.23 on implementation**. Their higher maturity is largely explained by larger ICT and security teams, structured governance processes and more formalised administrative procedures. These hospitals are therefore better positioned to reach the April 2026 maturity threshold, provided documentation efforts accelerate.

Psychiatric hospitals

Psychiatric hospitals show considerably lower maturity, with **1.30 on documentation** and **2.04 on implementation**. Many operate with very limited ICT staffing, few or no dedicated security roles and less formalised governance structures. This results in missing or incomplete documentation and limited capacity to embed processes. Without targeted support, psychiatric hospitals are at the highest risk of failing to meet the 2026 and 2027 Targets.

University hospitals

University hospitals score **1.79 on documentation** and **2.23 on implementation**, outperforming other hospital types particularly in documentation quality. Their broader governance maturity, larger teams and more standardised processes contribute to this higher performance. In several domains — especially respond and recover — they set a benchmark for the sector.

This comparison shows a clear structural trend: maturity correlates directly with available staffing, governance capability and dedicated information-security expertise. General and university hospitals benefit from stronger governance and operational structures, enabling faster growth in maturity. Psychiatric hospitals, however, require sustained and targeted sectoral support to overcome structural capacity limitations. These differences must be taken into account when shaping national strategy, funding and compliance planning.

1.6. Top performers vs underachievers

The maturity gap between the highest- and lowest-performing hospitals is substantial and highlights a structural divide within the Belgian healthcare sector. As shown in figures 7, 10 and 11, the top-performing hospitals achieve an overall maturity score of 2.64, while the lowest-performing hospitals average only 1.43. This difference of 1.21 points reflects significant disparities in governance, resources and the ability to formalise cybersecurity processes.

Top performers

The top five hospitals, all located in Flanders, demonstrate strong maturity across most domains, supported by well-developed governance structures, dedicated information-security resources and stable processes. Their documentation scores (**2.56**) and implementation scores (**2.72**) show that cybersecurity is both formalised and consistently executed. They excel particularly in communications, response planning, security monitoring and information-protection processes. These organisations are structurally well-positioned to reach or maintain compliance with the April 2026 requirements.

Underachievers

The five lowest-performing hospitals—consisting of both general and psychiatric hospitals—average **1.07 for documentation**, with several categories scoring at the minimum level of **1.00**, indicating absent or highly incomplete documentation. Implementation maturity remains limited as well, with a score of **1.79**, and critical gaps in response planning, recovery planning and improvements. These hospitals typically operate with limited staffing capacity, less formal governance and minimal dedicated security roles, which hinders their ability to formalise processes and embed consistent practices.

Significance of the gap

This maturity gap confirms a **two-speed cybersecurity landscape** within Belgian healthcare. Without targeted support, the lowest-performing hospitals—especially psychiatric institutions—are unlikely to reach the 2026 or 2027 maturity requirements. Not addressing this gap will result in a inconsistent national baseline for cybersecurity, increasing systemic risk and will jeopardize operational continuity across the entire sector.

1.7. SHIELD Library Benefits

The SHIELD Library (a freely available opensource Library - © 2025 Shield VZW – License **CC BY-NC-SA 4.0**) has proven to be one of the most effective accelerators for improving documentation maturity across the Belgian hospital sector. As shown in figures 12 and 13, hospitals that adopted the library achieved a substantial increase in documentation quality, with average documentation scores rising from **2.31 to 3.40** within approximately one year. This improvement demonstrates that structured, sector-specific templates can significantly accelerate progress toward CyberFundamentals compliance.

The library's impact is primarily driven by its comprehensive and standardised set of policies, processes, procedures and supporting documents, fully aligned with ISO/IEC 27001:2022 and CyberFundamentals 2023. Because the materials are openly available and tailored to the hospital environment, institutions can directly implement them without needing to develop documentation from scratch. This reduces administrative workload, improves consistency and enables smaller teams to deliver higher-quality documentation.

However, the library is **not a plug-and-play solution**. Effective use requires qualified staff, time and strong local ownership to adapt the templates, embed them in daily practice and keep them up to date. Some hospitals have experienced slower implementation progress because the library raised the maturity bar: as documentation improved, assessments became more thorough and revealing gaps in process execution. This underlines the importance of pairing documentation uplift with structured implementation support.

Overall, the SHIELD Library represents a **scalable, evidence-based method** to raise maturity across the sector. With sufficient staffing and governance commitment, it can significantly narrow the documentation gap and help hospitals move toward the 2026 and 2027 maturity requirements.

1.8. Priorities for April 2026 and 2027

Meeting the April 2026 CyberFundamentals Basic requirements, and preparing for the more stringent Important and Essential controls in 2027, will require coordinated sector-wide action. The assessments clearly show that the current maturity gap cannot be closed without targeted support, governance commitment and accelerated documentation efforts. The following priorities form the basis of the required national improvement strategy.

priority 1 – accelerate documentation through structured SHIELD Library adoption

Documentation remains the sector's largest maturity gap. Systematic adoption of the SHIELD Library, combined with protected time and local ownership, can rapidly raise documentation scores across all hospital categories. This is essential for reaching the Basic maturity threshold of 2.50 by April 2026.

priority 2 – provide targeted support to under-resourced and psychiatric hospitals

Psychiatric hospitals and smaller institutions face structural resource limitations that make independent compliance unlikely. Tailored support—through regional expertise centers, shared security resources or targeted funding—will be required to close the maturity gap and prevent a two-speed cybersecurity landscape.

priority 3 – complete assessment coverage across the sector

Several hospital entities have not yet been assessed. Completing the assessment programme ensures that maturity is measured consistently and that national planning reflects the full risk landscape. This is necessary for evidence-based policy decisions and coordinated sector improvement.

priority 4 – strengthen leadership involvement and ensure protected time

Hospitals that score highest demonstrate strong leadership engagement and dedicated ISMS staffing. Executives must place cybersecurity as a strategic domain, allocate protected time for documentation and governance activities and ensure that cybersecurity improvements are embedded within the whole of the organisation.

priority 5 – prepare early for the stricter 2027 maturity requirements

The Important and Essential Key Measures, which require a minimum score of 3.0, currently average only **1.33 for documentation** and **1.90 for implementation**. These low baselines underscore the need for early preparation, coordinated improvement planning and sector-wide resource allocation. Waiting until 2026 would create an unmanageable compliance burden.

Collectively, these priorities emphasise the need for a structured, resourced and centrally supported approach. Without accelerated documentation, targeted assistance for vulnerable segments and strengthened leadership commitment, a significant portion of the sector risks failing to meet both the 2026 and 2027 CyberFundamentals requirements.

1.9. Policy recommendations

The findings across all hospital categories, regions and CyFun domains make clear that sector-wide maturity will not improve at the required pace without coordinated policy intervention. To support hospitals in reaching the April 2026 and 2027 requirements, the following policy actions are recommended at national and regional level.

1. Establish a sector-wide documentation and governance programme

A unified documentation framework, built around the SHIELD Library, should be formally adopted as the national standard. This programme should guide hospitals in implementing consistent policies, processes and governance structures, supported by clear maturity milestones, templates and guidance.

2. Provide targeted funding and structural support to smaller and psychiatric hospitals

Psychiatric hospitals and under-resourced institutions require dedicated financial and operational support to build ISMS capacity, hire or share specialised personnel and embed documentation processes. Without such support, compliance gaps will persist and the sector will fragment into varying levels of maturity.

While structural funding is needed across all hospitals, smaller institutions and psychiatric hospitals require additional and differentiated support. Their limited staffing capacity, organisational constraints and absence of dedicated security roles make it unrealistic to expect them to reach the required maturity without targeted assistance. These organisations face a disproportionate burden relative to their available resources, and therefore remain a priority group for reinforced financial and operational support within the national strategy.

In practice, however, the lack of structural funding is not limited to smaller or psychiatric hospitals. For many general hospitals, insufficient allocated budget remains the primary barrier to bringing documentation and governance processes up to the required maturity level. Allocate additional financial resources for *all* hospitals would enable them to recruit dedicated full-time staff, such as a documentation or compliance officer, which is essential for achieving sustainable improvements.

Furthermore, it would be valuable for future assessments to verify that each hospital has formally assigned a responsible person or team for documentation and compliance tasks. This could serve as an additional measurement point in upcoming evaluation cycles and would help strengthen transparency and accountability in governance structures.

3. Implement a national maturity monitoring system with quarterly updates

A centralised dashboard should collect maturity scores, highlight gaps and track progress across all hospitals. Quarterly updates will enable evidence-based planning, early identification of stagnation and transparent reporting to governing bodies.

4. Complete assessments across all entities to ensure full national coverage

All hospitals and relevant care entities must be assessed using the standard SHIELD methodology. Comprehensive coverage ensures that maturity planning reflects the full risk landscape and prevents blind spots in national cybersecurity strategy.

5. Promote structured peer-learning between high- and low-performing hospitals

Top-performing hospitals consistently demonstrate maturity-driving practices, such as strong governance alignment, robust documentation processes and dedicated cybersecurity staffing. A structured peer-learning model—through regional working groups, shared resources or thematic workshops—can accelerate maturity growth across the sector.

These policy recommendations aim to create a coordinated, consistent and equitable approach to cybersecurity maturity across Belgian hospitals. Implementing them will help close the documentation gap, support vulnerable institutions, improve transparency and ensure that all hospitals progress toward the April 2026 and 2027 CyberFundamentals requirements.

1.10. Conclusion

The 2025 assessments show that the Belgian hospital sector is making progress in cybersecurity maturity, but not at the pace required to meet the April 2026 and 2027 CyberFundamentals thresholds. While implementation is advancing across most domains, **documentation remains the primary barrier**, with persistent gaps in governance, asset management and risk assessment.

General and university hospitals demonstrate stronger maturity trajectories, supported by larger teams and more formal governance structures. Psychiatric hospitals, however, face structural constraints that place them at high risk of non-compliance without targeted assistance. The significant gap between top and bottom performers confirms a **two-speed maturity development** that must be addressed to maintain a consistent national baseline of cyber resilience.

The SHIELD Library has proven to be an effective accelerator for documentation maturity, but its success depends on qualified staff, protected time and strong leadership commitment. Expanding its adoption, strengthening governance capacity and ensuring systematic support for under-resourced hospitals will be essential to closing the maturity gap.

Achieving the 2026 Basic requirements, and preparing for the more demanding Important and Essential controls in 2027, will require **coordinated action at national level**, including structured governance, targeted financing, comprehensive assessment coverage and regular maturity monitoring. With focused investment, strong executive leadership and consistent use of the SHIELD methodology, the sector can reach a stable and sustainable level of cybersecurity maturity that protects healthcare operations, patient safety and societal resilience.

Table of Contents

1.	Executive Summary	2
1.1.1.	sector status	2
1.1.2.	critical gaps	2
1.1.3.	what works	2
1.1.4.	top priorities	2
1.1.5.	policy actions	3
1.2.	Current maturity: what the numbers show	3
1.3.	Maturity per CyFun domain: identify is the weakest	4
1.4.	Regional comparison: maturity differs across regions.	5
1.5.	Maturity by hospital type.	6
1.6.	Top performers vs underachievers	7
1.7.	SHIELD Library Benefits	8
1.8.	Priorities for April 2026 and 2027	9
1.9.	Policy recommendations	10
1.10.	Conclusion	12
	Table of Figures	15
1.	Introduction	16
1.1.	The SHIELD Baseline Assessment	17
2.	Average Assessment Score Basic	18
2.1.1.	Overview with Important & Essential Key Measures	21
2.2.	Hospital Category Overview	22
2.2.1.	Documentation	22
2.2.2.	Implementation	22
2.2.3.	Conclusion	23
2.2.4.	Score by General Hospital:	23
2.2.5.	Score by Psychiatric Hospital:	24
2.2.6.	University Hospital scoring Overview	24
2.3.	Best in class	26
2.3.1.	Top 4 performers	26
2.3.2.	Bottom 5 performers	29
2.3.3.	Headline Gap - Top & Bottom 5	31

2.4.	The Value of the SHIELD Library	31
2.4.1.	How the SHIELD Library Boosted Documentation.....	33
2.4.2.	A Fast-Tracking ISMS Documentation	35
3.	Conclusion.....	36
4.	Appendix	38
4.1.	CyFun 2023 Basic Categories Mappings	38
4.2.	CyFun 2023 Key Measure Essential and Important Mappings	41
4.3.	Hospital Name per Categories	43
4.4.	SHIELD Baseline Assessment 50 Controls Overview	46

Table of Figures

Figure 1 Compliancy Status for Basic	17
Figure 2 Dot Chart Basic Score	19
Figure 3 Overview Basic.....	20
Figure 4 Dot Chart Important & Essential Key Measures.....	21
Figure 5 Compliancy Status for Important & Essential Key Measures.....	22
Figure 6 Average Score by General Hospital	23
Figure 7 Average Score by Psychiatric Hospital.....	24
Figure 8 Average by University Hospital	25
Figure 9 Top Performer Scoring Categories.....	28
Figure 10 Bottom Performer Scoring Categories	30
Figure 11 SHIELD Library Benefits Dots Chart.....	33
Figure 12 SHIELD Library Benefits Bars Chart Difference	33

1. Introduction

This report provides an overview of the CyberFundamentals assessments conducted across general, psychiatric and university hospitals as of 31 October 2025, covering a total of **55 completed assessments**. It summarises the current maturity status in relation to the April 2026 requirement, which mandates an average maturity score of **2.50** for all **34 Basic controls**. Within this Basic level, the **13 Key Measures** also require a minimum score of 2.50, while the remaining Basic controls do not have a category-specific threshold.

Maturity level thresholds			
	BASIC	IMPORTANT	ESSENTIAL
Each Key Measure Maturity level	$\geq 2,5/5$	$\geq 3/5$	$\geq 3/5$
Each Category Maturity level	n/a	n/a	$\geq 3/5$
Total Maturity level (average)	$\geq 2,5/5$	$\geq 3/5$	$\geq 3,5/5$

Figure 1 presents the CyFun maturity model.

To achieve the Basic requirements, hospitals must reach an average score of ≥ 2.50 across the full Basic control set. Across **1,904 assessed controls** (34 controls $\times$ 56 hospitals), only **453 controls (23.8%)** meet this threshold, while **1,451 controls (76.2%)** fall below it. Compliance varies considerably by control.

The **highest-scoring controls** include:

- PR.AC-1.1 (48%, 27/56)
- PR.AC-5.1 (39%, 22/56)
- DE.CM-4.1 (34%, 19/56)
- Several others cluster around 32%, including PR.AC-2.1, PR.AC-3.2, PR.AC-4.4, PR.AC-5.2 and PR.IP-4.1.

The **lowest-scoring controls** include:

- PR.PT-1.1 (9%, 5/56)
- DE.AE-3.1 (11%, 6/56)
- ID.AM-3.1 (11%, 6/56)
- ID.RA-5.1 (11%, 6/56)
- ID.AM-2.1 and ID.AM-5.1 at 12.5% (7/56).

These results confirm that weaknesses are concentrated in asset management and risk assessment.

When grouped by CyFun function, compliance rates are:

- **Protect:** 29.1% (highest)
- **Detect:** 22.3%
- **Recover:** 21.4%
- **Respond:** 20.2%
- **Identify:** 15.9% (lowest)

Notably, **no single control** is currently met by the majority of hospitals ($\geq 50\%$), confirming that maturity gaps are present across all domains. Figure 2 provides an overview of the compliance status of all 1,904 assessed controls.

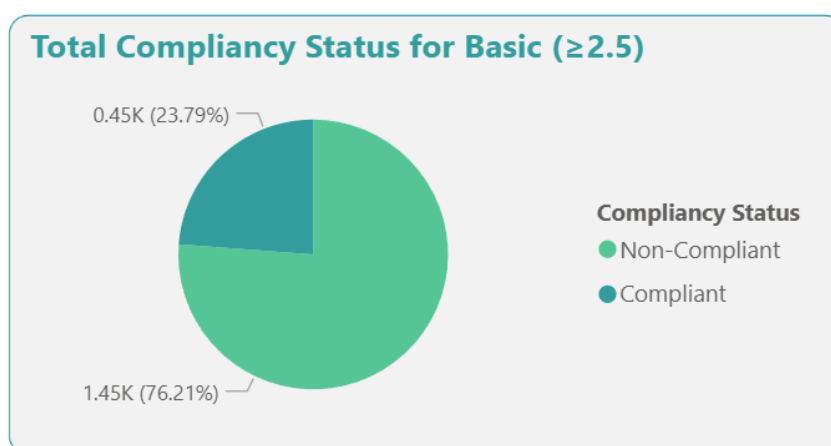


Figure 1 Compliancy Status for Basic

1.1. The SHIELD Baseline Assessment

Since June 2024, CyberFundamentals 2023 assessments have been conducted across Belgian hospitals, starting in Flanders and rapidly expanding to Brussels and Wallonia. The baseline SHIELD assessment currently evaluates **50 controls**—covering all Basic controls and Key Measures—providing a detailed view of both documentation and implementation maturity. Based on these 50 controls¹, the average maturity scores are **1.50 for documentation** and **2.09 for implementation**, confirming that documentation remains the primary gap across the sector.

At the time of reporting, **55 assessments** have been completed, **6 are ongoing**, and **18 additional assessments** are planned for late 2025 and early 2026². Several hospitals and

¹ An Overview of the 50 Controls is available in the [Appendix](#).

² The list of the assessment status is available in the [Appendix](#).

specific sub-entities within hospital networks—such as care hospitals and specialised units—have not yet been assessed³. These remaining entities will be included in subsequent phases to ensure complete national coverage.

Each assessment consists of structured interviews followed by a detailed maturity report for the hospital. This report includes:

- the hospital's documentation and implementation scores
- benchmarking against other assessed hospitals
- control-by-control recommendations to improve maturity

This approach provides hospitals with clear, actionable guidance to raise their maturity levels and ensures consistent evaluation across the sector.

2. Average Assessment Score Basic

The average Basic maturity scores for documentation and implementation across the three regions are presented below. These results provide an overview of how hospitals in Brussels, Flanders and Wallonia currently perform relative to the April 2026 maturity requirement of **2.50**.

Average scores across the three regions

- **1.57 documentation**
- **2.18 implementation**

Scores per region

- **Brussels:** 1.29 documentation, 1.99 implementation
- **Flanders:** 1.61 documentation, 2.22 implementation
- **Wallonia:** 1.49 documentation, 2.04 implementation

Across all regions, **implementation consistently outperforms documentation**, with a combined implementation score of 2.18 versus 1.57 for documentation—a structural gap of **0.61 points**. Compared to the required maturity score of 2.50, this corresponds to an average shortfall of **0.93** for documentation and **0.32** for implementation.

Regionally, **Brussels** shows the lowest maturity, with a documentation gap of **1.21** (1.29 → 2.50) and an implementation gap of **0.51** (1.99 → 2.50). **Flanders** is closest to the 2026 target, with

³ A non-exhaustive list of hospital categories is available in the [Appendix](#).

gaps of **0.89** (documentation) and **0.28** (implementation). **Wallonia** sits between both regions, with gaps of **1.01** and **0.46** respectively.

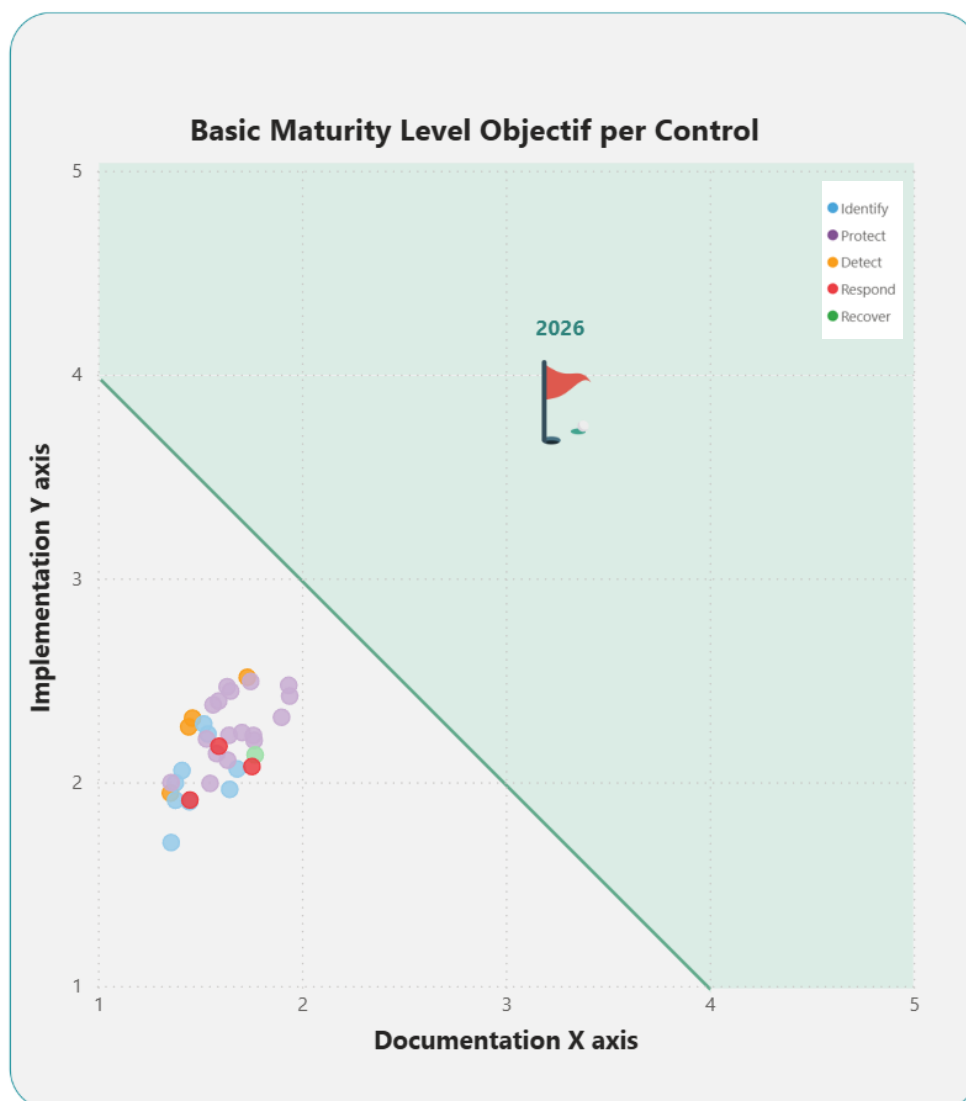


Figure 2 Dot Chart Basic Score

The dot chart above shows that most implementation scores cluster between **2.0 and 2.5**, while documentation scores fall between **1.3 and 1.8**. The green horizontal line marks the required **2.50** maturity level for April 2026. The goal is for all data points to move above this threshold, indicating a more consistent and resilient security baseline across all regions.

These results highlight a consistent national pattern: while operational execution of controls is progressing, **documentation remains the primary barrier** to achieving Basic maturity, with significant variation between regions. Strengthening documentation processes will therefore be essential to closing the maturity gap before 2026.

Average Basic score all hospitals categories combined:

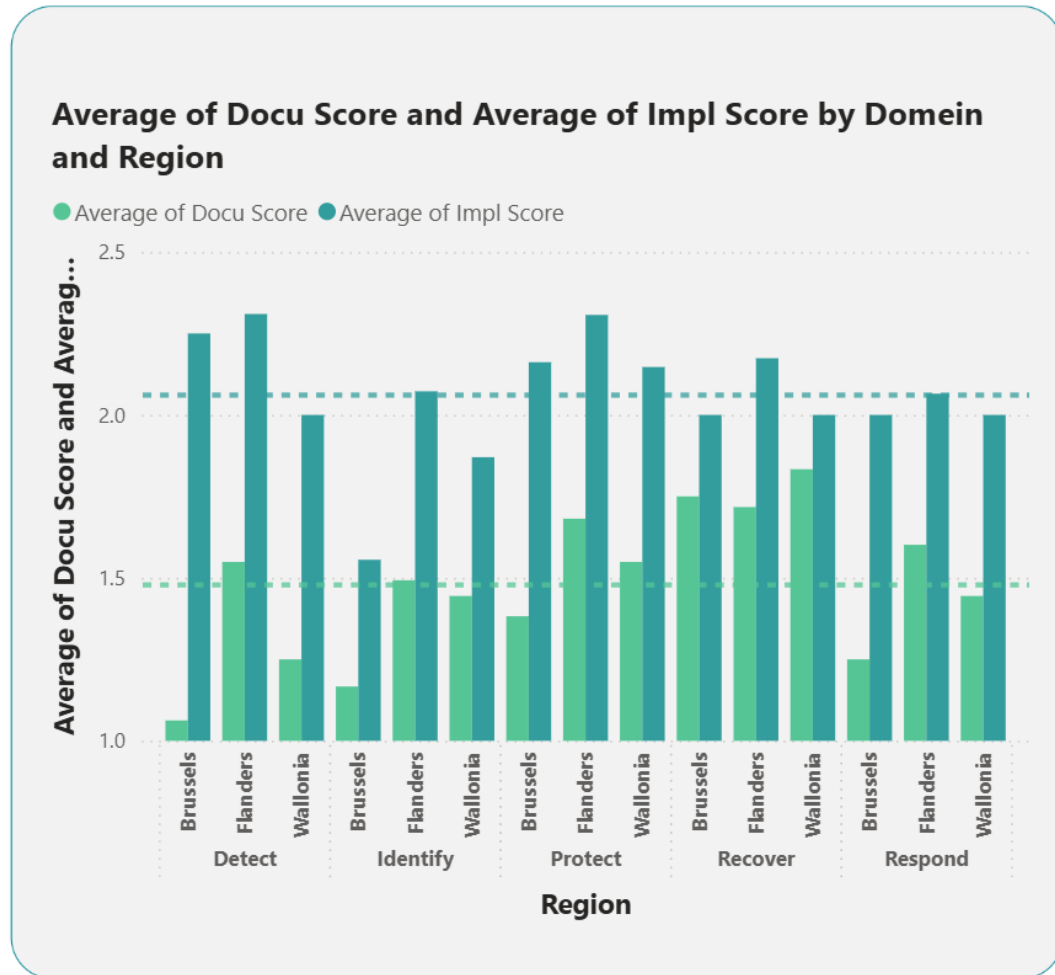
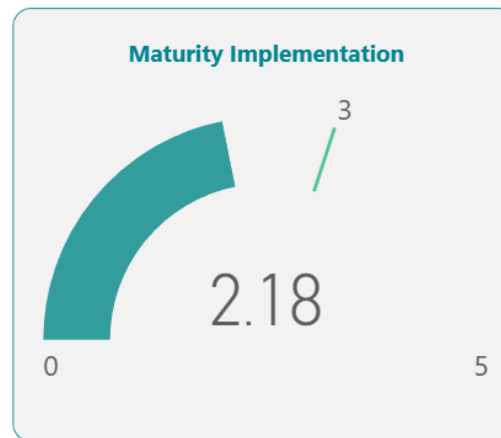
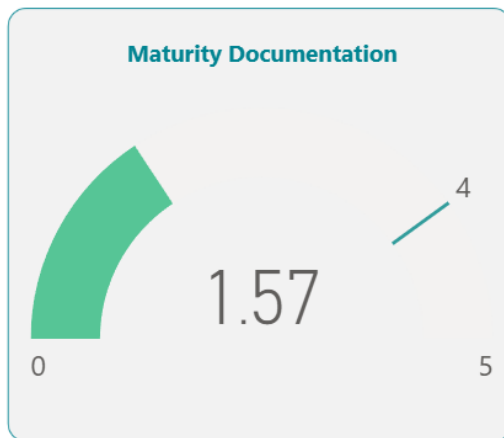
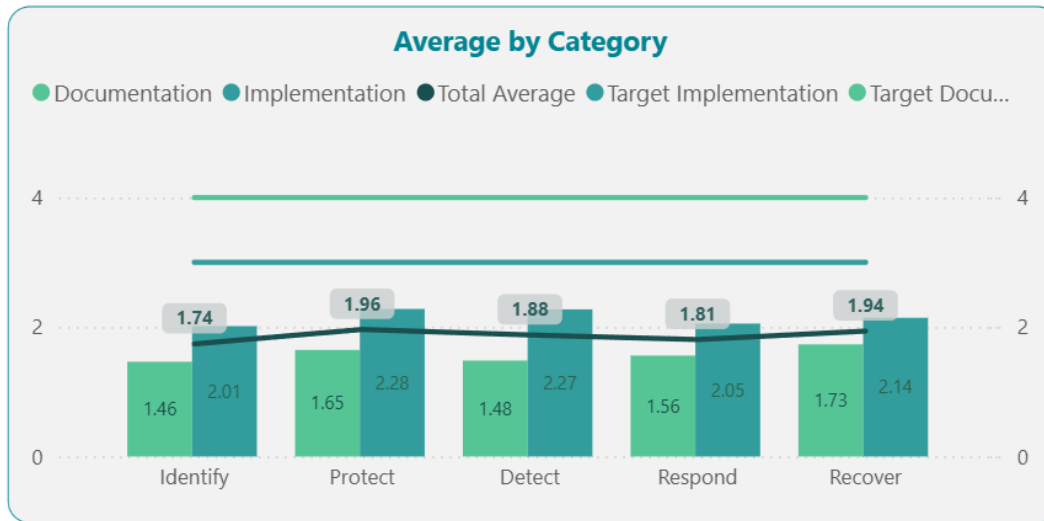


Figure 3 Overview Basic

2.1.1. Overview with Important & Essential Key Measures

As mentioned in Section 2.1 “The SHIELD Baseline Assessment”, we also assessed the other Key Measure categories (Important and Essential). Across the three regions, the average score for these two Key measures categories (covering 16 controls in total) is 1.33 for Documentation and 1.90 for Implementation. These results are lower than the Basic scores, which is expected, as Important and Essential controls require a higher level of maturity and more stringent requirements.

Following, the graph of the average score for the Important and Essential Key Measures of the three regions per CyFun category:

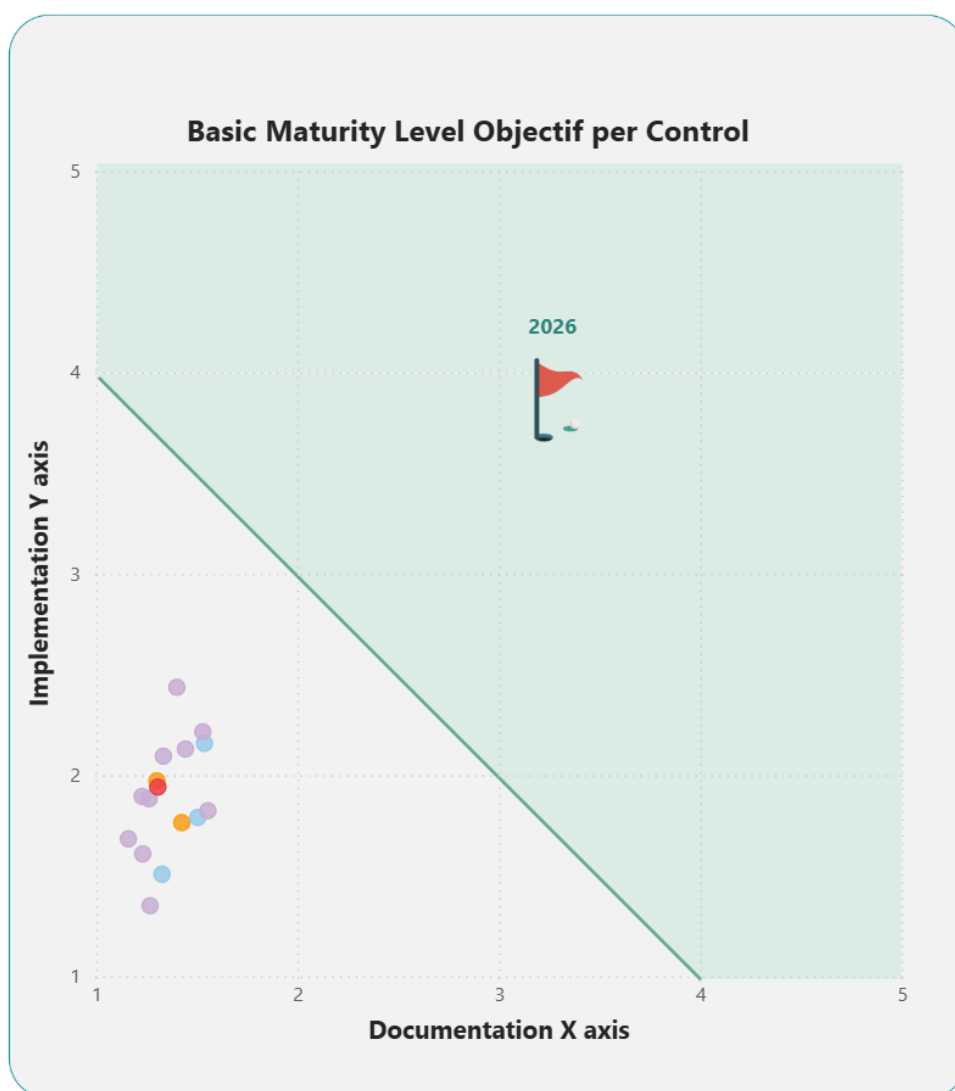


Figure 4 Dot Chart Important & Essential Key Measures

Comparing the two dot graphs in Sections 3 and this one above, we see that the dots in the second graph shift markedly to the left, indicating a significantly lower score.

Looking at the graph below, which presents the 2027 compliance status for the Important & Essential Key Measures, we recall that a minimum score of 3 out of 5 is required for each key measure. Out of a total of 2072 Important & Essential Key Measures assessed, only 122 (5.89%) currently meet this threshold, while 1950 (94.11%) remain below an average Documentation and Implementation score of 3.

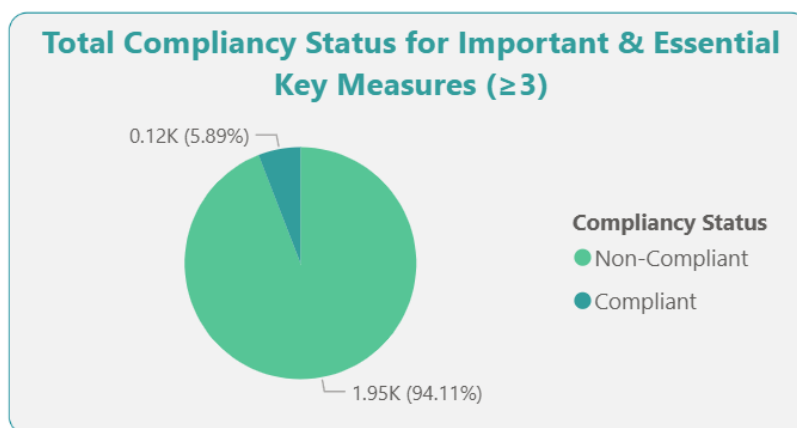


Figure 5 Compliance Status for Important & Essential Key Measures

2.2. Hospital Category Overview

General hospitals are nearer to 2.5 than Psychiatric hospitals, particularly on the Respond and Identify functions.

2.2.1. Documentation

Based on all assessments completed up to 31 October 2025, general hospitals score 1.66 on Documentation versus 1.30 for psychiatric hospitals an absolute difference of 0.36 points, i.e., ~28% higher relative to psychiatric hospitals. Qualitative feedback gathered during the assessments suggests this gap may reflect differences in staffing and available resources: general hospitals typically operate with larger IT/information-security teams, allowing more capacity to produce and maintain formal documentation.

2.2.2. Implementation

Across all hospitals, Implementation scores are consistently higher than Documentation. General hospitals score 2.23 on Implementation versus 2.04 for psychiatric hospitals an absolute difference of 0.19 points (approximately 9% higher relative to psychiatric hospitals).

The relatively small gap likely reflects offsetting factors: general hospitals face greater organizational and technical complexity, while also benefiting from larger teams to execute controls. The largest advantages for general hospitals are in Respond (Documentation 1.69 vs 1.13, +0.56; Implementation 2.17 vs 1.67, +0.50) and Identify (Documentation 1.57 vs 1.15, +0.42; Implementation 2.07 vs 1.89, +0.18).

Note: Although psychiatric hospitals score marginally higher on Detect (2.27 vs 2.26), this difference is not statistically meaningful given the sample sizes.

2.2.3. Conclusion

Both hospital categories remain below the 2.50 minimum required by April 2026 for the Basic measures. The shortfall is more pronounced for Documentation gaps of 0.84 in general hospitals and 1.20 in psychiatric hospitals than for Implementation (0.27 and 0.46, respectively).

Based on the assessments conducted, larger or better-resourced institutions appear more likely to reach compliance within the timeframe, contingent on sustained leadership alignment; however, such organizations represent a minority of the sector.

2.2.4. Score by General Hospital:

- General average score: 1.66 Documentation, 2.23 Implementation
- General score per Identify : 1.57 Documentation, 2.07 Implementation
- General score per Protect : 1.72 Documentation, 2.33 Implementation
- General score per Detect : 1.53 Documentation, 2.26 Implementation
- General score per Respond : 1.69 Documentation, 2.17 Implementation
- General score per Recover : 1.80 Documentation, 2.22 Implementation

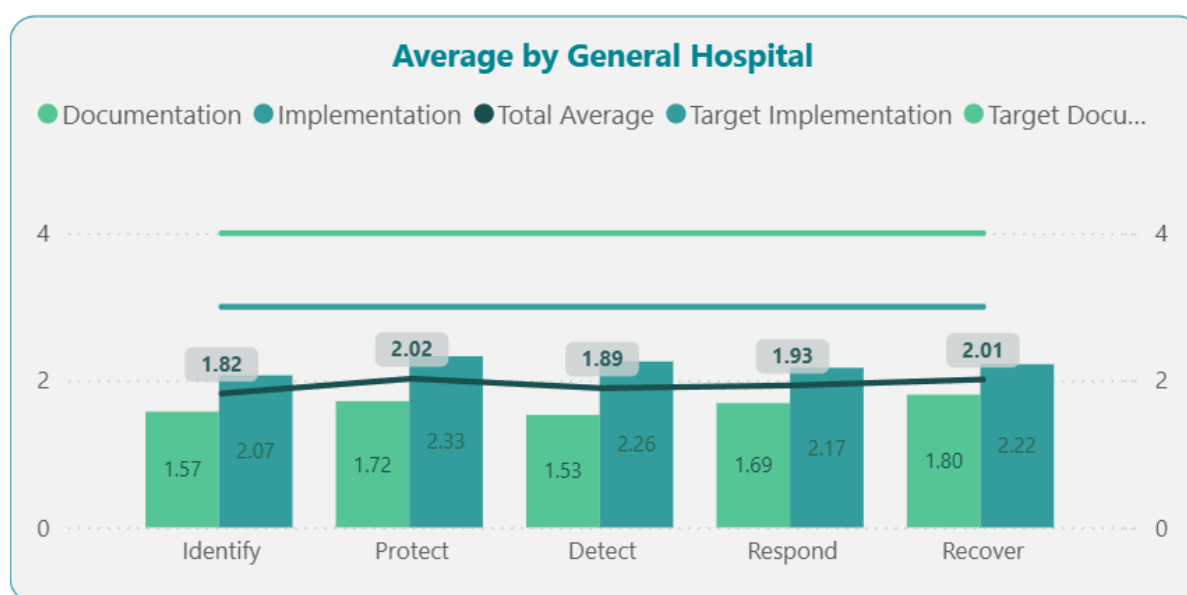


Figure 6 Average Score by General Hospital

2.2.5. Score by Psychiatric Hospital:

- Psychiatric average score: 1.30 Documentation, 2.04 Implementation
- Psychiatric score per Identify : 1.15 Documentation, 1.89 Implementation
- Psychiatric score per Protect : 1.41 Documentation, 2.14 Implementation
- Psychiatric score per Detect : 1.21 Documentation, 2.27 Implementation
- Psychiatric score per Respond : 1.13 Documentation, 1.67 Implementation
- Psychiatric score per Recover : 1.54 Documentation, 1.92 Implementation

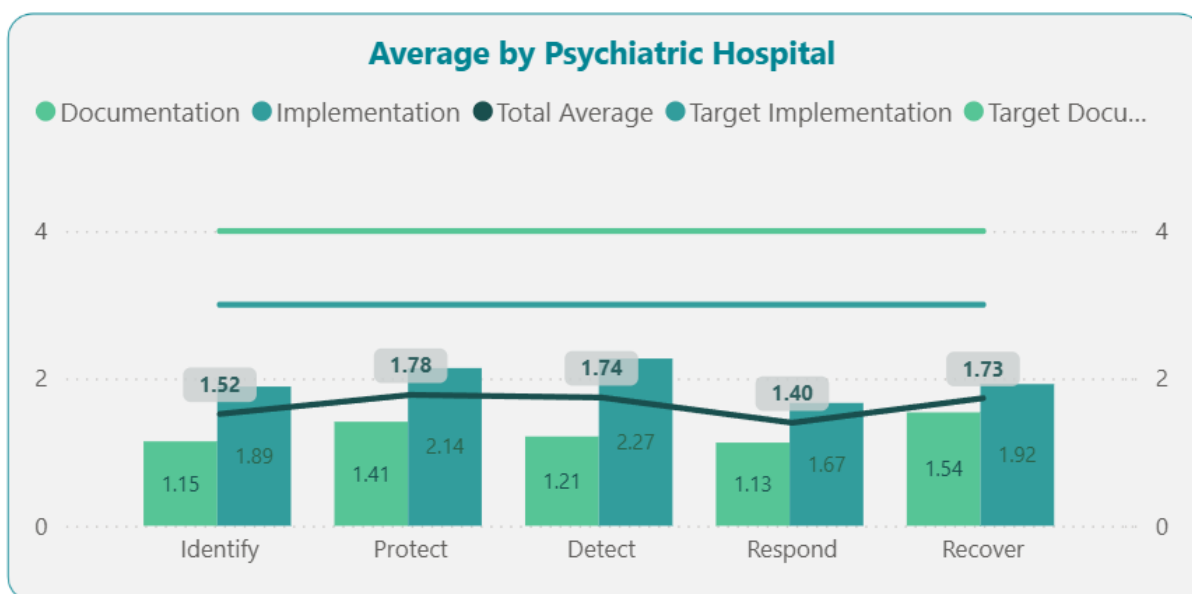


Figure 7 Average Score by Psychiatric Hospital

2.2.6. University Hospital scoring Overview

Among the **3 of 7** university hospitals assessed - and noting that in our Power BI model university hospitals are included within the General hospitals group - results are broadly in line with general hospitals overall, slightly higher on Documentation and on par for Implementation.

- Overall: University 1.79 Doc vs General 1.66 (+0.13); Implementation 2.23 vs 2.23 (0.00).
- Documentation (university minus general): Identify +0.10, Protect +0.14, Detect +0.05, Respond +0.31, Recover +0.20 => higher across all functions, especially Respond/Recover.
- Implementation (university minus general): Identify -0.07, Protect -0.09, Detect -0.01, Respond +0.27, Recover +0.11 => slightly behind on preventive areas (Identify/Protect), ahead on post-incident activities (Respond/Recover).

Takeaway: university hospitals don't diverge dramatically from the sector, but they document more consistently and show stronger response/recovery execution, with only marginal lags on Identify/Protect implementation.

- University average score: 1.79 Documentation, 2.23 Implementation
- University score per Identify : 1.67 Documentation, 2.00 Implementation
- University score per Protect : 1.86 Documentation, 2.24 Implementation
- University score per Detect : 1.58 Documentation, 2.25 Implementation
- University score per Respond : 2.00 Documentation, 2.44 Implementation
- University score per Recover : 2.00 Documentation, 2.33 Implementation

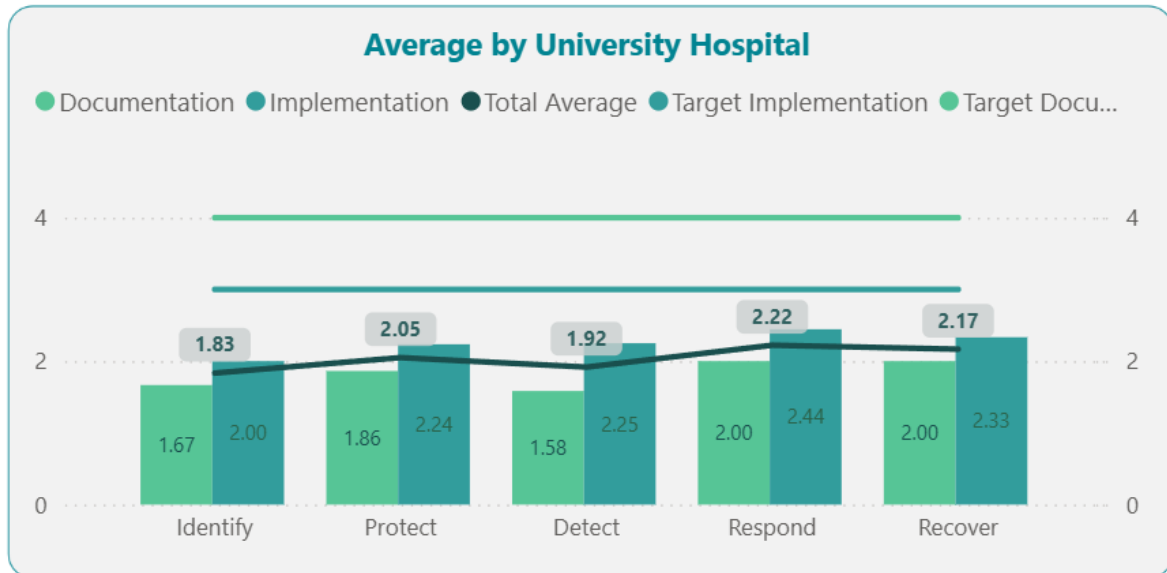


Figure 8 Average by University Hospital

The results for university hospitals should be interpreted with caution due to the limited sample size and the sensitivity of averages to individual scores. Preliminary analysis indicates that the maturity of university hospitals may diverge more strongly from general hospitals than initially concluded, particularly in the Identify and Protect implementation domains. An updated conclusion will be provided once all assessments are completed.

2.3. Best in class

2.3.1. Top 4 performers

The top four highest-scoring institutions include one university hospital, one university institution and two general hospitals, all located in different provinces in Flanders. As a group, they achieve an average maturity score of **2.64** across the 50 assessed controls, with **2.56 for documentation** and **2.72 for implementation**, placing them above the 2.50 Basic compliance threshold (key measures excluded).

Documentation performance

The strongest documentation scores are found in:

- communications (**2.83**)
- response planning (**2.83**)
- information protection processes and procedures (**2.75**)

Key documentation gaps remain in:

- data security (**2.17**)
- recovery planning (**2.00**)

At the 2.50 threshold level, additional uplift is needed in anomalies and events, improvements, maintenance and security continuous monitoring.

Implementation performance

Implementation maturity is consistently higher, with strong performance in:

- communications (**3.00**)
- security continuous monitoring (**3.00**)
- information protection processes and procedures (**2.83**)
- recovery planning (**2.83**)
- identity and access (**2.80**)

Lower-scoring areas include:

- anomalies and events (**2.17**)

- awareness and training (**2.33**)
- response planning (**2.33**)

Risk assessment remains below the 2.50 threshold.

Key insight

Even among the highest-performing hospitals, **implementation outpaces documentation**, and several foundational domains—particularly recovery planning (documentation) and anomalies and events (implementation)—still require targeted improvement to ensure full and consistent compliance across all categories.

Exceptional outlier performance

After the assessment cut-off date (31 October), one hospital in Wallonia achieved the highest maturity in the dataset, with **3.80 for documentation** and **3.56 for implementation** (average **3.68** across the 50 controls).

For the Basic scope including the Basic Key Measure, it reached **4.32 documentation** and **3.79 implementation**, meeting all 2026 Basic requirements except one control in awareness and training, which is expected to be completed by the deadline.

This exceptional performance is partly explained by its relatively low organisational complexity, a small but highly qualified team, strong leadership involvement and the ability to consistently allocate substantial resources to its security and compliance program.

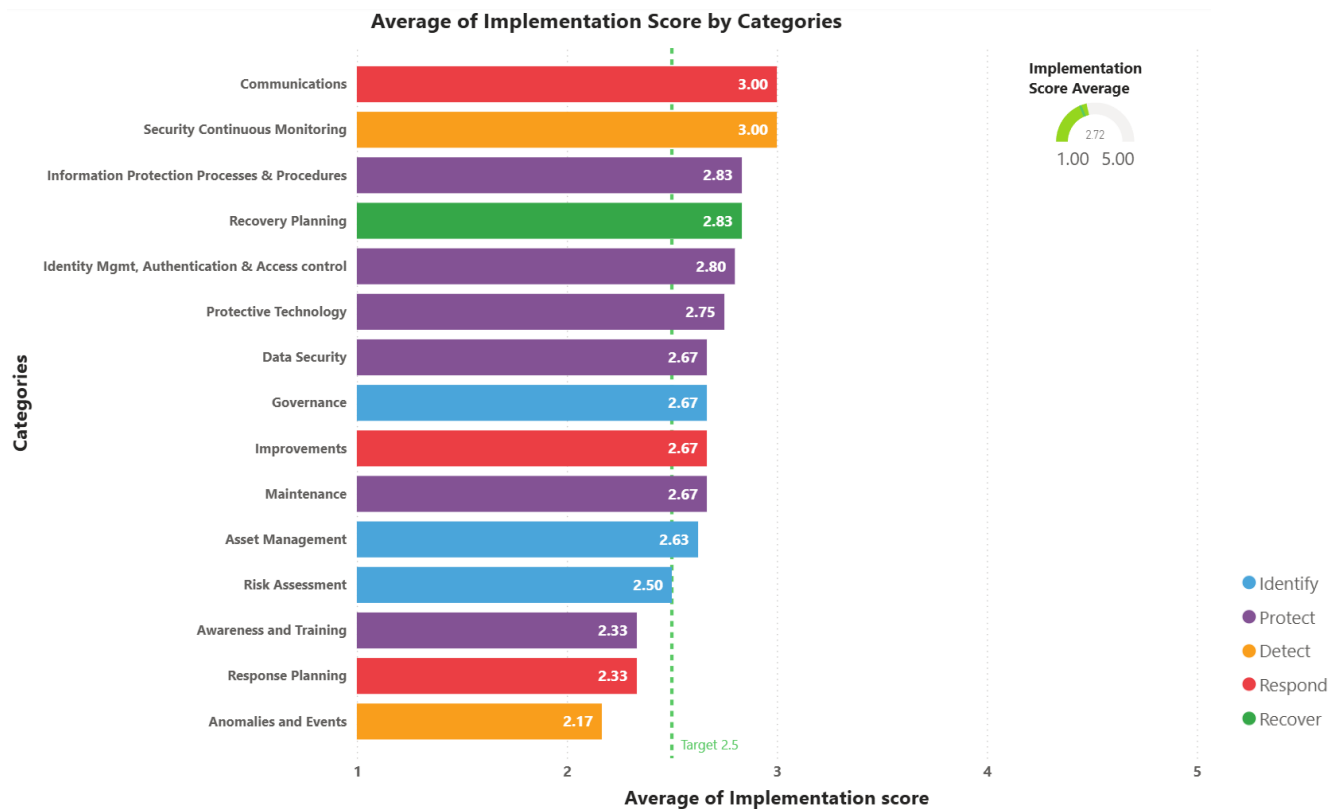
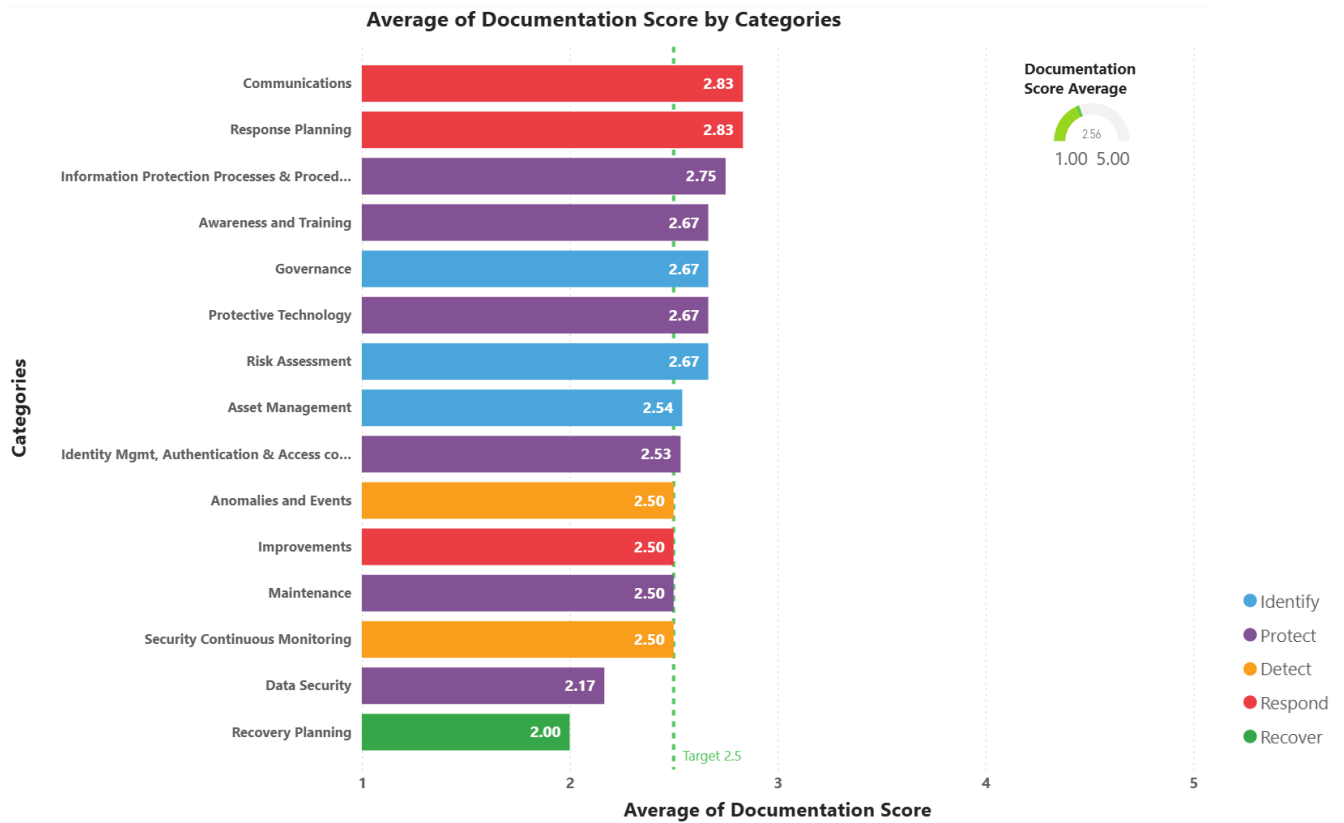


Figure 9 Top Performer Scoring Categories

2.3.2. Bottom 5 performers

The five lowest-scoring institutions consist of **two general hospitals and three psychiatric hospitals**, located across several provinces in Flanders. This cohort achieves an average maturity score of **1.43**, with **1.07 for documentation** and **1.79 for implementation**, placing them well below the Basic compliance threshold of 2.50.

- Documentation pervasive shortfall:
All categories are ≤ 1.20 . Several sit at the floor 1.00 (Anomalies & Events, Asset Management, Communications, Improvements, Maintenance, Recovery Planning, Response Planning, Risk Assessment), implying limited or no formal documentation. “Least bad” areas are at 1.20 (Awareness & Training, Data Security, Governance) and 1.13-1.10 (Security Continuous Monitoring 1.13, PR.IP 1.10, Protective Technology 1.10, Identity & Access 1.06).
- Implementation closest and weakest areas:
 - Closest to the threshold: Awareness & Training 2.40 (*gap 0.10*).
 - Mid gaps: Anomalies & Events 2.00 (*0.50*), Risk Assessment 2.00 (*0.50*), Security Continuous Monitoring 1.93 (*0.57*), PR.IP 1.90 (*0.60*).
 - Largest gaps: Response Planning 1.20 (*1.30*), Improvements 1.20 (*1.30*); Recovery Planning/Data Security 1.60 (*0.90*).

Takeaway: even within the lowest-performing group, **implementation (1.79) outpaces documentation (1.07)** by **0.72 points**, mirroring the sector-wide pattern. These institutions face fundamental structural challenges, with missing documentation, limited governance capacity and insufficient staffing. Without targeted support, they are unlikely to meet the April 2026 or April 2027 maturity requirements.

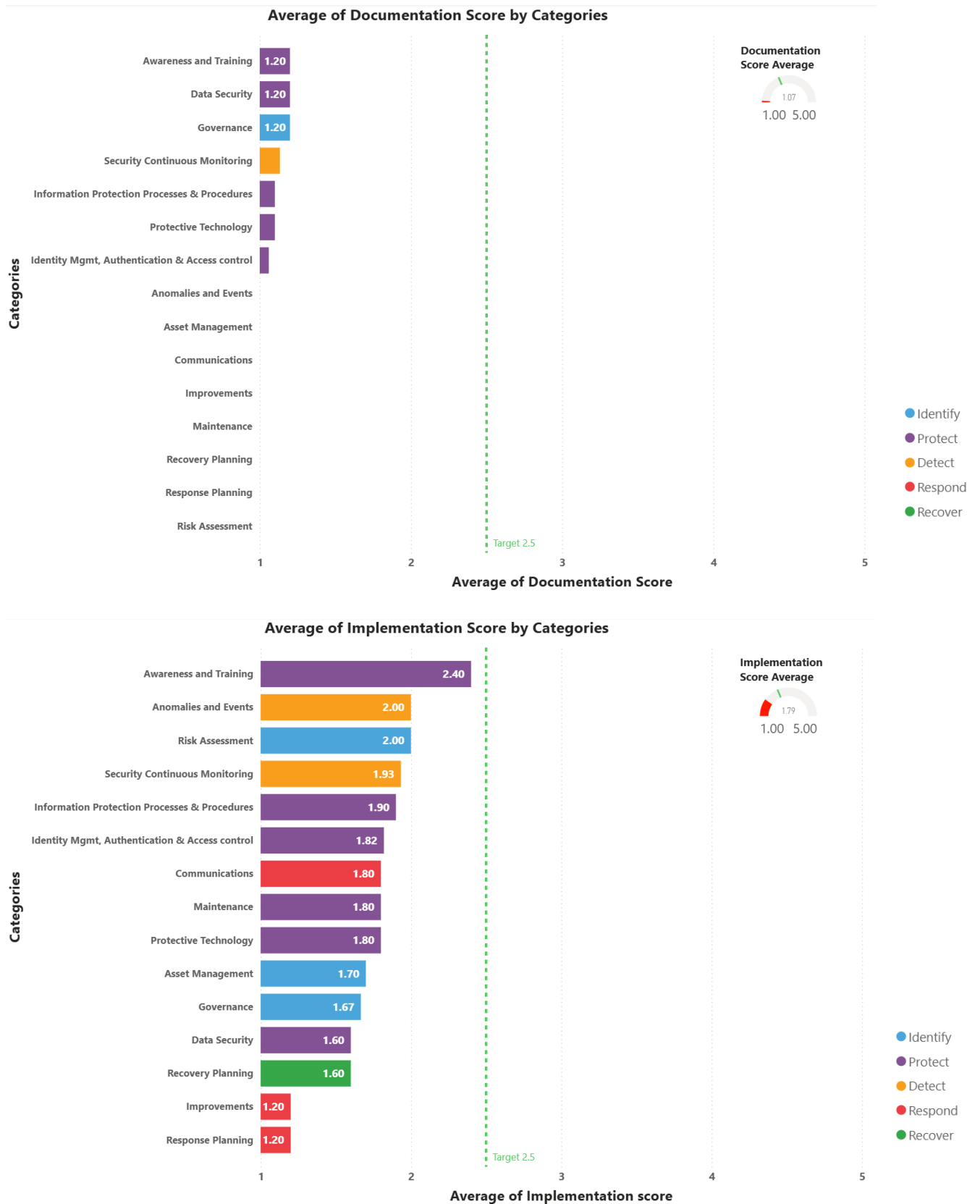


Figure 10 Bottom Performer Scoring Categories

2.3.3. Headline Gap - Top & Bottom 5

- Overall: Top-5 2.64 vs Bottom-5 1.43 → +1.21 points.
 - Documentation: 2.56 vs 1.07 → +1.49.
 - Implementation: 2.72 vs 1.79 → +0.93.
- Relative to 2.50 threshold: Top-5 sit +0.06 (Doc) and +0.22 (Impl) above; Bottom-5 are -1.43 (Doc) and -0.71 (Impl) below.

How many categories meet 2.50 (out of 15)?

- Top-5: 13/15 (Doc) and 12/15 (Impl) at ≥ 2.50 .
- Bottom-5: 0/15 (Doc) and 0/15 (Impl).

Where the gaps are largest (Top-5 minus Bottom-5)

- Documentation (biggest deltas):
 1. Communications +1.83; 2) Response Planning +1.83;
 2. Risk Assessment +1.67; 4) Info Protection (PR.IP) +1.65;
 3. Protective Technology +1.57; 6) Asset Management +1.54.
Smallest Doc deltas: Data Security +0.97, Recovery Planning +1.00.
- Implementation (biggest deltas):
 1. Improvements +1.47; 2) Recovery Planning +1.23;
 2. Communications +1.20; 4) Response Planning +1.13;
 3. Security Continuous Monitoring +1.07; 6) Data Security +1.07.
Smaller Impl deltas: Risk Assessment +0.50, Anomalies & Events +0.17.

2.4. The Value of the SHIELD Library

The SHIELD Library is a comprehensive, free set of documents⁴ tooling & process establishment practices designed to support an effective Information Security Management System (ISMS) implementation. The content aligns with ISO/IEC 27001:2022 and the CyberFundamentals 2023 (Essential) framework.

By using these ready-to-adapt templates, organizations can significantly reduce the time required to implement either framework, shifting effort from drafting documentation to execution and exception management. Members can tailor the materials to their context and proceed directly to implementation.

⁴ Under CC BY-NC-SA 4.0 License

While the SHIELD Library is often described in terms of its extensive set of policy, process and procedural templates, it should not be understood as merely a collection of documents that can be downloaded and placed on a shared drive. The library also includes process-establishment practices, workflow support, and practical tooling guidance that enable hospitals to operationalise and sustain their ISMS. Its purpose is to provide a structured foundation for embedding governance, processes and continuous maintenance into daily operations, rather than delivering static materials that remain detached from organisational practice.

It includes:

- 24 Policies
- 16 Processes
- 9 Procedures
- 4 Guidelines
- 18 Supporting Documents (e.g., organizational context, SWOT, supply-chain register)
- 16 Process Diagrams
- Additional helpful tools and registers

All topics within these documents are mapped to both ISO/IEC 27001:2022 and CyberFundamentals 2023 (Essential).

The Library has been refined through real-world deployments across several member organizations. In one measured case, an assessment of the 50 Controls conducted before adoption and repeated approximately one year after demonstrating clear efficiency and effectiveness gains attributable to the SHIELD Library.

2.4.1. How the SHIELD Library Boosted Documentation

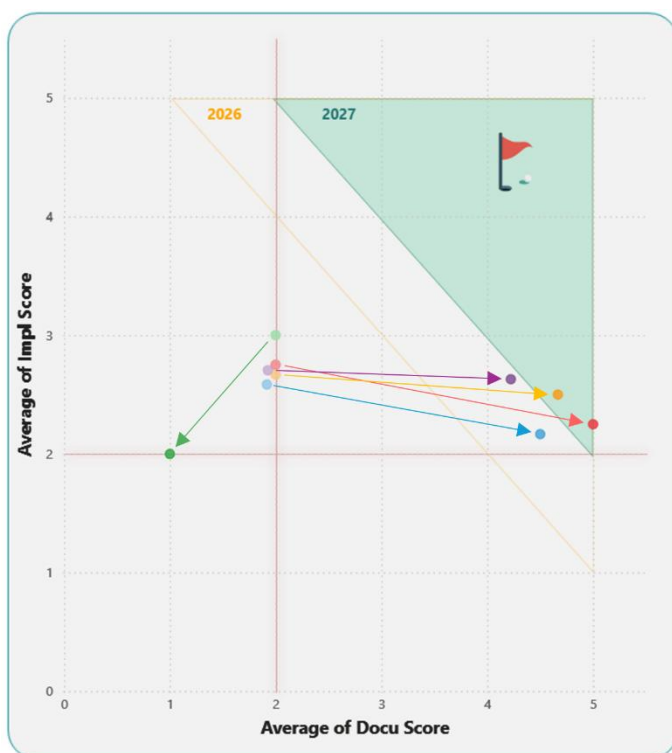


Figure 11 SHIELD Library Benefits Dots Chart

This chart compares the two aforementioned assessments. The lighter shapes show the earlier results; the darker shape shows the later results. Scores are plotted by domain **Identify**, **Protect**, **Detect**, **Respond**, and **Recover** with documentation on the x-axis and implementation on the y-axis. The members improved documentation (shift to the right) while implementation stayed roughly unchanged.

The assessment indicates a **major improvement** in documentation quality shown by a pronounced rightward shift on the x-axis while the implementation performance on the y-axis remained broadly stable.

The bar chart below shows the difference between documentation and implementation:

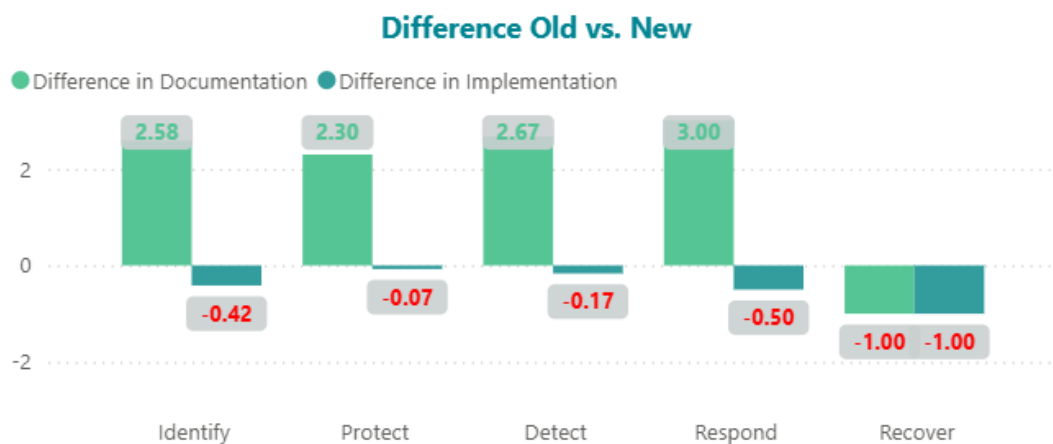


Figure 12 SHIELD Library Benefits Bars Chart Difference

Although the updated charts focus on domain-level results, the overall average score increased from 2,31 to 3,40 (not displayed in the graphs). From the detailed data, we note:

1. Implementation dipped overall. Despite stronger documentation, the aggregate implementation score is lower than in the first assessment.
2. Recover domain declined on both axes. Recover shows lower documentation and implementation scores compared to the initial baseline.
3. Identify gap persists. A material gap remains in the Identify domain, indicating continued weakness in foundational asset, risk, and context management.

2.4.1.1. Gaps Overview

The operational and regulatory complexity of healthcare environments helps explain several of the anomalies observed in this assessment. While the symptoms are easy to identify, the underlying causes are significantly more difficult to isolate. Together with the hospital, we conducted a detailed root-cause analysis to clarify the drivers behind each finding and to ensure that all conclusions are evidence-based.

decline in implementation maturity

Although documentation has improved, the overall implementation score decreased compared to the first assessment. This outcome is partly expected. The initial baseline is intentionally high-level and focuses on identifying major gaps. As maturity increases, the assessment becomes more rigorous, with deeper evidence testing, stricter validation requirements and reduced reliance on interviews. In other words, higher maturity raises the evaluation bar, which naturally exposes additional implementation issues that were not visible during the earlier, lighter assessment phase.

recover domain decline

Both documentation and implementation in the Recover domain declined relative to the baseline. This is consistent with recent findings: during implementation reviews we identified notable documentation gaps in several Recover controls. These gaps are currently being addressed through ongoing improvements and updates, which will be incorporated into future versions of the SHIELD Library. Maturity appears static because the new documentation is still under development, validation and formalisation; improvements will only be reflected in the next assessment cycle.

persistent identify weaknesses

The Identify domain continues to show structural weaknesses, particularly in asset management, risk assessment and contextual understanding of the hospital environment. As with the Recover domain, documentation for several risk and supply-chain controls is still being developed and will be added to the SHIELD Library once completed. This work-in-progress temporarily depresses current maturity scores but is expected to result in significant improvement once fully integrated.

2.4.2. A Fast-Tracking ISMS Documentation

The SHIELD Library - © 2025 Shield VZW – License CC BY-NC-SA 4.0 provides healthcare organisations with a fast and structured starting point for implementing ISO/IEC 27001:2022 and the CyberFundamentals 2023 Essential Framework. Its ready-to-use, sector-specific templates significantly reduce drafting effort, increase consistency and ensure alignment with recognised security standards.

However, the library is not a plug-and-play solution. To translate these templates into real and sustainable maturity, hospitals must adapt them to their own operational environment, integrate them into existing governance and clinical processes, and maintain them over time. This requires dedicated staff, protected time and clear local ownership.

The SHIELD Library accelerates the maturity journey and improves sector-wide consistency, but its effectiveness ultimately depends on the organisation's ability to tailor, implement and sustain the documentation so that policy, process and day-to-day practice remain fully aligned.

3. Conclusion

General hospitals remain measurably closer to the Basic maturity threshold of 2.50 than psychiatric hospitals, particularly within the Respond and Identify functions. However, neither group currently meets the April 2026 requirement. In both cases, the primary shortfall lies in **documentation**, with gaps of **0.84** for general hospitals and **1.20** for psychiatric hospitals, compared with smaller implementation gaps of **0.27** and **0.46** respectively. This confirms that many hospitals have operational controls in place but lack the formal, up-to-date documentation required for compliance. Notably, one university hospital and two general hospitals already exceed the overall average threshold of 2.50 but still fall below the required level on several individual Key Measures. An above-average total score therefore does not guarantee full compliance across all mandatory subcategories.

From a coverage perspective, SHIELD remains a developing program. To date, **55 assessments** have been completed, **6** are ongoing and **18** are scheduled for the coming weeks and early 2026, with further assessments planned. Each assessment consists of structured interviews followed by a detailed report including maturity scoring, a comparison with peer hospitals and targeted recommendations to improve both documentation and implementation. Nevertheless, several hospitals and specific sub-entities within hospital groups/networks - such as care organisations and specialised clinics - remain outside the current scope. Expanding and refining coverage in the next phases of SHIELD is essential to achieve a comprehensive, sector-wide maturity baseline and to ensure that no critical entities remain unassessed.

Within this broader context, the SHIELD Library plays an important enabling role. It offers a comprehensive set of sector-tailored documents to support effective ISMS implementation, fully aligned with ISO/IEC 27001:2022 and CyberFundamentals 2023 (Essential). With 24 policies, 16 processes, 9 procedures, 4 guidelines, 18 supporting documents, 16 process diagrams and additional tools, **all** mapped across both frameworks, the library provides broad coverage of the documentation requirements. However, despite being freely available, it is not a plug-and-play solution. Hospitals still require qualified personnel and protected time to tailor the templates to their environment, integrate them into existing processes, train staff and ensure ongoing maintenance. Without this investment, there is a risk of generating “paper compliance” that does not translate into sustainable operational maturity.

Experiences from real-world adoption show that, with sufficient resources, the SHIELD Library delivers substantial and measurable benefits. In one case, re-assessment of the 50 controls approximately one year after adoption increased the overall average maturity score from **2.31 to 3.40**, primarily due to stronger documentation. This demonstrates that systematic use of the library when combined with dedicated staffing and governance support can accelerate maturity growth significantly.

To close the remaining sector-wide gaps, the following priorities are essential:

- **scale SHIELD Library adoption** as the standard documentation accelerator, supported by administrative and security capacity, protected documentation time and standardised templates and processes
- **complete and refine assessment coverage**, ensuring that all hospitals and sub-entities are included in the national maturity baseline
- **provide targeted financial and technical support** to under-resourced and psychiatric hospitals, where capacity constraints are most severe
- **transfer practices from top performers** and maintain regular maturity monitoring against clear, resourced milestones, including preparation for the April 2027 requirements

In summary, SHIELD is an ongoing program that requires continued investment, structured governance and consistent adoption. By completing assessment coverage and systematically deploying the SHIELD Library—supported by adequate staffing and time for implementation and maintenance—the sector can progressively close its documentation and implementation gaps, strengthen resilience and move toward sustained compliance with both the 2026 and 2027 CyberFundamentals requirements.

4. Appendix

4.1. CyFun 2023 Basic Categories Mappings

ID	Category	Key Measure	Control Description
PR.AC-1.1	Identity Mgmt, Authentication & Access control	Yes	Identities and credentials for authorized devices and users shall be managed.
PR.AC-2.1	Identity Mgmt, Authentication & Access control	No	Physical access to the facility, servers and network components shall be managed.
PR.AC-3.1	Identity Mgmt, Authentication & Access control	No	The organization's wireless access points shall be secured.
PR.AC-3.2	Identity Mgmt, Authentication & Access control	Yes	The organization's networks when accessed remotely shall be secured, including through multi-factor authentication (MFA).
PR.AC-4.1	Identity Mgmt, Authentication & Access control	Yes	Access permissions for users to the organization's systems shall be defined and managed.
PR.AC-4.2	Identity Mgmt, Authentication & Access control	Yes	It shall be identified who should have access to the organization's business's critical information and technology and the means to get access.
PR.AC-4.3	Identity Mgmt, Authentication & Access control	Yes	Employee access to data and information shall be limited to the systems and specific information they need to do their jobs (the principle of Least Privilege).
PR.AC-4.4	Identity Mgmt, Authentication & Access control	Yes	Nobody shall have administrator privileges for daily tasks.
PR.AC-5.1	Identity Mgmt, Authentication & Access control	Yes	Firewalls shall be installed and activated on all the organization's networks.

PR.AC-5.2	Identity Mgmt, Authentication & Access control	Yes	Where appropriate, network integrity of the organization's critical systems shall be protected by incorporating network segmentation and segregation.
PR.AT-1.1	Awareness and Training	No	Employees shall be trained as appropriate.
PR.DS-3.1	Data Security	No	Assets and media shall be disposed of safely.
PR.IP-11.1	Information Protection Processes & Procedures	No	Personnel having access to the organization's most critical information or technology shall be verified.
PR.IP-4.1	Information Protection Processes & Procedures	Yes	Backups for organization's business critical data shall be conducted and stored on a system different from the device on which the original data resides
PR.MA-1.1	Maintenance	Yes	Patches and security updates for Operating Systems and critical system components shall be installed.
PR.PT-1.1	Protective Technology	Yes	Logs shall be maintained, documented, and reviewed.
PR.PT-4.1	Protective Technology	No	Web and e-mail filters shall be installed and used.
DE.AE-3.1	Anomalies and Events	Yes	The activity logging functionality of protection / detection hardware or software (e.g. firewalls, anti-virus) shall be enabled, backed-up and reviewed.
DE.CM-1.1	Security Continuous Monitoring	No	Firewalls shall be installed and operated on the network boundaries and completed with firewall protection on the endpoints.
DE.CM-3.1	Security Continuous Monitoring	No	End point and network protection tools to monitor end-user behavior for dangerous activity shall be implemented.
DE.CM-4.1	Security Continuous Monitoring	Yes	Anti-virus, -spyware, and other -malware programs shall be installed and updated.

ID.AM-1.1	Asset Management	No	An inventory of assets associated with information and information processing facilities within the organization shall be documented, reviewed, and updated when changes occur.
ID.AM-2.1	Asset Management	No	An inventory that reflects what software platforms and applications are being used in the organization shall be documented, reviewed, and updated when changes occur.
ID.AM-3.1	Asset Management	No	Information that the organization stores and uses shall be identified.
ID.AM-5.1	Asset Management	No	The organization's resources (hardware, devices, data, time, personnel, information, and software) shall be prioritized based on their classification, criticality, and business value.
ID.GV-1.1	Governance	No	Policies and procedures for information security and cyber security shall be created, documented, reviewed, approved, and updated when changes occur.
ID.GV-3.1	Governance	No	Legal and regulatory requirements regarding information/cybersecurity, including privacy obligations, shall be understood and implemented.
ID.GV-4.1	Governance	No	As part of the company's overall risk management, a comprehensive strategy to manage information security and cybersecurity risks shall be developed and updated when changes occur.
ID.RA-1.1	Risk Assessment	No	Threats and vulnerabilities shall be identified.
ID.RA-5.1	Risk Assessment	No	The organization shall conduct risk assessments in which risk is determined by threats, vulnerabilities and impact on business processes and assets.
RC.RP-1.1	Recovery Planning	No	A recovery process for disasters and information/cybersecurity incidents shall be developed and executed as appropriate.
RS.CO-3.1	Communications	No	Information/cybersecurity incident information shall be communicated and shared with the organization's employees in a format that they can understand.

RS.IM-1.1	Improvements	No	The organization shall conduct post-incident evaluations to analyse lessons learned from incident response and recovery, and consequently improve processes / procedures / technologies to enhance its cyber resilience.
-----------	--------------	----	--

4.2. CyFun 2023 Key Measure Essential and Important Mappings

ID	Category	Key Measure	Control Description
ID.SC-3.2	Supply Chain Risk Management	Yes	Contractual information security and cybersecurity' requirements for suppliers and third-party partners shall be implemented to ensure a verifiable flaw remediation process, and to ensure the correction of flaws identified during 'information security and cybersecurity' testing and evaluation. o ensure the correction of flaws identified during 'information security and cybersecurity' testing and evaluation.
ID.AM-6.1	Asset Management	Yes	Information security and cybersecurity roles, responsibilities and authorities within the organization shall be documented, reviewed, authorized, and updated and alignment with organization-internal roles and external partners. Key Measure
PR.MA-1.6	Maintenance	Yes	Maintenance tools and portable storage devices shall be inspected when brought into the facility and shall be protected by anti-malware solutions so that they are scanned for malicious code before they are used on organization's systems.
PR.PT-2.3	Protective Technology	Yes	Portable storage devices containing system data shall be controlled and protected while in transit and in storage.
PR.IP-1.1	Information Protection Processes & Procedures	Yes	The organization shall develop, document, and maintain a baseline configuration for the its business critical systems.
DE.AE-1.1	Anomalies and Events	Yes	The organization shall ensure that a baseline of network operations and expected data flows for its critical systems is developed, documented and maintained to track events.

ID.SC-3.3	Supply Chain Risk Management	Yes	The organization shall establish contractual requirements permitting the organization to review the 'information security and cybersecurity' programs implemented by suppliers and third-party partners.
RS.AN-5.1	Analysis	Yes	The organization shall implement vulnerability management processes and procedures that include processing, analyzing and remediating vulnerabilities from internal and external sources.
PR.AC-5.4	Identity Mgmt, Authentication & Access control	Yes	The organization shall monitor and control connections and communications at the external boundary and at key internal boundaries within the organization's critical systems by implementing boundary protection devices where appropriate.
DE.CM-1.2	Security Continuous Monitoring	Yes	The organization shall monitor and identify unauthorized use of its business critical systems through the detection of unauthorized local connections, network connections and remote connections.
PR.AC-7.1	Identity Mgmt, Authentication & Access control	Yes	The organization shall perform a documented risk assessment on organization's critical system transactions and authenticate users, devices, and other assets (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).
PR.MA-1.5	Maintenance	Yes	The organization shall prevent the unauthorized removal of maintenance equipment containing organization's critical system information.
PR.DS-5.1	Data Security	Yes	The organization shall take appropriate actions resulting in the monitoring of its critical systems at external borders and critical internal points when unauthorized access and activities, including data leakage, is detected.
PR.MA-1.7	Maintenance	Yes	The organization shall verify security controls following hardware and software maintenance or repairs/patching and take action as appropriate.
PR.AC-3.3	Identity Mgmt, Authentication & Access control	Yes	Usage restrictions, connection requirements, implementation guidance, and authorizations for remote access to the organization's critical systems environment shall be identified, documented and implemented.

PR.AC-5.3	Identity Mgmt, Authentication & Access control	Yes	Where appropriate, network integrity of the organization's critical systems shall be protected by (1) Identifying, documenting, and controlling connections between system components. (2) Limiting external connections to the organization's critical systems.
-----------	--	-----	--

4.3. Hospital Name per Categories

Name	Category	Name	Category
A.S.B.L. Santé et Prévoyance - Clinique Saint-Luc Bouge	Hospital - General	Epsilon A.S.B.L (Fond'Roy)	Hospital - Psychiatric
Algemeen Ziekenhuis Sint-Lucas vzw	Hospital - General	Feux Follets ASBL	Hospital - Psychiatric
Arteveldehogeschool vzw	Higher Education Institution	GPN SON	Care provider
AZ Alma	Hospital - General	Grand Hôpital de Charleroi	Hospital - General
AZ Delta	Hospital - General	Groep Zorg H. Familie	Care provider
AZ Groeninge	Hospital - General	Groupe santé CHC	Hospital - General (group)
AZ Herentals	Hospital - General	Heilig Hart Leuven	Hospital - General
AZ Jan Palfijn	Hospital - General	Heilig Hartziekenhuis Mol	Hospital - General
AZ Jan Portaels	Hospital - General	HeiligHart Lier	Hospital - General
AZ Klina	Hospital - General	Hôpital Erasme - Cliniques Universitaires de Bruxelles	Hospital - University
AZ Maria Middelaers	Hospital - General	Hopitaux Iris Sud	Hospital - General
AZ Monica	Hospital - General	Humani	Hospital - General (network)

Public

AZ Oostende	Hospital - General	IGL - Ter Heide	Care provider
AZ Oudenaarde	Hospital - General	Imelda	Hospital - General
AZ Rivierenland	Hospital - General	Integro	Care provider
AZ Sint-Blasius Campus Dendermonde ASBL	Hospital - General	Jan Yperman Ziekenhuis vzw	Hospital - General
AZ Sint-Jan Brugge AV	Hospital - General	Jessa ziekenhuis	Hospital - General
AZ Sint-Lucas & Volkskliniek vzw	Hospital - General	Karus vzw	Hospital - Psychiatric
AZ Sint-Maarten (Emmaüs)	Hospital - General	Katholieke Hogeschool VIVES	University college
AZ Sint-Maria	Hospital - General	Kliniek St. Josef - St. Vith	Hospital - General
AZ Turnhout	Hospital - General	Le Beau Vallon Namur asbl	Hospital - Psychiatric
AZ Vesalius	Hospital - General	MKL	Care provider
AZ Voorkempen (Emmaüs)	Hospital - General	Noorderhart	Hospital - General (network)
AZORG vzw	Care provider	Oeuvres des Frères de la Charité	Care provider
Becura Woonzorg vzw	Care provider	Openbaar Psychiatrisch Zorgcentrum Geel	Hospital - Psychiatric
Borgerstein VZW	Care provider	OPZC Rekem	Hospital - Psychiatric
Broeders van Liefde Organisatie vzw	Care provider	Psychiatrisch Ziekenhuis Bethanië (Emmaüs)	Hospital - Psychiatric
Centre Hospitalier de Mouscron	Hospital - General	Regionaal Ziekenhuis Heilig Hart Tienen	Hospital - General
Centre Hospitalier de Wallonie Picarde	Hospital - General	Sint-Andries Ziekenhuis Tielt	Hospital - General
Centre Hospitalier EpiCURA a.s.b.l.	Hospital - General	Sint-Franciscusziekenhuis	Hospital - General
Centre Hospitalier Régional Citadelle	Hospital - General	Sint-Jozefskliniek vzw	Hospital - General
Centre Hospitalier Regional de Verviers	Hospital - General	Sint-Trudo Ziekenhuis VZW	Hospital - General
Centre Hospitalier Régional Sambre et Meuse	Hospital - General	St. Nikolaus Hospital Eupen	Hospital - General
Centre Hospitalier Reine Astrid Malmedy	Hospital - General	Stijn vzw	Care provider
Centre Hospitalier Universitaire de Tivoli	Hospital - University	UHasselt	University

Public

Centre Neuro Psychiatrique Saint-Martin	Hospital - Psychiatric	Universitair Psychiatrisch Centrum Duffel (Emmaüs)	Hospital - Psychiatric
Centre Regional de Soins Psychiatriques Les Marronniers	Hospital - Psychiatric	Universitair Ziekenhuis Antwerpen	Hospital - University
CHIREC Hospital Group	Hospital - General	Universitair Ziekenhuis Gent	Hospital - University
CHR Haute Senne	Hospital - General	UZ Leuven	Hospital - University
CHU Brugmann	Hospital - University	VITAZ	Hospital - General
Chu Helora	Hospital - University	Vivalia	Hospital - General
CHU Saint-Pierre	Hospital - University	vzw Gezondheidszorg Bermhertigheid Jesu	Care provider
Clinique CHC MontLégia	Hospital - General	Wit-Gele Kruis van Limburg	Care provider
Clinique Notre-Dame de Grâce	Hospital - General	ZAS vzw	Hospital - General (network)
Clinique Saint-Pierre Ottignies	Hospital - General	Ziekenhuis Geel	Hospital - General
Cliniques de l'Europe / Europa Ziekenhuizen	Hospital - General	<i>Ziekenhuis Maas en Kempen vzw</i>	<i>Hospital - General</i>
Cliniques Universitaires Saint-Luc	Hospital - University	Ziekenhuis Oost-Limburg	Hospital - General
Covida vzw	Care provider	Zorggroep Annendael	Care provider
Emmaüs vzw	Care provider	Zorggroep Myna	Hospital - Psychiatric

4.4. SHIELD Baseline Assessment 50 Controls Overview



> ☒ BasicControlNoKeyMeasure

> ☒ BasicKeyMeasure

> ☒ ImportantEssentialKeymeasure

Total Members Assessed

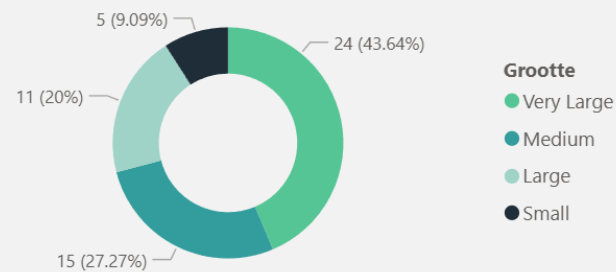
55

Total Controls Assessed

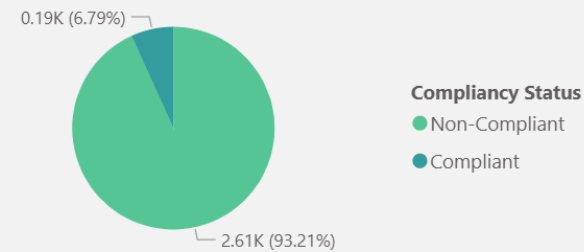
2800

Count of ID

Size spread



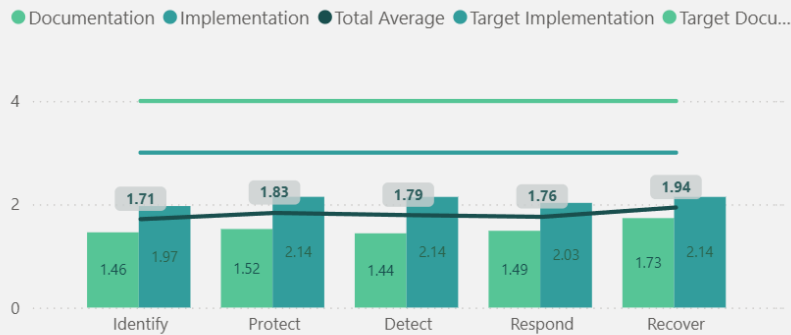
Total Compliancy Status for Important & Essential Key Measures (≥3)





- ▼ BasicControlNoKeyMeasure
- ▼ BasicKeyMeasure
- ▼ ImportantEssentialKeymeasure

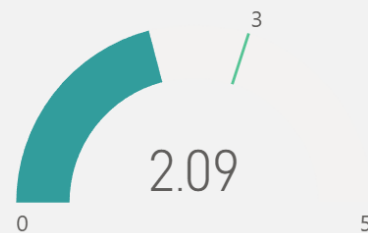
Average by Category



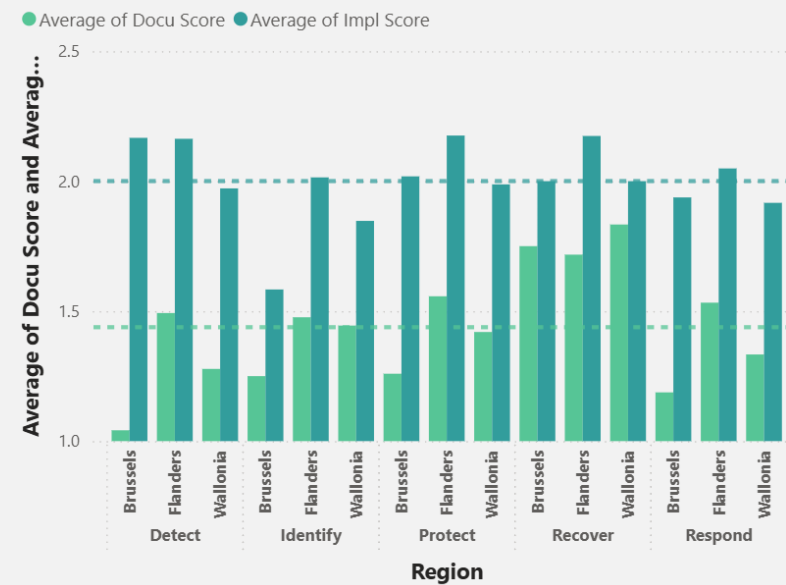
Maturity Documentation



Maturity Implementation



Average of Docu Score and Average of Impl Score by Domein and Region



DISCLAIMER:

The average figure is the weighted average across Belgium