SYMBEEO

PUBLIC

DESIGN STUDY

Current-state assessment and CSF 2.0 profile for a six-hospital group before a three-domain refresh

Complete design on current platforms

CAPABILITY	INDUSTRY	SETTING
Consulting & Engineering	Healthcare	Hospital group
DOCUMENT	**VERSION**	**DATE**
CON-004	1.1	Oct 10, 2026

WRITTEN BY

David Morgan, Principal Security Architect

© 2026 Symbeeo. All rights reserved.

Document control

Document	CON-004	Version	1.1
Issued	Oct 10, 2026	Status	Issued by Symbeeo
Classification	Public	Supersedes	1.0, Sep 27, 2026
Capability	Consulting & Engineering	Industry	Healthcare
Author	David Morgan	Role	Principal Security Architect
Credentials	CCISO, CISSP, CISSP-ISSEP, CISM, CISA, CRISC, PMP, CCSP, Adopting Zero Trust (Forrester)		
Approval	Approved by Edwin Ozer, Founder, Oct 10, 2026. Issued by Symbeeo, Oct 10, 2026. Design study: every figure is vendor-published, a design target or a marked assumption.		
Sign-off	"An engagement under this design is signed by the practice lead before the engagement starts."		

Contents

1 · Scope 3
1c · Public implementations this design follows 3
2 · Requirements register 4
3 · Architecture overview 5
4 · Design by subsystem 6
5 · Failure behavior 7
6 · Limits 7
7 · Lessons learned 7
8 · The author 7

© 2026 Symbeeo. All rights reserved. · Public

CONVENTIONS

Source tags. [S] figure or clause read from the standards body's or publisher's own current page on Sep 24, 2026 · [S*] figure from the page summary where the page itself could not be opened · [A] assumption about the typical buyer, to be confirmed by the signing engineer · [T] design target taken from the design's stated outcome or derived from it. Every figure carries one tag. No figure comes from any prior engagement, file or asset. A row with more than one tag is counted once: as a published figure if any tag is [S] or [S*], otherwise as an assumption if any tag is [A], otherwise as a design target.

Table 1. Revision history

Date	Version	Change
Sep 27, 2026	1.0	First issue.
Oct 10, 2026	1.1	Approval line now reads: approved by the Founder, issued by Symbeeo. David Morgan remains the author.

1 · Scope

Who it is for. The CIO of a hospital group who has network, data-center and security platforms all reaching end of support within three years, a board asking which to fund first, and no inventory anyone trusts — and who wants one measured baseline before any vendor is invited to propose.

Typical buyer [A]. A hospital group of six hospitals and 14 outpatient clinics in one EU member state: 11,000 staff, 2,300 beds, two data centers, one hyperscaler tenancy, about 9,000 networked clinical devices (infusion pumps, monitors, imaging) on the same campus networks as the office estate, and a CMDB last reconciled four years ago.

What is in. Current-state baseline of network, data center and security, including clinical devices by count and segment; lifecycle status of every reconciled item; CSF 2.0 Current and Target Organizational Profiles; a risk register on the group's criteria; NIS2 applicability; a sequenced roadmap in three horizons that says which domain to refresh first and why. SRA-CON-001 Model A. **What is out.** Clinical-device security testing; medical-device regulatory assessment; the design of any refresh (SRA-NET-001, SRA-DC-001 and SRA-SEC-001 own that); patient-data handling of any kind.

Assumptions. The group is an essential or important entity under national NIS2 transposition [A]. Active scans are not allowed on clinical-device segments; those segments are observed passively [A]. Each hospital names one delegate for the engagement [A]. No patient data is in scope and none is read [A].

Related documents, read Sep 24, 2026. SRA-CON-001, SDD-CON-001, STP-CON-001 (this capability) · NIST CSF 2.0 profiles page and Organizational Profile template, https://www.nist.gov/cyberframework/profiles · NIST CSF 2.0, CSWP 29, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf · NIST SP 1301, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1301.pdf · European Commission, action plan on the cybersecurity of hospitals and healthcare providers (Jan 15, 2025), https://commission.europa.eu/news/bolstering-cybersecurity-healthcare-sector-2025-01-15_en · NIS2, Directive (EU) 2022/2555, https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng.

1c · Public implementations this design follows

Each row is labeled. **Public deployment**: a named operator's real deployment, published and dated by the operator, its vendor or a partner, used where one exists. **Our own design**: the dated vendor or standards documentation this design was built from, where no public deployment of the design exists. Labels and dates checked Sep 27, 2026.

© 2026 Symbeeo. All rights reserved. · Public

Table 2. Public implementations this design follows

Implementation	Who published it · date	What it settles for this design	URL
Our own design, built from published documentation. CSF 2.0 Organizational Profile template: a spreadsheet for side-by-side Current and Target Profiles to identify and analyze gaps	NIST · profiles page updated Sep 17, 2026; template file dated Feb 20, 2024	R6 and §4.4: the profile is built on NIST's own template, so the board sees the same form the auditor and any successor assessor will use	https://www.nist.gov/cyberframework/profiles
Our own design, built from published documentation. European action plan on the cybersecurity of hospitals and healthcare providers: 309 cybersecurity incidents in EU health in 2023, more than any other critical sector; a support center at ENISA with guidance, tools and procurement good practice	European Commission · Jan 15, 2025	§4.6 and the roadmap: health is named by the Commission as the most-attacked critical sector, which sets the weight of the security domain in the sequencing; the center's procurement guidance is a source to check again before any tender	https://commission.europa.eu/news/bolstering-cybersecurity-healthcare-sector-2025-01-15_en
Our own design, built from published documentation. NIST SP 1301, Quick-Start Guide for Creating and Using Organizational Profiles: scope the profile, gather information, create the profiles, analyze gaps and plan, implement and update	NIST · published Feb 26, 2024; publication page read Sep 27, 2026	§4.1–§4.6: evidence is gathered before any profile is scored, and the gap analysis comes before the roadmap, in the guide's order	https://csrc.nist.gov/pubs/sp/1301/final
Public deployment. A US academic health system ran a standards-based NIST CSF 2.0 maturity assessment with an external assessor, as its governance, risk and compliance director describes	Clearwater Security blog · Jul 9, 2026 (date from the published summary; the page shows none) [S*]	§4.1–§4.5: a hospital system assessing itself on CSF 2.0 before acting. It reports a maturity score, not Organizational Profiles, so it settles the approach only; no figure from it enters the register	https://clearwatersecurity.com/blog/nist-csf-2-0-healthcare/

2 · Requirements register

Table 3. Requirements register

#	Requirement	Value	Source
R1	Scope	6 hospitals · 14 clinics · 2 data centers · 1 tenancy; domains network, data center, security	[A]
R2	Inventory coverage, IT	≥ 95 % of IT devices reconciled across two sources at every site	[T] from SRA-CON-001 R2
R3	Inventory coverage, clinical	clinical devices counted by segment from passive observation, matched to the biomedical engineering asset list	[T]
R4	Clinical-device population	about 9,000 networked devices	[A]
R5	Lifecycle status	100 % of reconciled IT items carry the vendor's end-of-sale and end-of-support dates, or "no public date" with the URL searched	[T]

© 2026 Symbeeo. All rights reserved. · Public

#	Requirement	Value	Source
R6	CSF 2.0 profiles	Current and Target at all 106 Subcategories on the NIST template; gap stated per Subcategory	[S] CSWP 29; NIST template
R7	Risk register	each gap entered with likelihood, impact, owner and treatment on the group's criteria	[S] ISO 31000:2018; ISO/IEC 27005:2022
R8	Refresh sequence	one ranked order of the three domains, each rank justified by ≥ 2 risk entries	[T]
R9	Roadmap	every item in one horizon (0–6, 6–18, 18–36 months) and linked to ≥ 1 gap and ≥ 1 requirement	[T] from SRA-CON-001 R11
R10	NIS2 applicability	marked, with one sentence of basis	[S] EUR-Lex
R11	Clinical safety	zero active scans on clinical segments; zero clinical-device reboots caused by the engagement	[T]
R12	Delegates	one named delegate per hospital, available for 2 interviews	[A]
R13	Turnaround	report issued ≤ 20 working days after access is granted	[T]
R14	Evidence handling	raw data held in the group's tenancy; no patient data read	[A]

Fourteen rows; three carry a published figure, four are design assumptions, seven are design targets.

3 · Architecture overview

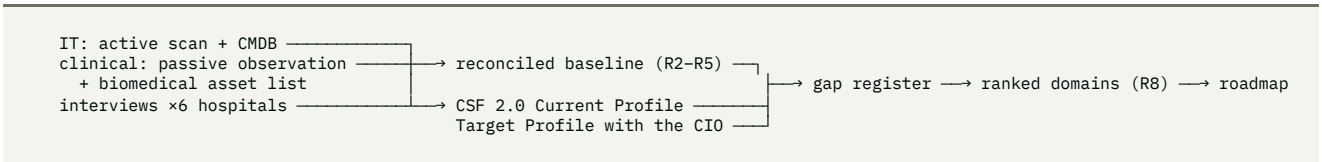


Figure 1. Baseline, profiles and domain ranking

Measure first, profile second, rank the three refreshes on the risks the measurement found.

Table 4. Architecture overview

Role	Component (exact name)	Qty	Capacity used	Why this unit
Security lens	NIST CSF 2.0 (CSWP 29)	1	106 Subcategories [S]	SRA-CON-001 D6: CSF 2.0 always
Profile form	NIST CSF 2.0 Organizational Profile template	2	Current and Target	Side-by-side gap form published by NIST [S]
Risk method	ISO 31000:2018 with ISO/IEC 27005:2022	1	every gap	Treatment on the client's own criteria [S]

© 2026 Symbeeo. All rights reserved. · Public

Role	Component (exact name)	Qty	Capacity used	Why this unit
IT discovery	active scan (SNMPv3, SSH read-only) plus the CMDB	2	20 sites, 2 data centers [A]	Two independent sources (SDD-CON-001 §4.1)
Clinical discovery	passive network observation plus the biomedical engineering asset list	2	about 9,000 devices [A]	No active scan on clinical segments (R11)

4 · Design by subsystem

4.1 IT baseline.

Active scan and CMDB reconciled on serial number per site (R2); lifecycle dates from each vendor's own page (R5). Items seen by one source only are findings. The first output the CIO sees is coverage per hospital, so a gap in access shows as a gap, not as a clean estate [A].

4.2 Clinical-device baseline.

Passive observation on a span or tap per campus core, matched to the biomedical engineering list by MAC address (R3). Counted by segment: how many clinical devices share a VLAN with office devices is the number the security domain is ranked on [A]. Rejected: active scanning of clinical segments at low rate — some devices are known to fail under scans, and the result would not change the count enough to justify the risk (R11) [A].

4.3 Interviews.

Sponsor, one delegate per hospital, data-center manager, network manager, information security officer, biomedical engineering lead, service desk, finance [A]. Each interview is scored into the Current Profile against the Subcategories it evidences.

4.4 CSF 2.0 profiles.

Current Profile first, from evidence and interview, then Target Profile set with the CIO on NIST's template (R6). A Subcategory with no evidence is scored as not achieved, not as unknown [A]. Rejected: a questionnaire-only maturity survey — it fails R2 and R5 because nothing is measured (SRA-CON-001 D8).

4.5 Risk register.

Each gap becomes a risk on the group's own likelihood and impact scales (R7); patient-safety impact is a named impact category, set with the group's clinical risk lead [A]. Every risk has an owner below the CIO.

4.6 Ranking the three refreshes.

Each domain is ranked by the risks it would treat (R8): for example, if flat clinical segments and an unsupported campus core carry the highest risks, the network refresh with segmentation ranks first, ahead of a data-center refresh whose risks are availability only [A]. The ranking is the one decision the board is asked for; the roadmap follows from it.

© 2026 Symbeeo. All rights reserved. · Public

5 · Failure behavior

Table 5. Failure behavior

Failure	Behavior	Source
Passive observation not possible at a campus	clinical count for that campus taken from the biomedical list only, marked single-source	[A]
A clinical device misbehaves during the engagement	observation stopped at that campus; incident reported to Level 2 contacts within 24 hours (SDD-CON-001 §6)	[T]
Hospital delegate unavailable	requirements from that site held "open"; sponsor names a replacement	[A]
Reconciliation below 95 % at a site	baseline marked partial for the site; gaps listed	[T]
Target Profile not agreed	ranking issued on the Current Profile gaps alone, with the limitation stated	[A]
Vendor publishes no lifecycle date	item marked "no public date" with the URL	[T]

6 · Limits

- Clinical devices are counted and placed, not tested; their security is out of scope.
- The ranking depends on the group's own risk criteria; different criteria can change the order.
- A CSF 2.0 profile is a statement of outcomes, not a certification.
- The NIS2 note is a finding, not legal advice.
- The baseline is a point in time; the roadmap assumes the CMDB is kept reconciled after handover.

7 · Lessons learned

None yet — this is a design study; populated after the first build against it.

8 · The author

WRITTEN BY

David Morgan

Principal Security Architect

CCISO, CISSP, CISSP-ISSEP, CISM, CISA, CRISC, PMP, CCSP, Adopting Zero Trust (Forrester)

Signed off by Edwin Ozer, Founder.

© 2026 Symbeeo. All rights reserved. · Public

SYMBEEO

Each vendor's tool shows you their option. We show you all of them against one requirement.

Compared. Then Delivered.

hello@symbeeo.com · symbeeo.com

© 2026 Symbeeo. All rights reserved.

Product and company names and logos are their owners' trademarks, shown only to identify the lines Symbeeo sources. Naming a vendor or showing its logo does not mean the vendor sponsors or approves Symbeeo's comparisons or any recommendation Symbeeo makes.

Figures are as published by their sources on the dates given in this document; figures marked [A] are assumptions.

CON-004 · Version 1.1 · Oct 10, 2026