SYMBEEO

PUBLIC

SOLUTION DESIGN DOCUMENT

# Assessment and program-governance design for a typical buyer, applying SRA-CON-001 Model B

Design document (HLD + LLD)

| CAPABILITY | DOCUMENT | VERSION | DATE |
|---|---|---|---|
| Consulting & Engineering | SDD-CON-001 | 1.2 | Oct 10, 2026 |

WRITTEN BY

**David Morgan**, Principal Security Architect



© 2026 Symbeeo. All rights reserved.

## Document control

| | | | |
|---|---|---|---|
| Document | SDD-CON-001 | Version | 1.2 |
| Issued | Oct 10, 2026 | Status | Issued by Symbeeo |
| Classification | Public | Supersedes | 1.1, Oct 7, 2026 |
| Capability | Consulting & Engineering | Author | David Morgan |
| Role | Principal Security Architect | Applies to | SRA-CON-001 v1.1, Model B (assess, specify and govern) |
| Tested by | STP-CON-001 | | |
| 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. | | |
| Sign-off | "The customer's named representative signs this document before the engagement starts; the practice lead signs it after." | | |

## Contents

1 · Introduction 3
2 · Prerequisites 4
3 · Solution overview 4
4 · Assessment design 4
5 · Governance design 6
6 · Evidence, security and lifecycle clauses 6
7 · Engagement plan 7
8 · Roles and deliverables 7

© 2026 Symbeeo. All rights reserved. · Public

CONVENTIONS

The reference architecture applied to one client. Model B is chosen because the typical buyer will buy network, data center and security platforms from different suppliers inside one program (SRA-CON-001 §5); Model A would be a shorter design that stops at the roadmap. Client values are the typical buyer's [A]; the design items follow SRA-CON-001 §4: discovery, cryptographic inventory, requirements, architecture review, security profile and risk, regulation, roadmap, program governance. 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 7, 2026 | 1.1 | §4.7 regime list narrowed to EU and US regimes, as in SRA-CON-001 R10. |
| Oct 10, 2026 | 1.2 | Approval line now reads: approved by the Founder, issued by Symbeeo. David Morgan remains the author. |

# 1 · Introduction

### 1.1 Purpose.

One independent, measured statement of the typical buyer's network, data center and security estate; a requirements register every supplier can be compared against; a sequenced roadmap; and governance of the program that delivers it. **1.2 Goals.** Nothing in the baseline asserted without two sources; no requirement that names a product; every risk owned; every supplier gated on a signed test record. **1.3 Approach.** Current state first, target second, as NIST SP 1301 orders the profiles [S]; requirements before options; governance starts only when the first supplier is contracted.

### 1.4 Change control.

The design here is the agreed scope of the engagement: its sites and domains (R1), deliverables (§8), model and timeline (§7). After this document is signed, any change to that scope is a **written change order** stating what changes, why, and its effect on cost and on schedule, including R13. Both parties sign it before the work it adds is started. A change to a supplier's own design is governed by that supplier's SDD, not by this clause.

### 1.5 Weekly status report.

Issued to the sponsor at the weekly checkpoint (§3.2): % complete per deliverable in §8, slippage against the §7 plan. In Model B the same report covers the governance work and is tabled at the design authority.

### 1.6 Escalation contacts [A].

Listed by role; names are filled in at the scoping workshop.

**Table 2.** Escalation contacts [A]

| Level | Client | Symbeeo |
|---|---|---|
| 1 | domain delegate (P1) | domain architect |
| 2 | sponsor (P1) | engagement lead |
| 3 | sponsor's executive (CIO or head of infrastructure) | practice lead; the Founder for conflict of interest (F5) |

© 2026 Symbeeo. All rights reserved. · Public

# 2 · Prerequisites

**Table 3.** Prerequisites

| # | Prerequisite | Owner | Status |
|---|---|---|---|
| P1 | Named sponsor and a delegate for each of network, data center, security, finance | client | open |
| P2 | Read-only access to the CMDB or source of truth, IPAM, and each hyperscaler tenancy | client | open |
| P3 | Written authorization for active discovery scans, with windows per site | client | open |
| P4 | Current support contracts and renewal dates | client | open |
| P5 | Client's risk criteria (likelihood and impact scales, appetite) | client | open |
| P6 | Workspace in the client's tenancy for evidence (SRA-CON-001 R15) | client | open |
| P7 | Independence declaration signed by every Symbeeo engagement member (R12) | Symbeeo | open |
| P8 | List of regulated entities and sectors in the client group, for R10 | client | open |

# 3 · Solution overview

### 3.1 Components (the engagement entry).

Discovery: active scan plus the client's CMDB, reconciled to ≥ 95 % (R2). Lifecycle: vendor end-of-life pages per item (R3). Cryptography: endpoint scan recorded as a CycloneDX 1.7 CBOM [S] (R4). Security profile: CSF 2.0 Current and Target Organizational Profiles on NIST's template [S] (R5). Requirements: register under 29148 (R6, R7). Architecture review: ATAM steps inside a 42030 evaluation (R8, R16). Risk: ISO 31000 / ISO/IEC 27005 register (R9). Governance: ISO 21503 program controls (R14, R17).

### 3.2 Team and cadence [A].

Engagement lead (the author's role); one architect per domain; an independent reviewer outside the engagement for R6. Weekly checkpoint with the sponsor; fortnightly design authority once suppliers are contracted.

# 4 · Assessment design

### 4.1 Discovery sources and reconciliation [A].

**Table 4.** Discovery sources and reconciliation [A]

| Device class | Source 1 | Source 2 | Reconciled on |
|---|---|---|---|
| switches, routers, firewalls, WLAN controllers | active scan (SNMPv3, SSH read-only) | CMDB / source of truth | serial number |
| servers and hypervisor hosts | hypervisor or BMC inventory | CMDB | serial number |
| cloud resources | provider's own inventory API | tagging standard | resource ID |
| endpoints (count only) | UEM | directory | device ID |
| OT devices | passive network observation | site asset list | MAC address |

© 2026 Symbeeo. All rights reserved. · Public

An item seen by one source only is listed as a finding, not dropped. Coverage reported per site.

### 4.2 Elicitation plan.

Interviews: sponsor, each domain delegate, service desk, finance, risk and compliance, two site managers. Two workshops: business drivers and utility tree (ATAM steps 2 and 5) [S]; requirements read-through.

### 4.3 Requirements register template.

Columns: ID · statement · value · rationale · source (interview or document) · priority (must / should / may) · verification method (inspection, analysis, demonstration, test) · owner · status. Each row reviewed by the independent reviewer against the 29148 characteristics before release (R6). A product or vendor name fails the row.

### 4.4 Quality-attribute scenarios [A].

Six of the ≥ 12 required by R8, proposed for the utility-tree workshop; values confirmed there.

**Table 5.** Quality-attribute scenarios [A]

| # | Attribute | Stimulus | Response measure | Feeds |
|---|---|---|---|---|
| Q1 | Availability | one data center lost | business services restored at the other ≤ 4 h | SRA-DC-001 |
| Q2 | Availability | branch WAN link lost | branch users keep SaaS access ≤ 60 s | SRA-NET-001 |
| Q3 | Security | user disabled in the directory | all access lost ≤ 5 min | SRA-SEC-001 R11 |
| Q4 | Modifiability | a fourth branch opens | in service ≤ 10 working days, no core redesign | SRA-NET-001 |
| Q5 | Cryptographic agility | a quantum-vulnerable algorithm must be withdrawn | replaced on external endpoints ≤ 90 days | R4 |
| Q6 | Operability | a supplier's platform fails | fault isolated to one supplier ≤ 30 min from telemetry | R14 |

### 4.5 Security profile and risk.

CSF 2.0 Current Profile scored per Subcategory from evidence and interview; Target Profile set with the sponsor; each gap entered as a risk on the client's criteria (P5), with owner and treatment (avoid, mitigate, transfer, accept). Where zero trust is in scope, the CISA ZTMM v2.0 stage per pillar is recorded and passed to SDD-SEC-001.

### 4.6 Cryptographic inventory.

External endpoints first, then internal management planes. Each quantum-vulnerable entry (RSA, ECDH, ECDSA) carries its IR 8547-draft horizon, set by its security strength (112 bits: deprecated after 2030, disallowed after 2035; 128 bits or more: disallowed after 2035; draft, not final on Sep 27, 2026; SRA-CON-001 §4.2) and a proposed ML-KEM / ML-DSA replacement path, hybrid where the platform supports it [S].

### 4.7 Regulatory applicability.

From P8: every regime on SRA-CON-001 R10's list (EU: NIS2, DORA, the Cyber Resilience Act, EU GMP Annex 11; US: NERC CIP, TSA security directives, HIPAA, PCI DSS v4.0.1, NYDFS 500, FFIEC, SEC 17a-4 and Regulation S-P, CJIS, FedRAMP/GovRAMP, Section 508, NDAA §889, 21 CFR Part 11, CMMC with NIST SP 800-171, AWIA §2013 (SDWA §1433)) marked applicable or not, one sentence of basis each; CRA supplier questions carried into the comparison.

© 2026 Symbeeo. All rights reserved. · Public

# 5 · Governance design

### 5.1 Design authority.

Chair: client sponsor. Members: client domain delegates, each supplier's lead architect, Symbeeo engagement lead as secretary and independent reviewer. Decisions recorded in the decision log with date, options considered and dissent.

### 5.2 Stage gates [A].

Each gate opens only on its signed evidence record (SRA-CON-001 R17).

**Table 6.** Stage gates [A]

| Gate | Opens when | Evidence |
|---|---|---|
| G0 | baseline and register signed | this document's §4 outputs |
| G1 | comparison issued; suppliers contracted | comparison record |
| G2 | each supplier's SDD signed | SDD-NET-001, SDD-DC-001, SDD-SEC-001 |
| G3 | each supplier's STP signed as passed | STP-NET-001, STP-DC-001, STP-SEC-001 |
| G4 | roadmap horizon 1 closed; lessons recorded | RAID log closed items |

### 5.3 Logs.

One integrated plan and one RAID log across suppliers (R14); items dated, owned, and reviewed at every design authority. **5.4 Interfaces.** Every supplier-to-supplier boundary (for example, access switch to policy engine, DC fabric to firewall) gets a numbered interface agreement: owner each side, protocol, test case in the relevant STP.

# 6 · Evidence, security and lifecycle clauses

The engagement builds nothing and installs nothing, so the clauses below apply to the buyer's data it handles and to the recommendations it makes, as follows.

- **Evidence location.** Raw scans, CBOM, interview notes and working registers live in the client's workspace (P6); Symbeeo copies are deleted ≤ 30 days after acceptance and the deletion is recorded (R15). No client data enters a Symbeeo publication; a comparison published later carries requirements and results, not the client's inventory.
- **Security incidents.** A security incident affecting the client's data or systems that arises from, or is discovered during, the engagement is reported to the Level 2 contacts (§1.6) **within 24 hours of discovery**.
- **Media sanitization.** Any Symbeeo storage medium that held client data (laptop drive, removable media) is sanitized to **NIST SP 800-88 Rev. 2** (final, September 2025) [S] before it leaves engagement use, with a certificate per device, filed with the deletion record.
- **End-of-sale and end-of-support.** Symbeeo quotes no equipment in this engagement (R12). Where the roadmap or the comparison recommends equipment, no item past its vendor's end-of-sale date is recommended, and the end-of-sale and end-of-support dates of every item are shown, from the vendor's own page (R3).
- **Support level by severity.** Symbeeo quotes no vendor support. The comparison requires every supplier's quote to state the vendor support level by severity (response time for severity 1 to 4), so that the clause reaches the quotes the client will sign.

© 2026 Symbeeo. All rights reserved. · Public

- **Handover pack**, at G0 (Model A) or G4 (Model B): the deliverables of §8 in their signed versions; the register version and hash handed to the comparison; the discovery and CBOM data in the client's workspace; every access granted for the engagement (P2, P3) listed and confirmed revoked, and any credential issued to Symbeeo returned or disabled; licenses bought for the engagement, if any, transferred or closed; the signed STP-CON-001; open items from the RAID log with owners. As-built drawings do not apply: nothing is built.

## 7 · Engagement plan

Table 7. Engagement plan

| Step | Action | Rollback |
|---|---|---|
| 1 | Scoping workshop; P1–P8 closed; independence declarations signed | engagement not started |
| 2 | Discovery and reconciliation, weeks 1–2; coverage reported per site | re-scan in the next window |
| 3 | Interviews, utility-tree workshop, CSF Current Profile, weeks 1–3 | delegate named (F3) |
| 4 | Register, review, risk register, roadmap; report ≤ 20 working days (R13) | rows held "open", not guessed |
| 5 | G0 signed; register handed to the comparison | register revised only by change order (§1.4) |
| 6 | Governance from G1 to G4; STP-CON-001 run at G0 and at G4 | gate stays closed |

## 8 · Roles and deliverables

Design authority: the client's sponsor and the practice lead (both sign). Deliverables: this document · STP-CON-001 with results · baseline inventory and CBOM · requirements register · CSF 2.0 profiles · risk register · roadmap · decision and RAID logs · weekly status reports (§1.5) · handover pack (§6) · acceptance certificate.

© 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.

SDD-CON-001 · Version 1.2 · Oct 10, 2026