SYMBEEO

PUBLIC

REFERENCE ARCHITECTURE

# Infrastructure assessment, requirements and program governance on 2026 standards: two engagement models

| CAPABILITY | DOCUMENT | VERSION | DATE |
| --- | --- | --- | --- |
| Consulting & Engineering | SRA-CON-001 | 1.4 | Nov 6, 2026 |

WRITTEN BY

**David Morgan**, Principal Security Architect



© 2026 Symbeeo. All rights reserved.

## Document control

| | | | |
|---|---|---|---|
| Document | SRA-CON-001 | Version | 1.4 |
| Issued | Nov 6, 2026 | Status | Issued by Symbeeo |
| Classification | Public | Supersedes | 1.3, Nov 4, 2026 |
| Capability | Consulting & Engineering | Author | David Morgan |
| Role | Principal Security Architect | 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 (version 1.2). Version 1.4 issued by Symbeeo, Nov 6, 2026. | | |
| Sign-off | "The practice lead signs this document before any engagement proceeds under it." | | |

## Contents

1 · Scope 3
2 · Requirements register 3
3 · Architecture overview 5
4 · Component design — written as standards entries [S] 6
5 · Options and platform choices 7
6 · Failure conditions 8
7 · Validation 8
8 · Operations and lessons learned 9
9 · Appendix 9

© 2026 Symbeeo. All rights reserved. · Public

CONVENTIONS

**Source tags.** [S] read Sep 24, 2026 from the standards body or publisher; full list with URLs in §9. The anchor is ISO/IEC/IEEE 29148:2018, still the current edition (revision P29148 under an IEEE PAR approved Sep 10, 2025). [A] typical-buyer assumption, to be confirmed at the scoping workshop. No product is required by this document; tools appear in §5 as options. 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 | R10's check list narrowed to EU and US regimes; the §9.1 rows outside them removed. |
| Oct 10, 2026 | 1.2 | Approval line now reads: approved by the Founder, issued by Symbeeo. David Morgan remains the author. |
| Nov 4, 2026 | 1.3 | Scope line, D1 and D9 reworded. |
| Nov 6, 2026 | 1.4 | R12 and D9 reworded: vendor commissions, rebates and incentives are declared before discovery. |

## 1 · Scope

**Who it is for.** The CIO or head of infrastructure about to run a multi-vendor comparison, or already running a program with three or more suppliers, who needs one independent statement of what exists, what is required, what is at risk and in what order to act — written so every vendor is tested against the same requirement.

**Typical buyer [A].** The SRA-NET-001 client: 1,500 users at HQ, 3 branches, 2 data centers 40 km apart, two hyperscaler tenancies, 30 % remote workforce; network, data center and security estates due for refresh between 2026 and 2029; an incumbent CMDB of unknown accuracy.

**What is in.** Current-state assessment (discovery, lifecycle, cryptography, contracts); requirements engineering; architecture and risk review; regulatory applicability; a costed, sequenced roadmap; governance of the multi-vendor program that delivers it. **What is out.** Detailed design of any practice (SRA-NET-001, SRA-DC-001, SRA-SEC-001 own that); penetration testing; legal opinion on regulation; staff augmentation.

**Related documents.** SDD-CON-001 (this architecture applied to the typical buyer) · STP-CON-001 (its test plan) · SRA-NET-001, SRA-DC-001, SRA-SEC-001 (the designs this work feeds) · the standards in the source tags [S].

## 2 · Requirements register

Every requirement row (R2–R17) is written to pass the ISO/IEC/IEEE 29148:2018 test the register itself imposes (R6): verifiable, unambiguous, singular, implementation-free. R1 is the scope input those rows are measured within.

© 2026 Symbeeo. All rights reserved. · Public

**Table 2.** Requirements register

| # | Requirement | Value | Source |
|---|---|---|---|
| R1 | Assessment scope — **input**, a scope statement: it bounds R2–R17 and is checked by inspection against the signed scoping record, not tested as a requirement | HQ · 3 branches · 2 DCs · 2 hyperscaler tenancies; domains network, data center, security | [A] |
| R2 | Inventory coverage | ≥ 95 % of in-scope IP-addressable devices reconciled across two independent sources | [A] |
| R3 | Lifecycle status | 100 % of reconciled hardware and software items carry the vendor's published end-of-sale and end-of-support dates, or "no public date" with the URL searched | [A] |
| R4 | Cryptographic inventory | 100 % of externally reachable TLS, SSH and IPsec endpoints recorded with algorithm and key size; each quantum-vulnerable entry dated by its security strength against the IR 8547 initial public draft (not final on Sep 27, 2026): at 112 bits, deprecated after 2030 and disallowed after 2035; at 128 bits or more, disallowed after 2035 | [S] IR 8547 ipd, Tables 2 and 4; FIPS 203/204/205 |
| R5 | Security posture baseline | Current and Target Organizational Profile at all 106 CSF 2.0 Subcategories; gap stated per Subcategory | [S] CSWP 29; SP 1301 |
| R6 | Requirement quality | 100 % of requirements in the delivered register meet the 29148:2018 characteristics of an individual requirement; zero name a product or vendor | [S] 29148 |
| R7 | Traceability | each requirement traces to one stakeholder need and one verification method (inspection, analysis, demonstration or test) | [S] 29148 |
| R8 | Architecture review | ≥ 12 quality-attribute scenarios, each with a stimulus and a measurable response | [S] ATAM; 42030 |
| R9 | Risk register | each risk carries likelihood, impact, owner and treatment on the client's own risk criteria | [S] ISO 31000:2018; ISO/IEC 27005:2022 |

© 2026 Symbeeo. All rights reserved. · Public

| # | Requirement | Value | Source |
|---|---|---|---|
| R10 | Regulatory applicability | each regime on the check list marked applicable or not applicable, with the basis in one sentence. Check list: EU: NIS2, DORA, the Cyber Resilience Act, EU GMP Annex 11 · US: NERC CIP, TSA security directives, HIPAA Security Rule, PCI DSS v4.0.1, NYDFS 23 NYCRR 500, FFIEC IT Examination Handbook, SEC Rule 17a-4 and Regulation S-P, CJIS Security Policy, FedRAMP / GovRAMP, Section 508, NDAA §889, 21 CFR Part 11, CMMC with NIST SP 800-171, AWIA §2013 (SDWA §1433). A regime not on this list is outside the check list | [S] EUR-Lex; European Commission; US issuers, read Sep 25, 2026 and Sep 27, 2026 (§9.1) |
| R11 | Roadmap | every item in one of three horizons (0–6, 6–18, 18–36 months), linked to ≥ 1 gap ID and ≥ 1 requirement ID | [A] |
| R12 | Independence | assessor declares, before discovery starts, any commission, rebate or incentive from a vendor in scope | [A] Symbeeo policy |
| R13 | Turnaround | assessment report issued ≤ 20 working days after discovery access is granted | [A] |
| R14 | Program control (Model B) | one integrated plan, one RAID log and one decision log across all suppliers | [S] ISO 21503:2022 |
| R15 | Evidence handling | raw discovery data and interview notes held in the client's tenancy; Symbeeo copies deleted ≤ 30 days after acceptance | [A] |
| R16 | Review findings traced | every risk, sensitivity point and trade-off recorded against one of the R8 scenarios | [S] ATAM; 42030 |
| R17 | Stage-gate evidence (Model B) | each stage gate passed only on its signed evidence record (SDD-CON-001 §5.2); a supplier's work accepted (G3) only on that supplier's signed STP acceptance record | [S] ISO 21503:2022 |

## 3 · Architecture overview

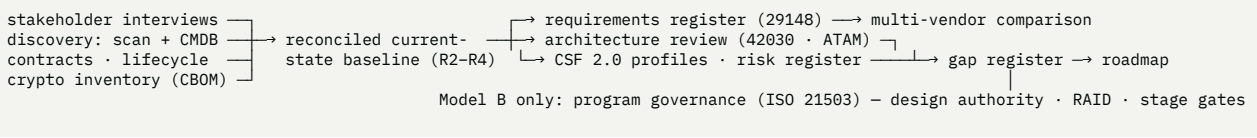



**Figure 1.** Assessment and governance flow

Model A stops at the roadmap; Model B adds the bottom line and runs through delivery.

© 2026 Symbeeo. All rights reserved. · Public

## 4 · Component design — written as standards entries [S]

**Model A · Assess and specify.** Work packages: discovery and baseline; stakeholder elicitation; requirements register; architecture review; security profile and risk register; regulatory applicability; roadmap. Governing standards: ISO/IEC/IEEE 29148:2018, 42010:2022, 42030:2019; NIST CSF 2.0 with SP 1301; ISO 31000:2018; ISO/IEC 27005:2022; FIPS 203/204/205 and IR 8547 (draft) for the cryptographic horizon. Ends with a signed requirements register that any vendor can be compared against.

**Model B · Assess, specify and govern.** Model A plus program governance through multi-vendor delivery: design authority, integrated plan, RAID and decision logs, stage gates bound to the practice test plans (STP-NET-001, STP-DC-001, STP-SEC-001). Adds ISO 21503:2022 (program management) and the PMBOK Guide 8th ed. for the projects inside it.

**Substitution rule [A].** The standards are fixed per model; the tools that produce the evidence are the client's incumbents where they reach the R2 coverage, and a Symbeeo working store otherwise (§5).

### 4.1 Discovery and baseline.

Two independent sources per device class — an active scan and the incumbent CMDB or source of truth — reconciled to R2; lifecycle dates from the vendor's own end-of-life pages (R3); support entitlements per item.

### 4.2 Cryptographic inventory.

Endpoint scan for protocols, algorithms and key sizes, recorded in a machine-readable cryptography bill of materials (CycloneDX 1.7 CBOM, adopted as ECMA-424 2nd ed. in December 2025) [S]. Every quantum-vulnerable item gets a replacement horizon from the IR 8547 draft dates (R4). FIPS 203 (ML-KEM), 204 (ML-DSA) and 205 (SLH-DSA) are the target algorithms, final since August 2024 [S]. The IR 8547 dates depend on security strength: RSA, ECDSA, finite-field and elliptic-curve Diffie-Hellman at 112 bits are deprecated after 2030 and disallowed after 2035; at 128 bits or more they are disallowed after 2035, with no deprecation step. IR 8547 is still the initial public draft of November 12, 2024 (comments closed January 10, 2025; no final on Sep 27, 2026), so every date it gives is a proposal and is checked again before each issue [S] (`https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf`, Tables 2 and 4, read Sep 27, 2026). The tables name security strengths, not key sizes; mapping a key size to a strength (for example RSA-2048 to 112 bits) uses NIST SP 800-57 Part 1 [A].

### 4.3 Requirements engineering.

Elicitation by interview and workshop; each requirement written, then tested against the 29148 characteristics by a second architect before the client sees it (R6). Attributes per row: ID, statement, value, rationale, source, priority, verification method (R7). A product name in a requirement fails the row.

### 4.4 Architecture review.

A 42030-conformant evaluation using the ATAM steps: business drivers, utility tree, quality-attribute scenarios, analysis of the current architecture's approaches (R8), then risks, non-risks, sensitivity points and trade-offs, each tied to a scenario (R16) [S]. Views follow 42010:2022 (stakeholders, concerns, viewpoints), not a vendor's diagram set.

### 4.5 Security profile and risk.

CSF 2.0 Current and Target Organizational Profiles on NIST's own template (R5); gaps entered as risks and treated per ISO 31000 and ISO/IEC 27005 (R9). Where the client's scope includes zero trust, the CISA Zero Trust Maturity Model v2.0 stage per pillar is recorded and handed to SRA-SEC-001.

© 2026 Symbeeo. All rights reserved. · Public

### 4.6 Regulatory applicability.

One line per regime (R10): NIS2 (Directive (EU) 2022/2555); DORA (applied since January 17, 2025); the Cyber Resilience Act (reporting from September 11, 2026, main obligations from December 11, 2027), which lands on suppliers and so becomes a question in every comparison [S]. The same one-line check covers EU GMP Annex 11 and the US regimes on R10's list (sources in §9.1); a regime that does not apply is marked so, not dropped. A finding, not legal advice.

### 4.7 Roadmap and cost.

Gaps sequenced into three horizons (R11); each item costed as a band and tagged to the FinOps Framework 2025 scope it spends in — public cloud, SaaS, data center, licensing or AI [S] — so that the comparison, not the roadmap, sets the price.

### 4.8 Program governance (Model B).

Design authority chaired by the client, Symbeeo as secretary and independent reviewer; one integrated plan and one RAID log across suppliers (R14); interface control between suppliers recorded as numbered interface agreements; stage gates open only on a signed evidence record, and a supplier's work is accepted only on its signed STP acceptance record (R17).

## 5 · Options and platform choices

One row per decision. No row is decided by a published comparison: this engagement produces the comparison, so no row carries [CMP].

**Table 3.** Options and platform choices

| ID | Decision | Requirement | Alternatives considered | Decision taken | Rationale |
|---|---|---|---|---|---|
| D1 | Engagement model | R1, R13, R14, R17 | Model A, assess and specify (one phase) · Model B, assess, specify and govern (adds monthly governance) | **Model A** where the client runs its own delivery; **Model B** for three or more suppliers | A ends at a comparable requirement and meets §2 with R14 and R17 n/a; B adds ISO 21503 control across suppliers [S] |
| D2 | Source of truth for the baseline | R2, R3 | client CMDB (e.g. ServiceNow on CSDM 5) · NetBox 4.6 · client IPAM · Symbeeo working store | incumbent first, where it reaches R2; Symbeeo working store otherwise | Substitution rule (§4) [A]; CSDM 5 published May 2025 [S]; cost band: license held or open source |
| D3 | Network model and assurance tooling | R2 | IP Fabric · Forward Networks · vendor controllers · none (scan and CMDB alone) | per client; optional | Speeds R2, not required by it [A]; cost band: subscription |
| D4 | Architecture evaluation method | R8, R16 | full ATAM (3–4 days of workshop) · ISO/IEC/IEEE 42030 lightweight review | **ATAM for Model B; 42030 lightweight review for Model A** | Both meet R8; the utility tree forces measurable scenarios [S] |
| D5 | Architecture description framework | R8, R16 | ISO/IEC/IEEE 42010:2022 views · full TOGAF 10 ADM | **42010 views**; TOGAF only where the client already uses it | 42010 views suffice for §2; TOGAF is not needed for it and its cost band is high [A] |
| D6 | Security lens | R5, R9 | NIST CSF 2.0 · ISO/IEC 27001:2022 Annex A · CISA ZTMM v2.0 | **CSF 2.0 always**; the others mapped where the client holds them | R5 names CSF 2.0 [S] |

© 2026 Symbeeo. All rights reserved. · Public

| ID | Decision | Requirement | Alternatives considered | Decision taken | Rationale |
|---|---|---|---|---|---|
| D7 | Service and cloud lenses | none required by §2 (option; serves the R1 tenancies) | ITIL (Version 5) · ITIL 4 · AWS, Azure, Google Cloud Well-Architected | the client's adopted ITIL; each provider's own framework per tenancy | ITIL 5 launched 2026 with ITIL 4 alongside in transition [S] |
| D8 | Assessment method | R2, R3, R4 | measured baseline (scan and two sources) · questionnaire-only assessment (lowest cost band) | **measured baseline** | Questionnaire-only fails R2, R3 and R4: nothing is measured |
| D9 | Vendor money and the assessor | R12 | every commission, rebate or incentive from a vendor in scope declared · none declared | **every one declared before discovery** | An undeclared commission, rebate or incentive from a vendor in scope fails R12 [A] Symbeeo policy |

## 6 · Failure conditions

**Table 4.** Failure conditions

| # | Condition | What the client sees | Recovers by itself | Needs a hand | Time |
|---|---|---|---|---|---|
| F1 | Discovery source unavailable or blocked | coverage below R2 | no | second source or access change | days |
| F2 | Reconciliation below 95 % after two passes | baseline marked partial; gaps listed by site | no | client asset owner | R13 at risk |
| F3 | Stakeholder unavailable for elicitation | requirement held as "open", not guessed | no | sponsor names a delegate | ≤ 5 working days |
| F4 | Vendor publishes no lifecycle date | item marked "no public date" with URL (R3) | yes, by rule | vendor query logged | 0 |
| F5 | Conflict of interest found after start | engagement paused; declaration re-issued | no | Founder decision | immediate |
| F6 | Scope change mid-engagement | written change order with its cost and schedule effect, including on R13 (SDD-CON-001 §1.4) | no | both parties sign before the work starts | days |
| F7 | Supplier misses a stage gate (Model B) | gate stays closed; RAID escalation | no | design authority | per plan |

## 7 · Validation

None yet. On the first engagement, measure R2 reconciliation and have an architect outside the engagement re-test a sample of requirements against R6; record both here.

© 2026 Symbeeo. All rights reserved. · Public

## 8 · Operations and lessons learned

From the sources [S]: build the Current Profile before the Target; the ATAM utility tree is where "highly available" becomes a number; 29148 is under revision, so check its status before each issue. Symbeeo lessons: to be written by the signing engineer.

## 9 · Appendix

All read Sep 24, 2026. ISO/IEC/IEEE 29148:2018 — https://www.iso.org/standard/72089.html · IEEE P29148 PAR — https://standards.ieee.org/ieee/29148/12262/ · ISO/IEC/IEEE 42010:2022 — https://www.iso.org/standard/74393.html · SEI ATAM — https://www.sei.cmu.edu/documents/629/2000_005_001_13706.pdf · NIST CSF 2.0 — https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf · CSF 2.0 Profiles — https://www.nist.gov/cyberframework/profiles · SP 1301 — https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1301.pdf · ISO 31000 revision — https://www.iso.org/standard/88574.html · NIST IR 8547 ipd — https://csrc.nist.gov/pubs/ir/8547/ipd · CycloneDX 1.7 — https://cyclonedx.org/news/cyclonedx-v1.7-released/ · ECMA-424 2nd ed. — https://ecma-international.org/publications-and-standards/standards/ecma-424/ · CISA ZTMM v2.0 — https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model · ISO 21503:2022 — https://www.iso.org/standard/82868.html · PMBOK Guide 8th ed. — https://www.pmi.org/standards/pmbok · ITIL (Version 5) — https://www.peoplecert.org/news-and-announcements/itil-version-5-explained · FinOps Framework 2025 — https://www.finops.org/insights/2025-finops-framework/ · CSDM 5 — https://www.servicenow.com/community/common-service-data-model/csdm-5-finally-get-the-csdm-5-white-paper-here/ta-p/3254967 · NetBox 4.6 — https://github.com/netbox-community/netbox/releases/tag/v4.6.4 · TOGAF 10th ed. — https://blog.opengroup.org/2025/07/01/navigating-the-togaf-standard-10th-edition-updates-and-insights/ · AWS Well-Architected — https://docs.aws.amazon.com/wellarchitected/2025-02-25/framework/conclusion.html · Azure Well-Architected — https://learn.microsoft.com/en-us/azure/well-architected/pillars · Google Cloud Well-Architected — https://docs.cloud.google.com/architecture/framework · NIS2 — https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng · DORA — https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng · Cyber Resilience Act — https://digital-strategy.ec.europa.eu/en/policies/cra-reporting · NIST SP 800-88 Rev. 2 (final, September 2025; supersedes Rev. 1) — https://csrc.nist.gov/pubs/sp/800/88/r2/final.

### 9.1 · Industry rules this architecture helps a buyer meet.

From Symbeeo's industry research of September 2026. Only rules that research links to this document's requirements are listed, and every rule listed is also on R10's check list. Rules that research found this document does not address are left out of this table and are outside R10's check list: the engagement neither marks them nor assesses them. Where a listed rule is covered in part, the part not addressed is named in its row and is likewise outside the check list.

**Table 5.** Industry rules this architecture helps a buyer meet

| Rule | Jurisdiction | What it asks of infrastructure | Requirements here | Coverage |
|---|---|---|---|---|
| NYDFS 23 NYCRR Part 500, Second Amendment (Nov 2023; last phase in force Nov 1, 2025) | US · New York · DFS-regulated financial entities | §500.13 written asset inventory | R2 (with SRA-SEC-001 R3) | full |
| America's Water Infrastructure Act 2018 §2013 (SDWA §1433) | US · community water systems serving more than 3,300 people | risk and resilience assessment covering electronic, computer and automated systems, recertified every 5 years | R9 | partial |

© 2026 Symbeeo. All rights reserved. · Public

| Rule | Jurisdiction | What it asks of infrastructure | Requirements here | Coverage |
|---|---|---|---|---|
| 21 CFR Part 11 (electronic records; electronic signatures) | US · FDA-regulated records | validated systems, with validation traceable to requirements | R7 | partial |
| EU GMP Annex 11 Computerized Systems (2011 revision in force; the revised draft consulted Jul 7 to Oct 7, 2025 is not adopted on Sep 27, 2026) | EU · medicinal-product manufacturers | validation traceable to user requirements | R7 | partial |

Naming a rule here is not a claim of compliance or certification: the buyer's assessor decides compliance, and Symbeeo holds no certification or authorization.

**Sources for §9.1, read Sep 25, 2026:** 23 NYCRR 500 [S] https://www.dfs.ny.gov/cybersecurity/23-NYCRR-Part-500 · amended text [S] https://www.dfs.ny.gov/system/files/documents/2023/10/rf_fs_2amend23NYCRR500_text_20231101.pdf · AWIA §2013 [S] https://www.epa.gov/waterresilience/awia-section-2013 · 21 CFR Part 11 [S] https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11 (text read on the eCFR) · EudraLex Volume 4, Annex 11 [S] https://health.ec.europa.eu/medicinal-products/eudralex/eudralex-volume-4_en.

**Further sources, read Sep 27, 2026:** Annex 11 revised-draft consultation, closed [S] https://health.ec.europa.eu/consultations/stakeholders-consultation-eudralex-volume-4-good-manufacturing-practice-guidelines-chapter-4-annex_en · NIST IR 8547 ipd, Tables 2 and 4 [S] https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf.

**Sources for the other regimes on R10's check list, read Sep 25, 2026:** NERC CIP standards [S] https://www.nerc.com/standards/reliability-standards/cip/cip-013-2 · TSA pipeline security directives [S] https://www.tsa.gov/sd-and-ea · HIPAA Security Rule [S] https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202510&RIN=0945-AA22 · PCI DSS v4.0.1 [S] https://www.pcisecuritystandards.org/document_library/ · FFIEC BCM booklet [S] https://www.occ.treas.gov/news-issuances/bulletins/2019/bulletin-2019-57.html · SEC Rule 17a-4 [S] https://www.federalregister.gov/documents/2022/11/03/2022-22670/electronic-recordkeeping-requirements-for-broker-dealers-security-based-swap-dealers-and-major · SEC Regulation S-P, 2024 amendments, all entities in compliance from Jun 3, 2026 [S] https://www.sec.gov/files/rules/final/2024/regulation-s-p-small-entity-compliance-guide.pdf · CJIS Security Policy v6.1 [S] https://le.fbi.gov/file-repository/cjis_security_policy_v6-1_20260625.pdf · FedRAMP Consolidated Rules for 2026, effective Jul 4, 2026 [S] https://www.fedramp.gov/2026/providers/updating/changes/ · GovRAMP, the operating name of StateRAMP since Feb 14, 2025 [S] https://govramp.org/news/blog/stateramp-announces-rebrand-to-govramp-reflecting-mission-to-unite-public-and-private-sectors-in-advancing-cybersecurity · Section 508 [S] https://www.access-board.gov/ict/ · NDAA §889 [S] https://www.acquisition.gov/far/52.204-25 · 21 CFR Part 11 [S] https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11 · CMMC, 32 CFR Part 170 (assesses against NIST SP 800-171 Rev. 2) [S] https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170 · DFARS rule, effective Nov 10, 2025 [S] https://www.federalregister.gov/documents/2025/09/10/2025-17359/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of-cybersecurity-requirements · NIST SP 800-171 Rev. 3 [S] https://csrc.nist.gov/pubs/sp/800/171/r3/final · AWIA §2013 [S] https://www.epa.gov/waterresilience/awia-section-2013.

© 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.

SRA-CON-001 · Version 1.4 · Nov 6, 2026