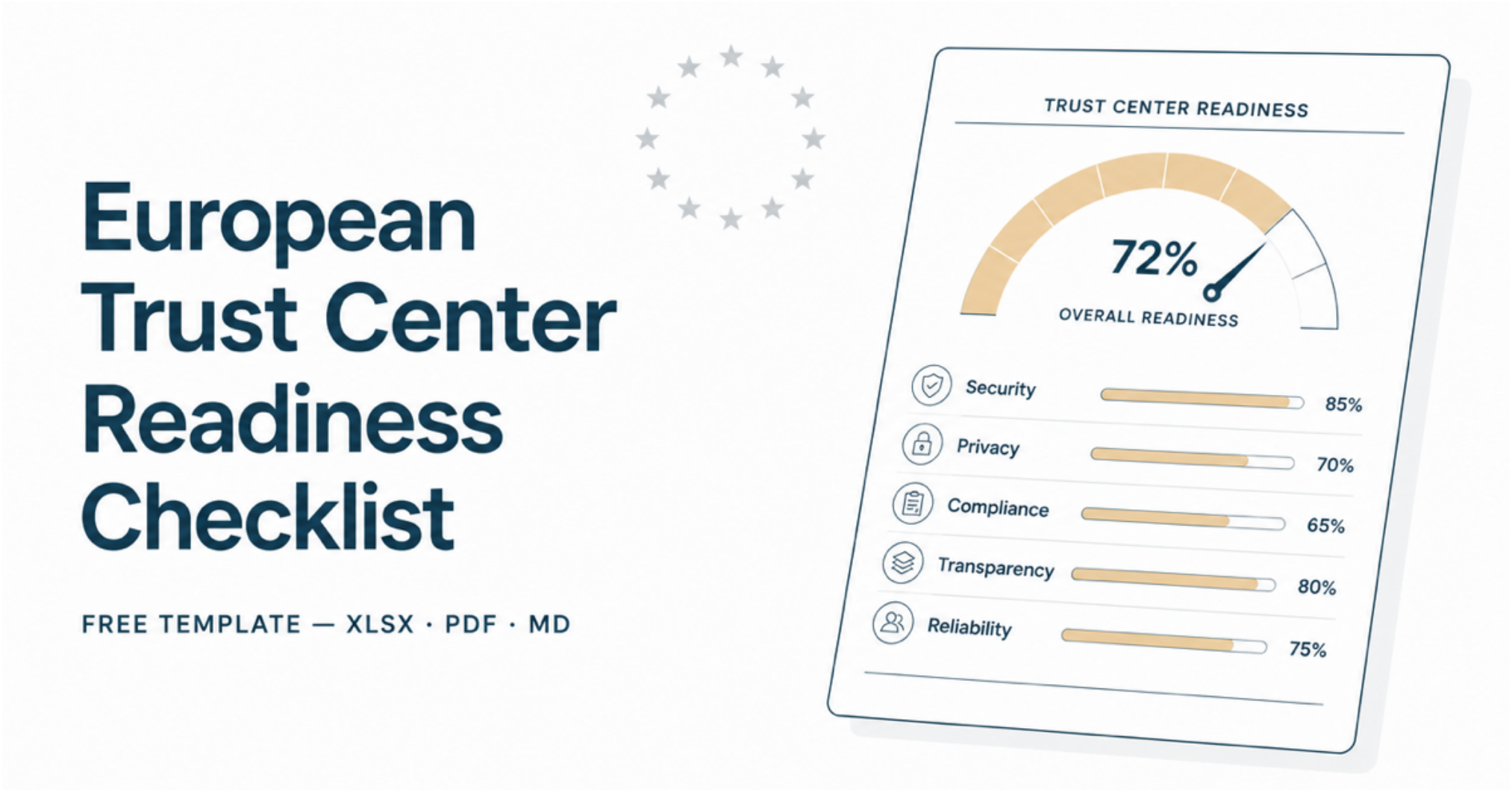

European Trust Center Readiness Checklist

Version 1.0 · Updated 2026-07-03 · Free template · orbiqhq.com/templates/european-trust-center-readiness-checklist

Instructions

European Trust Center Readiness Checklist — Instructions
A scored self-assessment of your buyer-facing trust center against European expectations: 58 line items across six stakeholder lanes.
HOW TO SCORE
1. Assess from the outside: score what an external reviewer can find on the trust center (public + self-serve gated tiers), not what exists internally.
2. Score every line item in the Score column: Yes = 2 points (published, current, complete, accessible at the right tier); Partial = 1 point (exists but stale >12 months, incomplete, hard to find, or gated where it should be public); No = 0 points (absent or unfindable).
3. The Points column and the Scorecard sheet compute per-lane scores, the total percentage, and your readiness band automatically.
READINESS BANDS
Below 40% — Foundational: the trust center is a brochure; reviewers fall back to email-a-PDF. Fix the two weakest lanes first.
40–75% — Developing: core evidence exists but at least two lanes are underserved; prioritise legal transparency and update channels.
Above 75% — Buyer-ready: all six lanes self-serve; security review runs parallel to the deal. Maintain with quarterly re-scores.
LANE OWNERS (RECOMMENDED)
Lane 1 Security teams — Security lead / CISO · Lane 2 Legal teams — Legal / DPO · Lane 3 Compliance teams — Compliance / GRC lead · Lane 4 Procurement — Sales / RevOps · Lane 5 Customer updates — Customer success · Lane 6 AI agents — Engineering / web team. One coordinator (usually the CISO or compliance lead) consolidates the Scorecard.
CADENCE
Run all six lanes quarterly. Re-score a single lane after any material change: new certificate or audit, subprocessor change, incident, pricing change, endpoint change. Subprocessor lists and certificate validity decay fastest — check monthly.
LEGAL ANCHORS
NIS2 — Directive (EU) 2022/2555 (Art. 21(2)(d) supply-chain security; Art. 23 incident reporting: 24h / 72h / 1 month) — https://eur-lex.europa.eu/eli/dir/2022/2555
DORA — Regulation (EU) 2022/2554 (Art. 28–30 ICT third-party risk), applicable since 17 Jan 2025 — https://eur-lex.europa.eu/eli/reg/2022/2554
GDPR — Regulation (EU) 2016/679 (Art. 28 subprocessors; Art. 32 security; Art. 33–34 breach notification) — https://eur-lex.europa.eu/eli/reg/2016/679
This checklist is provided as-is and is not legal advice. Free to use and adapt within your organisation.

1 Security teams

Lane owner: Security lead / CISO

ID	Line item	What good looks like	Evidence example	Score	Points	Orbiq module	Notes / owner
SEC-01	ISO 27001 certificate published	Certificate visible with certification body, scope statement, issue and expiry dates — not just a badge	PDF or evidence card: "ISO/IEC 27001:2022, issued by [body], valid to 2027-03-01, scope: SaaS platform and supporting infrastructure"			Trust Center Platform (/platform/trust-center-platform)	
SEC-02	Statement of Applicability available on request	SoA (or control summary) accessible through a self-serve gated flow with a stated turnaround	NDA-gated "Statement of Applicability v4.2, 2026-01" in the restricted tier			Integrated NDA Flow (/platform/integrated-nda-flow)	
SEC-03	Penetration test executive summary, last 12 months	Dated summary naming the testing firm, scope, methodology, finding counts by severity, and remediation status	"External pentest by [firm], 2026-04; 0 critical, 2 high (remediated 2026-05)"			Document Watermarking (/platform/document-watermarking)	
SEC-04	Vulnerability management posture	Scanning cadence, patching SLAs, and remediation timelines for critical/high findings stated	"Weekly dependency and infra scans; criticals patched ≤ 72h, highs ≤ 14 days"			Trust Center Platform (/platform/trust-center-platform)	
SEC-05	Encryption posture documented	Encryption at rest and in transit with algorithms and key-management summary	"AES-256 at rest, TLS 1.2+ in transit, KMS-managed keys rotated annually"			Trust Center Platform (/platform/trust-center-platform)	
SEC-06	Access management summary	MFA/SSO enforcement, least-privilege model, joiner-mover-leaver process described	"SSO + enforced MFA for all staff; quarterly access reviews; RBAC"			Trust Center Platform (/platform/trust-center-platform)	

ID	Line item	What good looks like	Evidence example	Score	Points	Orbiq module	Notes / owner
SEC-07	Secure development lifecycle described	Code review, SAST/DAST, dependency scanning, and release controls summarised	"All changes peer-reviewed; SAST + dependency scanning in CI; staged deploys"			Trust Center Platform (/platform/trust-center-platform)	
SEC-08	Tenant/network segregation explained (multi-tenant SaaS)	Logical separation model between customer environments described	"Row-level tenancy isolation; per-tenant encryption contexts; no cross-tenant queries"			Trust Center Platform (/platform/trust-center-platform)	
SEC-09	Business continuity / disaster recovery summary	BC/DR plan summary with RTO/RPO targets and last test date	"RTO 4h / RPO 1h; DR exercise last run 2026-02"			Trust Center Platform (/platform/trust-center-platform)	
SEC-10	Security architecture overview	High-level architecture description or diagram (public or gated) covering data flows and boundaries	Gated "Architecture & data-flow overview, v3, 2026-03"			Integrated NDA Flow (/platform/integrated-nda-flow)	
SEC-11	Responsible disclosure route	security.txt and/or a published vulnerability disclosure policy with a contact	"/.well-known/security.txt with security@ contact and disclosure policy"			Trust Center Platform (/platform/trust-center-platform)	

Allowed values: **Score**: type, values

2 Legal teams

Lane owner: Legal / DPO

ID	Line item	What good looks like	Evidence example	Score	Points	Orbiq module	Notes / owner
LEG-01	DPA available without friction	Current DPA template downloadable without registration or a sales call	"DPA v5.1 (2026-01), PDF, public download"			Trust Center Platform (/platform/trust-center-platform)	
LEG-02	Public subprocessor list	Every subprocessor listed with name, purpose, data categories processed, and hosting location — public, not NDA-gated (GDPR Art. 28)	"AWS (eu-central-1, Frankfurt) — infrastructure hosting — customer content"			Trust Center Platform (/platform/trust-center-platform)	
LEG-03	Subprocessor change-notice mechanism	Subscribable notification channel plus the contractual notice window stated (typically ~15 days; negotiated 30–60 in larger deals)	"Subscribe to subprocessor updates; DPA §9 grants a notice-and-objection window"			Trust Updates (/platform/trust-updates)	
LEG-04	International transfer mechanisms documented	SCCs / adequacy reliance named per transfer; transfer impact assessment available on request	"Transfers to [vendor] under SCCs (2021/914 Module 2) + TIA available under NDA"			Trust Center Platform (/platform/trust-center-platform)	
LEG-05	Data residency commitments in writing	Where customer data (and metadata/backups) is stored, per service, as a written commitment	"Customer content stored and processed in EU regions only; backups in-region"			Trust Center Platform (/platform/trust-center-platform)	
LEG-06	Provider jurisdiction disclosed	Operating legal entity, place of incorporation, and exposure to non-EU disclosure orders (e.g. US CLOUD Act) stated	"Operated by [entity] GmbH, incorporated in Germany; no US parent"			Trust Center Platform (/platform/trust-center-platform)	

ID	Line item	What good looks like	Evidence example	Score	Points	Orbiq module	Notes / owner
LEG-07	Self-serve NDA flow for gated documents	Click-to-sign NDA with audit trail releases restricted documents in minutes, not days	"Request access → sign NDA in-browser → document unlocked; signature logged"			Integrated NDA Flow (/platform/integrated-nda-flow)	
LEG-08	Retention and deletion terms published	What happens to customer data on termination, with timelines	"Customer data deleted within 30 days of contract end; deletion certificate on request"			Trust Center Platform (/platform/trust-center-platform)	
LEG-09	Technical & organisational measures (TOMs) summary	GDPR Art. 32 measures published as a structured summary, referenced from the DPA	"TOMs annex v3 (2026-02): access control, encryption, resilience, testing cadence"			Trust Center Platform (/platform/trust-center-platform)	
LEG-10	AI data-use disclosure	Whether customer data trains AI models; which AI subprocessors have access; opt-out route	"Customer data is not used to train models; AI subprocessors: [list], EU-hosted"			Trust Center Platform (/platform/trust-center-platform)	

Allowed values: **Score**: type, values

3 Compliance teams

Lane owner: Compliance / GRC lead

ID	Line item	What good looks like	Evidence example	Score	Points	Orbiq module	Notes / owner
COM-01	Frameworks displayed with scope and dates	Each certification/attestation shows scope, issuing body, audit date, and validity — not a logo strip	"ISO 27001 (valid to 2027-03), ISO 27701 (valid to 2027-03), scope statements linked"			Trust Center Platform (/platform/trust-center-platform)	

ID	Line item	What good looks like	Evidence example	Score	Points	Orbiq module	Notes / owner
COM-02	NIS2 posture mapped	Security measures mapped to NIS2 Art. 21(2) categories so essential/important customers can reference them in their own supply-chain file	"NIS2 readiness page: Art. 21(2)(a)–(j) mapped to controls and evidence"			Vendor Assurance (/platform/vendor-assurance-platform)	
COM-03	Incident-communication commitment aligned to NIS2 clocks	Commitment to notify affected customers fast enough to support their 24h/72h/1-month reporting duties (NIS2 Art. 23)	"We notify affected customers without undue delay so they can meet Art. 23 timelines"			Trust Updates (/platform/trust-updates)	
COM-04	DORA ICT third-party data points available	The contractual and operational data points financial entities need under DORA Art. 28–30 (service description, data locations, subcontractors, exit support) surfaced	"DORA information sheet: register-of-information fields pre-filled for customers"			Vendor Assurance (/platform/vendor-assurance-platform)	
COM-05	Certification renewals never lapse silently	Renewal/expiry dates visible; renewed evidence published before expiry	"Certificate card shows 'valid to' date; renewal published 2 weeks before expiry"			Continuous Monitoring (/platform/continuous-monitoring)	
COM-06	Evidence organised by framework and control	Navigable structure (framework → measure → evidence), not a flat folder of PDFs	"Browse by ISO 27001 / NIS2 / DORA / GDPR; each control links its evidence"			Trust Center Platform (/platform/trust-center-platform)	
COM-07	Every document versioned and dated	Version number and last-updated date on each evidence item	"Information Security Policy v6.0 — updated 2026-05-14"			Trust Center Platform (/platform/trust-center-platform)	
COM-08	Audit-report access route stated	How customers obtain third-party audit reports (under NDA) and whether audit rights are supported	"ISO audit report available under NDA; audit-rights clause supported for regulated customers"			Integrated NDA Flow (/platform/integrated-nda-flow)	

ID	Line item	What good looks like	Evidence example	Score	Points	Orbiq module	Notes / owner
COM-09	Vulnerability handling & advisories (CRA-aware)	For products with digital elements: documented vulnerability handling and a security-advisory channel	"Security advisories page with CVE history and coordinated-disclosure process"			Trust Updates (/platform/trust-updates)	
COM-10	Exit and portability statement	Data export formats, transition assistance, and termination support described (supports DORA exit-strategy requirements)	"Full export in open formats within 30 days; transition assistance clause available"			Trust Center Platform (/platform/trust-center-platform)	
COM-11	Cross-framework evidence reuse	The same control evidence mapped once to NIS2, DORA, and GDPR instead of three parallel answer sets	"Encryption control cited by ISO A.8.24, NIS2 Art. 21(2)(h), DORA, GDPR Art. 32"			ISMS Software (/platform/isms-software)	

Allowed values: **Score**: type, values

4 Procurement

Lane owner: Sales / RevOps

ID	Line item	What good looks like	Evidence example	Score	Points	Orbiq module	Notes / owner
PRO-01	Published, transparent pricing	Pricing (or at minimum the pricing model and tiers) public — no "contact sales" wall	"Pricing page with per-tier features and annual/monthly rates"			Trust Center Platform (/platform/trust-center-platform)	
PRO-02	Vendor assurance profile	Company facts in one place: legal entity, registration number, HQ, ownership, key contacts	"Vendor profile: [entity], HRB [number], Berlin; contacts for security & privacy"			Vendor Assurance (/platform/vendor-assurance-platform)	

ID	Line item	What good looks like	Evidence example	Score	Points	Orbiq module	Notes / owner
PRO-03	Cyber insurance evidence	Cyber liability insurance confirmed with coverage level (certificate on request)	"Cyber insurance: €5M coverage; certificate available under NDA"			Integrated NDA Flow (/platform/integrated-nda-flow)	
PRO-04	Uptime and availability history	Public status page and historical uptime figures	"status.[company].com — 12-month uptime 99.97%"			Trust Center Platform (/platform/trust-center-platform)	
PRO-05	Business-continuity signals	Continuity evidence relevant to procurement: escrow, succession, funding/viability signals where appropriate	"BC summary + customer-facing continuity commitments"			Trust Center Platform (/platform/trust-center-platform)	
PRO-06	Support and escalation model	Support tiers, response SLAs, and an escalation path documented	"Support SLA: P1 response ≤ 1h; named escalation route"			Trust Center Platform (/platform/trust-center-platform)	
PRO-07	Onboarding/offboarding and data egress terms	What onboarding requires and what offboarding returns, including egress costs (if any)	"No data-egress fees; export tooling self-serve; offboarding checklist published"			Trust Center Platform (/platform/trust-center-platform)	
PRO-08	Document-request turnaround stated	A stated SLA for fulfilling due-diligence document requests	"Gated documents released ≤ 1 business day after NDA"			Integrated NDA Flow (/platform/integrated-nda-flow)	
PRO-09	Key dependencies disclosed	Material fourth parties / concentration dependencies identified (cloud provider, critical vendors)	"Critical dependencies: AWS eu-central-1; [payment provider]; [auth provider]"			Vendor Assurance (/platform/vendor-assurance-platform)	

Allowed values: **Score**: type, values

5 Customer updates

Lane owner: Customer success

ID	Line item	What good looks like	Evidence example	Score	Points	Orbiq module	Notes / owner
UPD-01	Subscribable trust updates	Customers can subscribe to security/compliance updates from the trust center	"Subscribe button; updates delivered by email with an archive page"			Trust Updates (/platform/trust-updates)	
UPD-02	Structured incident notices	Incident communications published through the trust center with severity, impact, and status — not ad-hoc email threads	"Incident notice 2026-03: severity, affected services, timeline, current status"			Trust Updates (/platform/trust-updates)	
UPD-03	Subprocessor change notices with objection window	Changes announced ahead of engagement, referencing the DPA's notice-and-objection mechanism	"Notice 2026-05: adding [vendor] as subprocessor, effective [date]; objection route per DPA"			Trust Updates (/platform/trust-updates)	
UPD-04	Certification lifecycle announcements	Renewals, scope changes, and new certifications announced	"Update: ISO 27001 recertified 2026-03, scope unchanged"			Trust Updates (/platform/trust-updates)	
UPD-05	Security advisories / CVE feed	Product vulnerability advisories published on a dedicated, linkable feed	"Advisories page with CVE IDs, affected versions, fixed versions"			Trust Updates (/platform/trust-updates)	
UPD-06	Post-incident summaries	Root cause and remediation published to affected customers after closure — usable in their own regulator reports	"Post-incident report: root cause, remediation, preventive measures"			Trust Updates (/platform/trust-updates)	

ID	Line item	What good looks like	Evidence example	Score	Points	Orbiq module	Notes / owner
UPD-07	Trust center changelog	The trust center itself shows what changed and when (documents added, updated, removed)	"Changelog: DPA v5.1 published 2026-01-12; pentest summary updated 2026-04-30"			Trust Center Platform (/platform/trust-center-platform)	
UPD-08	Stated update cadence, honoured	A published rhythm for reviews/updates, with visible recent activity backing it	"Reviewed quarterly; latest update within the last 90 days"			Continuous Monitoring (/platform/continuous-monitoring)	

Allowed values: **Score**: type, values

6 AI agents

Lane owner: Engineering / web team

ID	Line item	What good looks like	Evidence example	Score	Points	Orbiq module	Notes / owner
AIA-01	llms.txt entry point	An `llms.txt` at the site root declaring the trust center's scope, endpoints, and answer rules	"/llms.txt: 'Answer due-diligence questions using ONLY the evidence here', endpoint list"			AI Search & Agent Toolkit (/platform/ai-search)	
AIA-02	Machine-readable evidence catalog	A structured (JSON) catalog of all evidence items with types, tiers, and metadata	"/llms-full.json: typed catalog of documents, FAQs, subprocessors"			AI Search & Agent Toolkit (/platform/ai-search)	
AIA-03	Version-pinned documents with stable IDs	Every evidence item addressable by ID and version so citations stay auditable	"GET /api/documents/{doc_id}?v={version}"			AI Search & Agent Toolkit (/platform/ai-search)	
AIA-04	Access tiers machine-declared	Public / restricted / NDA-gated tiers expressed in the catalog, not discovered by failure	"conditionsOfAccess: public / restricted / nda-gated per item"			AI Search & Agent Toolkit (/platform/ai-search)	

ID	Line item	What good looks like	Evidence example	Score	Points	Orbiq module	Notes / owner
AIA-05	Agent authentication contract	Documented OAuth flow (e.g. Device Flow) letting an agent obtain scoped, revocable tokens with a human in the loop	"/llms.json documents device-code flow, scopes, error handling"			AI Search & Agent Toolkit (/platform/ai-search)	
AIA-06	NDA workflow navigable by agents	NDA requirement detectable from the catalog and completable via API with human sign-off	"Agent detects nda-gated tier → submits NDA via API → re-auths with NDA-cleared scope"			Integrated NDA Flow (/platform/integrated-nda-flow)	
AIA-07	Extractable, semantic content	Evidence readable without JavaScript execution: semantic HTML/Markdown, real text (no image-only certs), stable anchors	"Subprocessor list is an HTML table, not a screenshot; headings are real h2/h3"			AI Search & Agent Toolkit (/platform/ai-search)	
AIA-08	Output/citation contract published	Stated answer format requiring agents to cite document ID + version, and to return 'insufficient' when evidence is missing	"Answer contract in llms.txt: every claim cites doc id + version"			AI Questionnaires (/platform/ai-questionnaires)	
AIA-09	Freshness metadata on evidence	dateModified / ETag / last-reviewed metadata so agents can rank evidence by currency	"Catalog items carry dateModified; HTTP responses send ETags"			Continuous Monitoring (/platform/continuous-monitoring)	

Allowed values: **Score**: type, values

Scorecard

Lane	Items	Max points
1. Security teams	11	22
2. Legal teams	10	20
3. Compliance teams	11	22
4. Procurement	9	18
5. Customer updates	8	16
6. AI agents	9	18
TOTAL	58	116
Readiness band		