Vendor Security Questionnaire Response Kit

Template answers, evidence pointers, and a 30-day rollout checklist your sales and security teams can run together.

30	4hrs	5
pre-written answers across SIG, CAIQ & custom VSQs	target turnaround vs. the 4-day fire drill	reusable evidence artifacts that back every answer

For fintech SaaS, wealth-tech, and lending platforms selling into regulated financial services.
Campaign VSQ-2026-Q2 · Region US / UK / EU · Internal & customer-facing use

How to use this kit

By the time a Vendor Security Questionnaire (VSQ) lands, legal and commercial terms are usually close to done. The security review is what slips the deal. This kit exists so an AE can answer a VSQ at 9pm on a Thursday without paging the on-call security engineer.

The kit has three parts:

1. The Evidence Library ,the five reusable artifacts every answer points to. Build these once, version them quarterly.
2. The Answer Bank ,30 pre-written responses to the questions that show up across SIG, CAIQ, and buyer-custom VSQs, organized by category.
3. The 30-Day Rollout & SLA ,how to stand the kit up and the response-time commitment to operate against.

> **Rules of engagement for AEs**
> Use answers verbatim only when the buyer's wording matches. When in doubt, attach the evidence artifact and copy the answer's intent ,don't invent specifics. Anything in the "Escalate if" row goes to Security before it goes to the buyer. Never share raw scan output or internal ticket links externally; share the packaged artifact.

Why modern VSQs break old playbooks

Five years ago a VSQ was a compliance ritual: do you enforce MFA, is the laptop fleet encrypted, do you have an incident-response plan. The answer was almost always "yes," the evidence was a policy PDF, and the review closed in a week. Three things changed that.

Frameworks matured

The SIG (Standardized Information Gathering, from Shared Assessments) and the CAIQ (Consensus Assessments Initiative Questionnaire, from the Cloud Security Alliance) now ship with question banks that go well past policy. Buyers layer in deal-specific asks that reflect their own regulators' expectations.

Regulation caught up

The SEC's amended Regulation S-P took effect for larger entities in December 2025, with smaller entities following in mid-2026, pushing covered firms to demand evidence rather than assurances from service providers. In the EU, DORA's third-party register provisions require financial entities to document operational dependencies on ICT vendors ,detail that flows straight back into procurement questionnaires.

Buyers got burned

Recent software supply-chain incidents made one lesson hard to ignore: a declared software inventory is not the same as understanding what executes in production. An SBOM shows what a

product contains; it does not, by itself, prove which components are loaded, reachable, or on a customer-data path.

The net effect: questionnaires shifted from ***"do you have"*** to ***"show me."*** Policy attestation is now table stakes. The questions that decide deals ask for evidence drawn from your live environment.The four questions scanners can't answer

Static analyzers and SBOM generators still answer what's in the box. These four patterns ask what the box does in production ,and they appear in nearly every modern fintech procurement review.

Pattern	What the buyer is really asking	Scanner alone?
Continuous component evaluation	What happens on day 47, when a new CVE drops against a library you still ship? Frequency and method of ongoing detection.	Answers half
Runtime third-party monitoring	Of everything declared in the manifest, which libraries actually load and execute on the customer-data path?	**No**
Exploitability evidence	For open High/Critical findings, is the vulnerability reachable in your environment ,with evidence, not assertion?	**No**
Real-time scope documentation	A data-flow diagram that reflects last week's deploy, not last year's architecture review.	**No**

Each of these sits one layer below what a typical SAST/SCA toolchain produces. They're not asking what your code looks like ,they're asking what it does in production. That's why the answer bank in this kit pairs every response with a runtime evidence artifact.

Part 1 The Evidence Library

A “VSQ-ready” posture isn’t a bigger policy library. It’s a small set of artifacts your sales team can pull on demand and your security team can defend on a follow-up call. Build them once; version them on the cadence shown.

Buyer asks for	What you produce	Refresh	Owner
Component inventory	SBOM with a loaded-in-production flag per component	**Continuous**	AppSec
Vulnerability status	Open findings list with reachability classification (reachable / unreachable / unknown)	**Continuous**	AppSec
Data-flow scope	Architecture diagram with customer-data-path services highlighted, plus third-party dependencies for each	Per release	Eng / Arch
Detection coverage	Mapping of detection rules to MITRE ATT&CK techniques relevant to the customer-data path	Quarterly	Security Ops
Compliance attestation	SOC 2 Type II, ISO 27001, plus pre-filled SIG and CAIQ responses	Annual / on issue	GRC

The two rows most teams miss

The loaded-in-production SBOM and the reachability-classified vulnerability list are the artifacts that usually need new tooling ,and the ones that turn a four-day questionnaire response into a four-hour one. The rest can be assembled from sources you already have.

Where to store it

Put the artifacts somewhere AEs can self-serve ,a trust center, a sales-shared drive, or a controlled portal. Keep a single source of truth and link to it from the answer bank so nobody pastes a stale SBOM into a buyer thread.

Part 2 The Answer Bank

Thirty answers across seven categories. Each card gives you the buyer's likely wording, a recommended response, the evidence artifact to attach, and the condition that should trigger escalation to Security. Adapt names and numbers to your environment; never paste in figures you can't back with an artifact.

Category A ,Runtime & Third-Party Components

The deal-deciders. These four map directly to the patterns scanners can't answer.

Q1 Runtime third-party monitoring	
Buyer's wording	*Identify which third-party libraries are loaded and executed in your production environment that processes Customer Data.*
Recommended answer	We maintain a continuously generated SBOM in which every component carries a loaded-in-production flag, distinguishing components that execute on the customer-data path from those merely declared in a manifest. As of the most recent refresh, [N] of [M] declared components are observed loaded in the production runtime that processes Customer Data. The remainder are declared dependencies not loaded at runtime. We can provide the filtered, loaded-in-production component list scoped to the services in your data path on request.
Evidence to attach	**Loaded-in-production SBOM (filtered to customer-data-path services)**
Escalate if	Buyer asks for a component-by-component attestation signed by an officer, or names a component you can't classify.

Q2 Continuous component evaluation	
Buyer's wording	*Describe how your third-party and open-source components are evaluated on an ongoing basis, including frequency and method of detection for newly disclosed vulnerabilities.*
Recommended answer	Components are evaluated continuously, not at a point in time. New vulnerability disclosures are matched against our live runtime inventory automatically, so a CVE published after onboarding is detected against the components we actually run. Detection is continuous; triage and prioritization follow our documented vulnerability-management SLA, with reachability used to rank remediation. We can share our most recent open-findings export with detection timestamps.
Evidence to attach	**Continuous SBOM + vulnerability-management policy**
Escalate if	Buyer requires a specific scan frequency or third-party scanning vendor you don't use.

Q3 Exploitability / reachability evidence	
Buyer's wording	*For any High or Critical vulnerabilities open longer than [N] days, provide rationale for non-remediation, including evidence the vulnerability is not exploitable in your environment.*
Recommended answer	We classify every open finding by reachability ,reachable, unreachable, or unknown ,relative to the customer-data code path, rather than treating all Highs equally. Example structure for our response: of the [73] High findings in the latest scan, [9] are reachable from a customer-data path; for those we provide a mitigation plan and timeline. The remainder are not reachable in our deployed configuration, with classification rationale available per finding. We do not assert non-exploitability without reachability data behind it.
Evidence to attach	**Reachability-classified open-findings list + mitigation timeline for reachable items**
Escalate if	Any reachable High/Critical lacks a committed remediation date, or buyer disputes a reachability classification.

Q4 Real-time scope documentation	
Buyer's wording	*Provide a current data-flow diagram showing all systems, services, and third-party dependencies in the Customer Data processing path.*
Recommended answer	We maintain an architecture diagram refreshed per release that highlights the services on the customer-data path and lists the third-party dependencies for each. The diagram reflects the current deployed architecture, not a prior annual review. We can scope a version to the services relevant to your engagement.
Evidence to attach	**Customer-data-path architecture diagram (current release)**
Escalate if	Buyer’s data-residency or sub-processor questions go beyond what the diagram documents.

Category B ,Vulnerability & Patch Management

Process questions where evidence beats prose.

Q5 Vulnerability management program	
Buyer's wording	*Describe your vulnerability management program, including discovery, prioritization, and remediation SLAs.*
Recommended answer	We run continuous discovery against the live runtime inventory, prioritize by severity and reachability, and remediate against documented SLAs by severity tier. Reachability lets us remediate the right findings first rather than chasing every declared dependency.
Evidence to attach	**Vulnerability-management policy + reachability-classified findings sample**
Escalate if	Buyer requests SLAs stricter than your committed tiers.

Q6 Patch cadence	
Buyer's wording	*What is your patching cadence for operating systems, runtimes, and third-party libraries?*
Recommended answer	Critical patches follow an expedited path; routine patching follows a regular release cadence. Library updates are driven by the continuous inventory so newly disclosed CVEs against running components are surfaced immediately. We can provide recent remediation timestamps as evidence.
Evidence to attach	**Patch-management policy + remediation log excerpt**
Escalate if	Buyer asks for guaranteed patch windows shorter than your process supports.

Q7 Penetration testing	
Buyer's wording	*Do you conduct independent penetration testing? Provide frequency and a summary of the most recent test.*
Recommended answer	Yes. We engage an independent third party on a regular cadence and remediate findings against tracked timelines. We can share an executive summary or attestation letter under NDA; full reports are available through our trust process.
Evidence to attach	**Latest pen-test attestation / executive summary (under NDA)**
Escalate if	Buyer asks for the full unredacted report before an NDA is in place.

Category C ,Detection, Monitoring & Incident Response

Q8 Detection coverage	
Buyer's wording	*Provide evidence of detection coverage for the systems handling our data.*
Recommended answer	We map our detection rules to MITRE ATT&CK techniques relevant to the customer-data path, so coverage is expressed against a recognized framework rather than asserted generally. We can share the coverage mapping scoped to the technique categories most relevant to your environment.
Evidence to attach	**Detection-rule → MITRE ATT&CK coverage mapping**
Escalate if	Buyer asks for raw SIEM rule logic or log samples containing other customers' data.

Q9 Logging & monitoring	
Buyer's wording	*Describe your logging and monitoring of production systems, including retention.*
Recommended answer	Production systems on the customer-data path are centrally logged and monitored, with alerting tied to our detection coverage. Retention follows our documented data-retention schedule. Monitoring scope aligns to the services shown on the customer-data-path diagram.
Evidence to attach	**Logging & monitoring policy + retention schedule**
Escalate if	Buyer requires retention longer than your documented schedule.

Q10 Incident response plan	
Buyer's wording	*Do you maintain a documented incident response plan, and how often is it tested?*
Recommended answer	Yes. We maintain a documented IR plan with defined roles, severity tiers, and communication paths, and we exercise it on a regular cadence. Notification commitments to customers are defined in our standard terms / DPA.
Evidence to attach	**Incident-response policy + most recent tabletop summary**
Escalate if	Buyer asks for breach-notification windows tighter than your contractual commitment.

Q11 Breach notification	
Buyer's wording	*What is your customer breach-notification commitment and process?*
Recommended answer	Our notification commitments and process are defined contractually. On confirmation of a qualifying incident affecting Customer Data, we notify per those terms with the information available at the time and follow up as the investigation progresses.
Evidence to attach	**DPA / MSA security-incident clause**
Escalate if	Buyer wants a notification SLA that differs from signed contract language ,route to Legal + Security.

Category D ,Access Control & Authentication

Q12 MFA enforcement	
Buyer's wording	*Is multi-factor authentication enforced for all access to systems processing Customer Data?*
Recommended answer	Yes. MFA is enforced for administrative and production access to systems processing Customer Data, consistent with our access-control policy.
Evidence to attach	**Access-control policy + SSO/MFA configuration attestation**
Escalate if	Buyer asks for evidence of MFA on a system you can’t confirm ,verify with IT before answering.

Q13 Least privilege & access reviews	
Buyer's wording	*Describe how you enforce least privilege and how often access is reviewed.*
Recommended answer	Access is granted on a least-privilege, role-based basis and reviewed on a recurring schedule, with joiner/mover/leaver processes governing changes. Privileged access is restricted and monitored.
Evidence to attach	**Access-control policy + access-review cadence evidence**
Escalate if	Buyer requests user-level access listings ,do not export externally.

Q14 Privileged access management	
Buyer's wording	*How is privileged / administrative access to production managed and monitored?*
Recommended answer	Privileged access is limited to authorized personnel, requires MFA, and is logged and monitored. Standing access is minimized in favor of scoped, time-bound grants where feasible.
Evidence to attach	**Privileged-access policy**
Escalate if	Buyer asks for the named list of privileged users.

Category E ,Data Protection & Encryption

Q15 Encryption in transit & at rest	
Buyer's wording	*Is Customer Data encrypted in transit and at rest? Specify standards.*
Recommended answer	Yes. Customer Data is encrypted in transit using current TLS standards and at rest using industry-standard algorithms, consistent with our encryption policy and key-management practices.
Evidence to attach	**Encryption / key-management policy**
Escalate if	Buyer requires a specific cipher or key-length you can't confirm ,verify with Eng.

Q16 Key management	
Buyer's wording	*Describe your encryption key-management practices, including rotation.*
Recommended answer	Keys are managed through a centralized key-management process with restricted access, separation of duties, and rotation on a defined schedule.
Evidence to attach	**Key-management policy**
Escalate if	Buyer asks for customer-managed-key (BYOK) support you don't offer.

Q17 Data segregation & residency	
Buyer's wording	*How is Customer Data segregated from other tenants, and where is it stored?*
Recommended answer	Customer Data is logically segregated per tenant. Primary processing and storage locations are documented; we can confirm the regions relevant to your engagement. Sub-processors and their locations are listed in our sub-processor register.
Evidence to attach	**Sub-processor list + data-flow / residency documentation**
Escalate if	Buyer has a hard data-residency requirement ,confirm with Eng before committing.

Q18 Data retention & deletion	
Buyer's wording	*What are your data-retention and secure-deletion practices for Customer Data on termination?*
Recommended answer	Retention follows our documented schedule. On termination, Customer Data is deleted or returned per the terms of the agreement within the defined window, using secure-deletion methods.
Evidence to attach	**Data-retention & deletion policy + DPA clause**
Escalate if	Buyer requires certified destruction documentation per deletion event.

Category F ,Governance, Compliance & Risk

Q19 Certifications & attestations	
Buyer's wording	*List your current security certifications and audit reports (e.g., SOC 2, ISO 27001).*
Recommended answer	We maintain SOC 2 Type II and ISO 27001. Current reports and certificates are available through our trust process under NDA, alongside pre-filled SIG and CAIQ responses.
Evidence to attach	**SOC 2 Type II report + ISO 27001 certificate + pre-filled SIG/CAIQ**
Escalate if	Buyer requires a certification you don’t hold (e.g., PCI DSS, FedRAMP).

Q20 Security governance	
Buyer's wording	*Describe your security governance structure and executive ownership.*
Recommended answer	Security is owned at the executive level (CISO or equivalent) with a defined governance structure, documented policies reviewed at least annually, and risk reporting to leadership.
Evidence to attach	**Information-security policy + org/governance overview**
Escalate if	Buyer asks for named individuals or org-chart detail beyond role level.

Q21 Risk assessment	
Buyer's wording	*How often do you perform security risk assessments?*
Recommended answer	We perform risk assessments on a recurring basis and after significant changes, tracking identified risks to remediation through our risk-management process.
Evidence to attach	**Risk-management policy**
Escalate if	Buyer wants the full risk register ,share summary only.

Q22 Regulatory alignment (S-P / DORA)	
Buyer's wording	*Describe how your controls support our regulatory obligations under [Regulation S-P / DORA / GLBA].*
Recommended answer	Our control set and evidence artifacts are designed to support customers' third-party oversight obligations ,including evidence-based vendor due diligence and documentation of operational dependencies. We can map relevant artifacts to the specific obligations you cite.
Evidence to attach	**Control-to-obligation mapping + relevant policies**
Escalate if	Buyer asks us to attest to their compliance ,route to GRC/Legal; we support, we don't certify their posture.

Category G ,Secure Development & Supply Chain

Q23 Secure SDLC	
Buyer's wording	*Describe your secure software development lifecycle, including security testing in CI/CD.*
Recommended answer	Security is integrated across the SDLC: code review, automated security testing in CI/CD, dependency analysis against the live inventory, and pre-release checks. Findings feed the same reachability-based prioritization used in production.
Evidence to attach	**Secure-SDLC policy + CI/CD security-gate description**
Escalate if	Buyer requires a specific SAST/DAST tool you don't run.

Q24 Supply-chain integrity / CI-CD security	
Buyer's wording	*How do you protect your build pipeline and repository secrets against supply-chain compromise?*
Recommended answer	Build pipelines enforce access controls and secret hygiene; repository secrets are managed through a secrets-management process and rotated. We monitor dependencies at runtime so a compromised or vulnerable component is detected against what actually executes, not just what's declared.
Evidence to attach	**CI/CD & supply-chain security policy + loaded-in-production SBOM**
Escalate if	Buyer asks for build-system architecture detail or artifact-signing you can't confirm.

Q25 SBOM provision	
Buyer's wording	*Can you provide a Software Bill of Materials for the product version we will use?*
Recommended answer	Yes. We can provide an SBOM, and ,importantly ,a version annotated with loaded-in-production flags so you can distinguish components that execute on the customer-data path from declared-only dependencies. A raw 2,400-line SBOM that doesn't separate loaded from declared isn't an answer; ours does.
Evidence to attach	**Loaded-in-production SBOM (version-specific)**
Escalate if	Buyer requires a specific SBOM format (SPDX / CycloneDX version) ,confirm export support.

Q26 Change management	
Buyer's wording	*Describe your change-management process for production systems.*
Recommended answer	Production changes follow a documented change-management process with review, approval, testing, and rollback procedures. Security-relevant changes are assessed before release.
Evidence to attach	**Change-management policy**
Escalate if	Buyer requires customer notification ahead of every change.

Category H ,People, Resilience & Sub-processors

Q27 Security awareness training	
Buyer's wording	*Do personnel receive security awareness training, and how often?*
Recommended answer	Yes. All personnel complete security awareness training at onboarding and on a recurring basis, with role-specific training for engineering and privileged roles.
Evidence to attach	**Security-training policy + completion-rate attestation**
Escalate if	Buyer asks for per-employee completion records.

Q28 Background checks	
Buyer's wording	*Are background checks performed on personnel with access to Customer Data?*
Recommended answer	Background checks are performed on personnel where permitted by law and consistent with role sensitivity, as part of our HR security process.
Evidence to attach	**HR / personnel-security policy**
Escalate if	Buyer requires checks beyond what local law permits in a given region.

Q29 Business continuity & DR	
Buyer's wording	*Describe your business-continuity and disaster-recovery capabilities, including RTO/RPO.*
Recommended answer	We maintain documented BC/DR plans with defined RTO and RPO targets, backed by regular backups and tested recovery procedures. We can confirm the specific RTO/RPO targets applicable to your tier.
Evidence to attach	**BC/DR policy + most recent DR-test summary**
Escalate if	Buyer requires RTO/RPO tighter than your committed targets.

Q30 Sub-processor management	
Buyer's wording	*How do you manage and disclose sub-processors handling Customer Data?*
Recommended answer	We maintain a sub-processor register, perform security due diligence before onboarding a sub-processor, and provide notice of changes per our DPA. The register lists each sub-processor and its function.
Evidence to attach	**Sub-processor register + DPA sub-processor clause**
Escalate if	Buyer objects to a listed sub-processor ,route to Legal.

Part 3 The 30-Day Rollout & SLA

Stand the kit up in four weeks. The goal isn't a one-time scramble; it's converting VSQ response time from a recurring fire drill into an operational metric the business can improve.

Week 1 ,Inventory the questions

- Pull the last six VSQs your team answered.
- Tag every question by category (governance, access control, encryption, vuln management, IR, data flow, third-party).
- Count how many fall into the four runtime patterns. For most fintech SaaS sellers this lands at 15–30 per VSQ ,enough to be the bottleneck.

Week 2 ,Stand up the evidence artifacts

- For each of the five artifacts, name an owner, a storage location, and what must change to refresh it weekly without a human in the loop.
- The loaded-in-production SBOM and reachability-classified vulnerability list usually need new tooling; the rest assemble from sources you have.

Week 3 ,Pre-write the answers

- For your top 30 most-frequent questions across SIG, CAIQ, and custom history, draft a one-paragraph answer and a one-line evidence pointer (this kit gives you the starting set).
- Keep the response kit under 40 pages so it stays usable.

Week 4 ,Hand it to sales

- Train AEs on what the kit contains ,and what isn't in it, so they escalate the right exceptions.
- Set the internal SLA below.

Standard VSQ	Complex VSQ	Net-new pattern
< 24 hours Answerable from existing artifacts.	**< 72 hours** Needs scoped artifacts or CISO review.	**Escalate** Question not in the kit → Security owns, kit updated after.

Trust as a wedge, not an afterthought

The fintech SaaS companies winning late-stage procurement reviews aren't the ones with the longest policy libraries ,they treat runtime evidence as part of their sales infrastructure. The same data that helps you patch the right thing helps you close the right deal. VSQs won't get shorter; the teams that build for that once, and let the work compound, close faster than the teams rewriting the same answers every quarter.

Ready to put this into practice?

Kodem helps fintech SaaS, wealth-tech, and lending platforms produce the runtime evidence modern procurement reviews demand ,loaded-in-production SBOMs, reachability-classified findings, and detection coverage your sales team can pull on demand.

- Book a walkthrough of the loaded-in-production SBOM and reachability classification.
- Join the UK webinar on cutting VSQ turnaround from days to hours.

This kit is for informational purposes only and does not constitute legal or compliance advice. References to SEC Regulation S-P, DORA, SOC 2, and ISO 27001 are summary in nature; consult qualified counsel for application to your organization. Answer language is a starting template ,confirm every specific claim against your own evidence before sending to a buyer.