Kailash Consult Free resource · kailashconsult.com/resources

Enterprise Security Review Kit

50 questions that commonly appear in SIG Lite, CAIQ and buyers' own spreadsheets, an example answer for each, and 6 documents buyers often request.

How to use

- Work top to bottom. Set 'Your status' for each question: Ready, Partial, Not yet or N/A.
- Example answers are starting points for a 20-200 person SaaS team. Replace every [bracket] and only state what is true today.
- Attach the evidence listed. A short true answer with evidence beats a long answer without it.
- Anything marked Partial or Not yet is your gap list. Fix those before the next big deal reaches security review.

Example answers and mappings are templates, not facts about your company. Edit every bracket and validate each statement before sharing it with a customer or auditor.

Governance and policies

ID	Question buyers ask	What they are really checking	Example answer (edit before use)	Evidence to attach
A01	Do you have a documented information security policy approved by leadership?	That security is owned and written down, not ad hoc.	Yes. [Company] maintains an information security policy set approved by [CEO/CTO] on [date] and reviewed at least annually. It covers access control, data protection, incident response, vendor management and secure development.	Policy index with approval date
A02	Who is responsible for information security?	A named owner with authority and time.	[Name, title] owns the security program and reports to [CEO/CTO]. Engineering leads own controls in their areas. Security topics are reviewed with leadership [monthly/quarterly].	Org chart or RACI
A03	Do you have a SOC 2 report or ISO 27001 certificate?	Independent proof, or a credible date for it.	[Option 1] Yes, our SOC 2 Type [I/II] report dated [date] is available under NDA. [Option 2] We are preparing for SOC 2 Type [I/II] with an independent CPA firm and expect the report in [month, year]. A readiness summary is available under NDA.	Report or certificate; or readiness letter

Kailash Consult

ID	Question buyers ask	What they are really checking	Example answer (edit before use)	Evidence to attach
A04	How often do you review and update security policies?	Policies are living documents, not shelfware.	Policies are reviewed at least annually and after major changes to systems, vendors or regulations. Each policy records its owner, version and last review date.	Policy version history
A05	Do you perform a formal risk assessment?	Risks are identified, rated and treated on purpose.	Yes. We run a risk assessment at least annually and when major changes happen. Risks are scored on likelihood and impact, each has an owner, and treatment is tracked in our risk register.	Risk register extract
A06	Do employees complete security awareness training?	People, the most common entry point, are trained.	All employees and contractors complete security awareness training at onboarding and annually, including phishing and data handling. Completion is tracked; [phishing simulations run quarterly].	Training completion report

People and HR security

ID	Question buyers ask	What they are really checking	Example answer (edit before use)	Evidence to attach
A07	Do you run background checks on employees?	Screening proportional to access and local law.	Yes, where permitted by law, all employees with access to production or customer data pass a background check before access is granted.	Screening policy; sample confirmation
A08	How quickly is access removed when someone leaves?	Former staff cannot reach customer data.	Access to SSO, production and customer data is removed within [24 hours] of departure, usually on the last working day, using an offboarding checklist tracked in [tool].	Offboarding checklist; recent ticket
A09	Do staff sign confidentiality agreements?	Legal obligation to protect customer data.	Yes. All employees and contractors sign confidentiality terms before they receive access, and the obligation continues after they leave.	Template agreement
A10	Do you have an acceptable use policy and device standards?	Laptops are managed and used responsibly.	Yes. Our acceptable use policy covers company devices, data handling and approved tools. Company laptops are managed through [MDM] with disk encryption, screen lock and OS updates enforced.	Policy; MDM compliance screenshot

Free to use inside your company. Not for resale. kailashconsult.com/resources

Access control

ID	Question buyers ask	What they are really checking	Example answer (edit before use)	Evidence to attach
A11	Do you use single sign-on for internal systems?	Central control of who gets in.	Yes. Workforce access to business and engineering systems goes through [Google Workspace/Okta] SSO wherever the system supports it. Exceptions are listed and reviewed.	SSO app list
A12	Is multi-factor authentication enforced?	Stolen passwords alone cannot get in.	Yes. MFA is enforced for all workforce accounts through our identity provider, and separately for cloud consoles, source control and admin tools.	IdP MFA enforcement setting
A13	How do you apply least privilege?	People only see what their job needs.	Access is role-based. New access needs a request and manager approval. Production and customer data access is limited to [number/roles] engineers who need it to run the service.	Role matrix; access request example
A14	Do you review user access regularly?	Stale access gets caught.	Yes. Access to production, customer data and critical SaaS tools is reviewed [quarterly] by system owners. Removals are tracked to closure.	Last access review record
A15	How is privileged and production access controlled?	Admin power is rare, logged and temporary.	Production access requires SSO with MFA and is limited to named engineers. [Break-glass or just-in-time] access is time-limited and logged. Admin actions are recorded in [CloudTrail/audit logs].	Admin list; audit log sample
A16	What are your password requirements?	Weak passwords are not possible.	Passwords follow current NIST guidance: minimum [12] characters, checks against known breached passwords, no forced periodic changes, and MFA required. A company password manager is provided.	IdP password policy
A17	Can our users sign in to your product with SSO and roles?	Their IT team keeps control of their own users.	[Yes, SAML/OIDC SSO and role-based permissions are available on the [plan] plan.] [Or: SSO is on our roadmap for [quarter]; today we support MFA and admin-managed roles.]	Product docs link

Data protection and encryption

ID	Question buyers ask	What they are really checking	Example answer (edit before use)	Evidence to attach
A18	Do you classify data and handle it by sensitivity?	Customer data is treated as the most sensitive.	Yes. Data is classified as [Public, Internal, Confidential, Customer Restricted]. Customer data is Restricted, with the strictest access, encryption and retention rules.	Data classification policy

ID	Question buyers ask	What they are really checking	Example answer (edit before use)	Evidence to attach
A19	Is customer data encrypted at rest?	Stolen disks or snapshots are unreadable.	Yes. Customer data in databases, object storage and backups is encrypted at rest with AES-256 using [AWS KMS/GCP KMS] managed keys.	Cloud encryption settings
A20	Is data encrypted in transit?	Nobody can read traffic on the wire.	Yes. All external traffic uses TLS 1.2 or higher with modern ciphers. Internal service traffic is encrypted [within the VPC/with TLS].	TLS scan result
A21	How are encryption keys managed?	Keys are controlled, rotated and separated.	Keys are managed in [AWS KMS/GCP KMS] with access restricted to [roles]. Key use is logged and keys rotate [automatically/annually]. [Customer-managed keys are available on enterprise plans, if true.]	KMS configuration
A22	Where is our data stored and processed?	Data residency and legal exposure.	Customer data is stored and processed in [cloud provider] [region(s), e.g. US-East]. Subprocessors and their locations are listed at [link].	Hosting regions; subprocessor list
A23	What happens to our data when the contract ends?	They can leave cleanly.	Customers can export their data during the term. After termination, customer data is deleted from production within [30] days and from backups within [backup retention period], and deletion can be confirmed in writing.	Retention and deletion policy
A24	Is customer data used in development or test environments?	Real data is not copied to weaker environments.	No. Development and test use synthetic or masked data. Production data stays in production unless a customer authorizes a specific support action.	SDLC policy extract

Infrastructure and operations

ID	Question buyers ask	What they are really checking	Example answer (edit before use)	Evidence to attach
A25	Where is the service hosted and who is responsible for what?	They understand the shared responsibility split.	The service runs on [AWS/GCP/Azure] in [region]. The provider secures the physical data centers and core infrastructure (covered by their SOC 2 and ISO 27001 reports). [Company] secures our accounts, configuration, application and data.	Architecture diagram; provider reports link
A26	How is your network protected?	Production is not open to the internet.	Production runs in private networks. Only load balancers are public, with security groups that deny by default. Admin access goes through [SSO-backed bastion/VPN/zero-trust tool].	Network diagram; security group review

Kailash Consult

ID	Question buyers ask	What they are really checking	Example answer (edit before use)	Evidence to attach
A27	How do you find and fix vulnerabilities?	Known holes get patched on a clock.	We scan infrastructure, containers and dependencies [continuously/weekly] with [tool]. Fix targets: critical [7] days, high [30] days, medium [90] days. Exceptions need a documented approval.	Scan report; remediation SLA policy
A28	Do you have an independent penetration test? When was the last one?	A third party tried to break in recently.	Yes. An independent firm, [name], tested our application and infrastructure in [month, year]. All critical and high findings were fixed and retested. An executive summary is available under NDA.	Pen test letter or executive summary
A29	How do you protect employee laptops?	Endpoints are not the weak link.	Company laptops are managed with [MDM] and run [EDR/anti-malware]. Disk encryption, firewall, screen lock and automatic updates are enforced and monitored.	MDM and EDR compliance report
A30	What do you log and how do you monitor it?	They would notice an attack.	We log authentication, admin actions, production access and application security events to [tool]. Logs are kept for [12 months]. Alerts for suspicious activity go to [on-call channel] and are triaged [24/7 or business hours].	Logging config; alert example
A31	How do you keep systems securely configured?	No drift into insecure settings.	Infrastructure is defined as code in [Terraform/CloudFormation] and changes go through review. Cloud configuration is checked against [CIS benchmarks] with [tool], and findings are tracked to closure.	IaC repo; config scan report

Secure development

ID	Question buyers ask	What they are really checking	Example answer (edit before use)	Evidence to attach
A32	Do you follow a secure development process?	Security is built in, not bolted on.	Yes. Every change goes through a pull request with peer review. Security-relevant changes get an extra review. Developers receive secure coding training [annually].	SDLC policy; sample PR
A33	Do you scan code and dependencies?	Vulnerable code and libraries are caught early.	Yes. [SAST tool] scans code and [dependency tool] scans open-source libraries on every pull request. High-risk findings block the merge until fixed or approved.	CI pipeline config; scan results

Free to use inside your company. Not for resale. kailashconsult.com/resources

ID	Question buyers ask	What they are really checking	Example answer (edit before use)	Evidence to attach
A34	How do changes reach production?	No unreviewed change goes live.	Changes deploy only through our CI/CD pipeline after review and automated tests pass. Branch protection prevents direct pushes to main. Emergency changes are reviewed after the fact within [2 business days].	Branch protection settings; deploy log
A35	How do you manage secrets like API keys and passwords?	No credentials sitting in code.	Secrets are stored in [AWS Secrets Manager/Vault], never in source code. Secret scanning runs on every commit, and exposed secrets are rotated immediately.	Secret manager config; scanner setting
A36	Are development, test and production separated?	A mistake in test cannot hit production.	Yes. Production runs in a separate [cloud account/project] with separate access. Developers do not have standing write access to production.	Account structure diagram

Vendors and subprocessors

ID	Question buyers ask	What they are really checking	Example answer (edit before use)	Evidence to attach
A37	Who are your subprocessors?	Where their data goes beyond you.	Our current subprocessor list, with purpose and location, is published at [link] and available on request. It includes [cloud provider, email provider, support tool, AI provider if used].	Subprocessor list
A38	How do you assess vendor security?	Your suppliers are not their weak link.	Vendors that handle customer or sensitive data are reviewed before onboarding and annually: security reports (SOC 2/ISO 27001), data handling and contract terms. Results are recorded in our vendor register.	Vendor register extract
A39	Will you notify us before adding a new subprocessor?	They can object before data moves.	Yes. We give at least [30] days' notice of new subprocessors through [email/subscription page], as set out in our DPA.	DPA clause
A40	Do you offer a data processing agreement?	GDPR, CCPA and contractual cover.	Yes. Our DPA covers GDPR and CCPA/CPRA requirements, including [Standard Contractual Clauses] for international transfers, and is available at [link] or on request.	DPA

Kailash Consult

Incident response

ID	Question buyers ask	What they are really checking	Example answer (edit before use)	Evidence to attach
A41	Do you have an incident response plan? Is it tested?	They will respond fast and in order.	Yes. Our incident response plan defines severity levels, roles, communication and evidence handling. We test it with a tabletop exercise at least annually; the last was [date].	IR plan summary; tabletop notes
A42	How quickly will you tell us about a breach affecting our data?	A notification commitment they can hold you to.	We will notify affected customers without undue delay and within [72 hours] of confirming a security incident affecting their data, with updates until resolved.	IR plan clause; contract clause
A43	Have you had a security incident or breach in the last [24] months?	Honesty and what you learned.	[No incidents affecting customer data in the last [24] months.] [Or: one incident in [month, year]; describe impact, response and fixes briefly and truthfully.]	Incident log summary
A44	How can someone report a vulnerability to you?	A clear door for security reports.	Security reports can be sent to [security@company.com]. We acknowledge within [2 business days] and publish a disclosure policy at [link/security.txt].	security.txt or disclosure page

Business continuity and backups

ID	Question buyers ask	What they are really checking	Example answer (edit before use)	Evidence to attach
A45	How often do you back up data and test restores?	Data can actually be recovered.	Production databases are backed up [daily with point-in-time recovery], encrypted, and stored in [separate region/account]. Restores are tested at least [annually]; the last test was [date].	Backup config; restore test record
A46	What are your recovery time and recovery point objectives?	How long they could be down, and how much they could lose.	Our targets are RTO [X hours] and RPO [Y hours] for the core service, documented in our business continuity plan and tested [annually].	BC/DR plan summary
A47	What uptime do you commit to and how do we see status?	Reliability they can plan around.	We target [99.9]% monthly uptime [backed by an SLA on enterprise plans]. Live status and incident history are at [status page link].	SLA; status page

Kailash Consult

AI in your product (if used)

ID	Question buyers ask	What they are really checking	Example answer (edit before use)	Evidence to attach
A48	Does the product use AI or large language models? Which providers?	What AI touches their data.	[Yes. Features [X, Y] use [provider/model] through [API/region]. AI providers are listed as subprocessors.] [Or: no AI or machine learning processes customer data.]	AI feature list; subprocessor list
A49	Is our data used to train AI models?	Their data does not improve someone else's product.	No. Customer data is not used to train or fine-tune models, ours or our providers'. Our AI providers are contractually barred from training on it [and retain data for at most [X] days / zero retention].	Provider terms; internal policy
A50	How do you control AI output and errors?	AI mistakes do not become their problem.	AI output is [shown as a suggestion that users review / limited to [scope]]. We test features before release, monitor quality after, and users can report issues in product.	AI feature docs; evaluation notes

The 6 documents buyers usually request

ID	Question buyers ask	What they are really checking	Example answer (edit before use)	Evidence to attach
D1	Information security policy (or policy index)	Shows the program exists and is approved.	Policy set with owner, version and approval date	
D2	Penetration test letter or executive summary	Independent testing in the last 12 months.	Letter from the testing firm; findings fixed and retested	
D3	Architecture and data-flow diagram	Where their data lives and moves.	One page: hosting, services, data stores, encryption, subprocessors	
D4	Incident response plan (summary)	You can handle a breach.	Two-page summary: roles, severity, notification timeline	
D5	Business continuity and backup summary	You can recover.	Backups, RTO and RPO, last restore test date	
D6	SOC 2 report, ISO 27001 certificate, or readiness letter	Independent proof, or a credible date for it.	Under NDA; bridge letter if the report period has ended	

Kailash Consult

Add-on: healthcare (HIPAA)

ID	Question buyers ask	What they are really checking	Example answer (edit before use)	Evidence to attach
H1	Will you sign a Business Associate Agreement?	Required before they share PHI.	Yes. We sign BAAs with covered entities and require BAAs from our own subcontractors that handle PHI.	BAA template
H2	Have you completed a HIPAA security risk analysis?	The core HIPAA Security Rule requirement.	Yes. Our risk analysis under 45 CFR 164.308(a)(1) was completed on [date] and is updated at least annually and after major changes.	Risk analysis summary
H3	Do you log access to PHI?	Audit controls for who saw what. HIPAA's six-year rule covers required documentation, not automatically every access log.	Yes. Access to PHI is logged with user, time and action, kept for [period] under our retention policy [and BAA terms], and reviewed [monthly] for unusual activity.	Audit log sample; retention policy
H4	Is your workforce trained on HIPAA?	Staff know the rules.	All workforce members with PHI access complete HIPAA training at onboarding and annually.	Training records
H5	How do you limit PHI to the minimum necessary?	PHI does not spread to tickets and logs.	PHI access is role-based. Support works from de-identified views where possible, and PHI is filtered from application logs and support tickets.	Access matrix; logging rules
H6	How fast will you notify us of a breach of PHI?	HIPAA and contract timelines.	We notify the covered entity without unreasonable delay after discovery, and in all cases within the HIPAA maximum or any shorter period in our BAA ([X] days).	BAA notification clause

Add-on: banks and financial services

ID	Question buyers ask	What they are really checking	Example answer (edit before use)	Evidence to attach
F1	Can you share financial statements or proof of financial stability?	You will still exist next year.	We can share [funding summary/financial statements] under NDA and a brief continuity plan for the service.	Funding letter or statements
F2	What cyber insurance do you carry?	Who pays if something goes wrong.	We carry cyber liability insurance of [$X] per claim with [carrier]. A certificate of insurance is available on request.	Certificate of insurance

Kailash Consult

ID	Question buyers ask	What they are really checking	Example answer (edit before use)	Evidence to attach
F3	Do you allow customer audits or provide audit rights?	They can verify, not just trust.	We provide our independent reports and answer follow-up questions. Additional audit rights are available [under the enterprise agreement, with reasonable notice].	Contract clause
F4	How do you oversee your own subcontractors (fourth parties)?	Risk does not hide one level down.	Subprocessors with access to customer data are assessed before onboarding and annually, and are bound by security and confidentiality terms at least as strict as ours.	Vendor register; flow-down clause
F5	Is data kept in the United States and how is it protected?	Regulatory location and control.	Customer data is stored in [US region(s)] and encrypted at rest and in transit. Access is restricted to authorized personnel [in the US].	Hosting regions; access matrix
F6	What happens to our data if we exit?	A clean, documented exit.	We provide a full export in [format] on request and certify deletion within [30] days after termination.	Exit and deletion procedure

Add-on: state and agency buyers

ID	Question buyers ask	What they are really checking	Example answer (edit before use)	Evidence to attach
G1	Do you have StateRAMP / GovRAMP or FedRAMP status?	Program status agencies recognize.	[We are [status] with StateRAMP/GovRAMP.] [Or: not yet. Our application has no authorization of its own; it runs on [AWS/Azure] services that are FedRAMP authorized, and we can share our NIST 800-53 control mapping.]	Status letter or control mapping
G2	Can you map your controls to NIST 800-53?	Their framework, not yours.	Yes. We maintain a mapping of our controls to NIST SP 800-53 [moderate baseline] and can share it under NDA.	Control mapping
G3	Is data stored in the US and administered by US persons?	Data sovereignty rules. US persons (citizens or permanent residents) is not the same as US-based staff.	Data is stored only in [US regions]. Administrative access is limited to [US persons / staff located in the US], as the contract requires.	Hosting and access statement
G4	Do you provide an accessibility conformance report (VPAT)?	Section 508 procurement rules.	[Yes, our VPAT based on WCAG 2.1 AA is available.] [Or: in progress, expected [month].]	VPAT
G5	Can you meet our records retention and public records rules?	Agency legal obligations.	We support configurable retention and full export so the agency can meet its records obligations.	Retention settings

Kailash Consult

Free resource from Kailash Consult. Free to use inside your company. Not for resale or redistribution. kailashconsult.com/resources

Kailash Consult