The Enterprise Security Answer Bank

50 ready-to-use template answers organised by the 12 most common question categories from 230+ enterprise security questionnaires

Securilix | TrustOps™ Service

March 2026

This answer bank is built from Securilix's direct experience answering 230+ enterprise security questionnaires across regulated industries including financial services, healthcare, government, and technology. Each category includes the typical question phrasing buyers use, a template answer you can adapt, the evidence you should attach, and the red flags that cause procurement teams to escalate, delay, or reject.

SECURILIX

Contents

00

How to use this answer bank

Each of the 12 categories in this answer bank contains two representative questions. For every question you will find four components:

- **Typical question phrasing** — the way buyers commonly word this question across major frameworks (SIG, CAIQ, HECVAT, and custom questionnaires).
- **Template answer** — a ready-to-adapt response that covers the key points procurement teams expect. Placeholders in [BRACKETS] should be replaced with your organisation's specifics.
- **Evidence to attach** — the supporting documents that strengthen your answer and reduce follow-up questions.
- **Red flags to avoid** — the statements and omissions that cause procurement teams to escalate, delay, or reject.

230+	12	50	24
questions	categories	answers	answers

Based on analysis of 230+ enterprise security questionnaires across 12 categories, covering SIG, SIG Lite, CAIQ, HECVAT, VSA, and custom buyer-specific frameworks. Sectors represented: 38% financial services, 22% technology, 18% healthcare, 12% government, 10% other regulated industries.

01

Information security governance

How your organisation governs and manages information security at a strategic level.

> **Do you have a documented information security policy? When was it last reviewed?**

Template answer

Yes. We maintain a comprehensive Information Security Policy that is approved by senior leadership and reviewed annually, or following any significant organisational or technological change. The policy aligns with ISO 27001:2022 requirements and covers scope, objectives, roles and responsibilities, acceptable use, and compliance obligations. The policy was last reviewed and approved on [DATE].

Evidence to attach

- Information Security Policy (current version)
- Policy review and approval log
- ISO 27001 Statement of Applicability (if certified)

Red flags to avoid

- Saying the policy exists but cannot provide it on request
- Policy dated more than 18 months ago with no evidence of review
- No named policy owner or approving authority

> **Do you have a named individual responsible for information security?**

Template answer

Yes. [NAME/ROLE] serves as our designated Information Security Lead, reporting directly to [SENIOR EXECUTIVE/BOARD]. This individual is responsible for the development, implementation, and ongoing management of our information security programme, including risk assessments, incident response, and compliance. Security is a standing agenda item at our quarterly leadership meetings.

Evidence to attach

- Organisation chart showing reporting line
- Board or leadership meeting minutes referencing security
- Role description or terms of reference

Red flags to avoid

- No named individual — security is 'everyone's responsibility' without ownership
- Security reports through IT operations with no board visibility
- Unable to articulate who holds accountability for security decisions

02

Access control and identity management

How you manage who can access what, and how access is granted, reviewed, and revoked.

> **Do you enforce multi-factor authentication (MFA) for all user access?**

Template answer

Yes. Multi-factor authentication is enforced for all user access to production systems, cloud environments, and administrative consoles. We use [PROVIDER, e.g. Okta, Azure AD, Google Workspace] as our identity provider with hardware tokens or authenticator app-based MFA. MFA is mandatory — it cannot be bypassed or deferred. Privileged accounts require additional step-up authentication.

Evidence to attach

- Identity provider configuration screenshot showing MFA enforcement
- Conditional access or security policy documentation
- Privileged access management (PAM) policy

Red flags to avoid

- MFA is 'available' but not enforced for all users
- MFA not applied to privileged or admin accounts
- Using SMS-only as a second factor without alternative options

> **How do you manage user access provisioning and de-provisioning?**

Template answer

We follow the principle of least privilege for all access provisioning. Access is requested through [SYSTEM, e.g. Jira, ServiceNow], approved by the resource owner, and provisioned by IT. Access reviews are conducted quarterly for all systems containing sensitive data. De-provisioning is automated through our HR-IT integration — when an employee leaves or changes role, access is revoked within 24 hours via our identity provider. Termination access revocation is verified as part of our offboarding checklist.

Evidence to attach

- Access provisioning and de-provisioning procedure
- Evidence of quarterly access reviews
- Automated de-provisioning workflow documentation

- Sample offboarding checklist

Red flags to avoid

- No formal access review process
- Manual de-provisioning with no defined SLA
- Former employees retaining access for weeks after departure
- No evidence of least privilege implementation

03

Data protection and encryption

How you protect data at rest, in transit, and throughout its lifecycle.

> **Do you encrypt data at rest and in transit?**

Template answer

Yes. All data at rest is encrypted using AES-256 encryption. All data in transit is protected using TLS 1.2 or higher. Database encryption is managed through [PROVIDER, e.g. AWS KMS, Azure Key Vault, GCP Cloud KMS] with customer-managed encryption keys available on request. We do not support TLS 1.0 or 1.1, and SSL is fully deprecated across our infrastructure.

Evidence to attach

- Encryption policy document
- TLS configuration scan results
- Key management procedure
- Cloud provider encryption documentation

Red flags to avoid

- Supporting TLS 1.0 or 1.1 in production
- Unable to specify encryption algorithm or key length
- No key rotation policy or evidence of key management
- Encrypting data in transit but not at rest

> **How do you handle data classification and data loss prevention?**

Template answer

We maintain a data classification policy that categorises data into four tiers: Public, Internal, Confidential, and Restricted. Each tier has defined handling requirements for storage, transmission, sharing, and disposal. Data loss prevention (DLP) controls are implemented at the endpoint and network level to prevent unauthorised exfiltration of Confidential and Restricted data. Classification is applied at the point of creation and reviewed during access reviews.

Evidence to attach

- Data classification policy

- DLP tool configuration and coverage
- Data handling matrix by classification tier
- Training records on data handling

Red flags to avoid

- No data classification scheme in place
- All data treated the same regardless of sensitivity
- DLP mentioned but no tooling or enforcement
- Unable to describe how client data is classified

04

Network security

How you protect your network infrastructure from external and internal threats.

> **Describe your network security architecture and segmentation approach.**

Template answer

Our network architecture follows a defence-in-depth model with multiple layers of security controls. We segment our network into distinct zones: production, staging, development, and corporate. Each zone is isolated using firewalls and network access control lists (ACLs). Production environments are further segmented by service and data sensitivity. We use [PROVIDER, e.g. AWS VPC, Azure Virtual Network] for cloud network isolation with security groups enforcing least-privilege connectivity between services.

Evidence to attach

- Network architecture diagram
- Firewall rule set documentation
- Segmentation policy
- Cloud security group configuration

Red flags to avoid

- Flat network with no segmentation
- Unable to produce a network diagram
- Development and production environments sharing the same network
- No firewall change management process

> **Do you perform regular vulnerability scanning and penetration testing?**

Template answer

Yes. We perform automated vulnerability scanning on a continuous basis using [TOOL, e.g. Qualys, Tenable, Rapid7]. Critical and high-severity vulnerabilities are remediated within 14 days; medium-severity within 30 days. We commission independent, third-party penetration testing at least annually, covering external infrastructure, web applications, and API endpoints. Results are reviewed by our security team, findings are tracked to remediation, and the executive summary is available to customers on request under NDA.

Evidence to attach

- Most recent penetration test executive summary
- Vulnerability management policy
- Remediation SLA documentation
- Scanning tool dashboard or report sample

Red flags to avoid

- No penetration testing in the last 12 months
- Penetration testing performed internally with no third-party validation
- Unable to share even a summary of findings
- No defined remediation timelines for vulnerabilities

05

Incident response and management

How you detect, respond to, and recover from security incidents.

> **Do you have a documented incident response plan? How often is it tested?**

Template answer

Yes. We maintain a documented Incident Response Plan that defines roles, responsibilities, escalation procedures, communication protocols, and post-incident review processes. The plan follows the NIST SP 800-61 framework and covers identification, containment, eradication, recovery, and lessons learned. We test the plan at least annually through tabletop exercises and simulated incidents. The plan was last tested on [DATE], and findings were incorporated into the current version.

Evidence to attach

- Incident Response Plan (current version)
- Tabletop exercise report or evidence of testing
- Incident response contact list
- Post-incident review template

Red flags to avoid

- Plan exists but has never been tested
- No defined escalation path or communication protocol
- No post-incident review process
- Incident response is ad-hoc with no documented procedure

> **What is your notification timeline if a security incident affects our data?**

Template answer

We commit to notifying affected customers within 72 hours of confirming a security incident that involves their data, in line with GDPR requirements and industry best practice. Initial notification includes: nature of the incident, data potentially affected, containment actions taken, and designated point of contact. We provide ongoing updates until the incident is fully resolved and deliver a post-incident report within 30 days of closure. Our Data Processing Agreement (DPA) formalises these obligations.

Evidence to attach

- Breach notification procedure
- Data Processing Agreement (DPA) template
- Incident communication template
- Evidence of previous incident handling (if applicable, anonymised)

Red flags to avoid

- No defined notification timeline
- Notification only 'when legally required' with no proactive commitment
- Unable to provide a DPA or breach notification clause
- No evidence of ever having managed an incident (for mature organisations this raises questions)

06

Business continuity and disaster recovery

How you ensure operational resilience and recover from disruptive events.

> **Do you have documented business continuity and disaster recovery plans?**

Template answer

Yes. We maintain separate but integrated Business Continuity (BCP) and Disaster Recovery (DR) plans. The BCP covers people, processes, and facilities. The DR plan covers technology recovery, including defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for each critical system. Our production infrastructure is hosted across multiple availability zones with automated failover. Both plans are reviewed and tested annually.

Evidence to attach

- Business Continuity Plan summary
- Disaster Recovery Plan with RTO/RPO definitions
- DR test results from most recent exercise
- Cloud infrastructure availability zone configuration

Red flags to avoid

- No defined RTO or RPO values
- Plans exist but have never been tested
- Single availability zone or data centre with no redundancy
- Unable to articulate recovery capabilities for specific services

> **How are system backups managed and tested?**

Template answer

System backups are automated and performed daily for all production databases and critical systems. Backups are encrypted using AES-256 and stored in a geographically separate location from the primary data. Backup integrity is verified through automated checksum validation, and full restore tests are conducted quarterly. Backup retention follows our data retention policy: 30 days for operational backups, 12 months for compliance-required data.

Evidence to attach

- Backup policy and schedule

- Backup encryption documentation
- Most recent backup restoration test results
- Retention schedule

Red flags to avoid

- Backups not encrypted
- No evidence of backup restore testing
- Backups stored in the same region or facility as production
- No defined retention period

07

Compliance and certifications

What compliance frameworks you adhere to and how you demonstrate ongoing compliance.

> What security certifications or compliance frameworks do you hold?

Template answer

We hold [CERTIFICATIONS, e.g. ISO 27001:2022 certification (Certificate No. [NUMBER], issued by [BODY], valid until [DATE])]. We also maintain SOC 2 Type II compliance, with our most recent report covering the period [DATES]. Our controls are mapped to [ADDITIONAL FRAMEWORKS as applicable, e.g. NIST CSF 2.0, CIS Controls v8, GDPR]. Copies of our ISO certificate and SOC 2 Type II report are available on request under NDA.

Evidence to attach

- ISO 27001 certificate
- SOC 2 Type II report (under NDA)
- Compliance mapping document
- Audit schedule and next audit date

Red flags to avoid

- Claiming compliance without holding certification
- Certificate expired or audit overdue
- SOC 2 Type I only when Type II was expected
- Unable to share any compliance documentation

> How do you ensure ongoing compliance between audit cycles?

Template answer

We maintain continuous compliance through a combination of automated monitoring, internal audits, and management reviews. Our GRC platform tracks control effectiveness against our Statement of Applicability. Internal audits are conducted quarterly, covering a rotating selection of controls. Management reviews occur at least annually and assess the performance of the entire information security management system. Any non-conformities identified are tracked through our corrective action process with defined remediation timelines.

Evidence to attach

- Internal audit schedule and recent audit report
- Management review minutes
- GRC platform dashboard or evidence of continuous monitoring
- Corrective action log

Red flags to avoid

- No activity between annual audits
- No internal audit programme
- Corrective actions from previous audits still open with no progress
- Compliance treated as a point-in-time exercise

08

Human resources and security awareness

How you manage the human element of security through hiring, training, and awareness.

> **Do you conduct background checks on employees with access to sensitive data?**

Template answer

Yes. All employees undergo pre-employment background checks appropriate to their role and the data they will access. Checks include identity verification, right-to-work confirmation, and criminal record screening where legally permitted. For roles with access to highly sensitive or regulated data, enhanced checks are conducted including professional reference verification and, where applicable, credit screening. Background check requirements are defined in our HR Security Policy.

Evidence to attach

- HR Security Policy
- Background check procedure
- Evidence of screening provider or process
- Role-based screening matrix

Red flags to avoid

- No background checks conducted
- Background checks only for 'senior' roles
- Unable to describe what checks are performed
- No contractual security obligations for employees

> **Do you provide security awareness training to all employees?**

Template answer

Yes. All employees complete mandatory security awareness training during onboarding and annually thereafter. Training covers: phishing recognition, social engineering, data handling, incident reporting, password hygiene, and acceptable use of company systems.
Role-specific training is provided for developers (secure coding), IT administrators (privileged access management), and customer-facing teams (data privacy). We supplement formal training with regular phishing simulations, achieving an average click-through rate below [X]%.

Evidence to attach

- Training programme outline and curriculum
- Training completion records
- Phishing simulation results
- Role-specific training documentation

Red flags to avoid

- No formal training programme
- Training is optional or has low completion rates
- No phishing simulations or testing
- Training content not updated in over 12 months

09

Third-party and supply chain risk

How you manage security risks from your own vendors and subprocessors.

> Do you have a third-party vendor risk management programme?

Template answer

Yes. We maintain a formal Third-Party Risk Management (TPRM) programme that assesses all vendors who access, process, or store data on our behalf. Vendors are tiered by risk level (Critical, High, Medium, Low) based on the nature of data accessed and the criticality of the service. Critical and High-risk vendors undergo a full security assessment before onboarding, including review of their certifications, penetration test results, and incident history. Reassessments are conducted annually for Critical vendors and biannually for High-risk vendors.

Evidence to attach

- Third-party risk management policy
- Vendor risk assessment template
- Vendor risk register or inventory
- Evidence of vendor reassessments

Red flags to avoid

- No formal vendor assessment process
- Unable to provide a list of subprocessors
- No ongoing monitoring or reassessment of existing vendors
- Vendor risk management is informal or ad-hoc

> Can you provide a list of subprocessors who may access our data?

Template answer

Yes. We maintain a current subprocessor list that identifies all third parties who may access, process, or store customer data as part of our service delivery. The list includes the subprocessor name, service provided, data processed, and hosting location. Our current subprocessor list is available at [URL or on request]. We notify customers of any changes to subprocessors with at least 30 days' advance notice, as defined in our Data Processing Agreement.

Evidence to attach

- Subprocessor list (current version)
- Data Processing Agreement with subprocessor notification clause
- Subprocessor change notification template
- Evidence of subprocessor security assessments

Red flags to avoid

- Unable to provide a subprocessor list
- No advance notification process for subprocessor changes
- Subprocessors located in jurisdictions without adequate data protection
- No security assessment of subprocessors conducted

10

Application security and SDLC

How you build and maintain secure software through your development lifecycle.

> **Describe your secure software development lifecycle (SDLC).**

Template answer

We follow a secure SDLC that integrates security at every stage of development. Threat modelling is conducted during design. Code reviews include security-focused review by peers. Static Application Security Testing (SAST) runs automatically in our CI/CD pipeline on every pull request. Dynamic Application Security Testing (DAST) is performed on staging environments before release. Dependencies are scanned for known vulnerabilities using [TOOL, e.g. Snyk, Dependabot]. All findings are triaged and resolved before production deployment.

Evidence to attach

- SDLC documentation or development security policy
- CI/CD pipeline configuration showing security gates
- SAST/DAST tool output examples
- Dependency scanning evidence

Red flags to avoid

- No security integration in the development process
- Security testing only performed manually or ad-hoc
- No dependency scanning or known-vulnerable libraries in production
- No evidence of code review practices

> **How do you manage application vulnerabilities and patching?**

Template answer

Application vulnerabilities are managed through our vulnerability management programme. Critical vulnerabilities are patched within 24 hours. High-severity within 7 days. Medium within 30 days. We subscribe to vendor security advisories and CVE feeds relevant to our technology stack. Patch deployment follows our change management process, with emergency patches having an expedited approval path. All patches are tested in staging before production deployment.

Evidence to attach

- Vulnerability management policy with SLAs
- Patch management procedure
- Evidence of recent patching activity
- Change management process documentation

Red flags to avoid

- No defined patching SLAs
- Known critical vulnerabilities unpatched for extended periods
- No change management process for patches
- Unable to describe vulnerability discovery and triage process

11

Privacy and data processing

How you handle personal data, meet privacy obligations, and support data subject rights.

> Are you GDPR compliant? Do you have a Data Protection Officer?

Template answer

Yes. We are fully compliant with the UK GDPR and EU GDPR. We have appointed a Data Protection Officer (DPO) who can be contacted at [EMAIL]. We maintain Records of Processing Activities (ROPA), conduct Data Protection Impact Assessments (DPIAs) for high-risk processing, and have established procedures for handling Data Subject Access Requests (DSARs) within the statutory 30-day timeline. Our Privacy Policy is publicly available at [URL].

Evidence to attach

- Privacy Policy
- Data Protection Impact Assessment template or example
- DSAR handling procedure
- Records of Processing Activities
- DPO appointment documentation

Red flags to avoid

- Claiming GDPR compliance but unable to produce a ROPA
- No DPO or privacy lead appointed
- No DSAR handling procedure
- Privacy policy outdated or not publicly accessible

> Where is our data stored and processed? Do you transfer data internationally?

Template answer

Customer data is stored and processed in [REGION, e.g. EU (Ireland), UK (London), US (Virginia)]. Our primary infrastructure is hosted on [PROVIDER, e.g. AWS, Azure, GCP] in [SPECIFIC REGIONS]. Where international data transfers occur, they are governed by appropriate safeguards including Standard Contractual Clauses (SCCs) and Transfer Impact Assessments (TIAs) in accordance with GDPR Chapter V requirements. Data residency options are available for customers with specific jurisdictional requirements.

Evidence to attach

- Data processing locations documentation
- Standard Contractual Clauses (executed)
- Transfer Impact Assessment
- Cloud provider data residency documentation

Red flags to avoid

- Unable to specify where data is stored
- International transfers with no legal basis documented
- No SCCs or alternative transfer mechanism in place
- Data stored in jurisdictions without adequacy decisions and no safeguards

12

Physical and environmental security

How you secure physical access to facilities and infrastructure.

> What physical security controls protect your data centres or offices?

Template answer

Our production infrastructure is hosted on [PROVIDER, e.g. AWS, Azure, GCP], which maintains SOC 2 Type II certified data centres with enterprise-grade physical security controls including 24/7 security personnel, biometric access controls, CCTV surveillance, mantraps, and environmental controls (fire suppression, climate control, redundant power). Our corporate offices implement access control systems, visitor management procedures, and CCTV. Sensitive areas within the office (e.g. server rooms, if applicable) require additional authorisation.

Evidence to attach

- Cloud provider SOC 2 Type II report or physical security documentation
- Office access control policy
- Visitor management procedure
- Clean desk policy

Red flags to avoid

- Unable to describe physical security at the data centre level
- No visitor management procedure
- Sensitive data accessible from uncontrolled areas
- No clean desk or physical security policy for the office environment

> What environmental controls are in place to protect infrastructure?

Template answer

Our cloud infrastructure provider maintains comprehensive environmental controls including redundant power supplies with UPS and generator backup, fire detection and suppression systems (pre-action dry pipe or gas-based), climate control systems with continuous monitoring, and water detection systems. These controls are independently audited as part of the provider's SOC 2 Type II certification. For our corporate environment, we maintain fire alarms, suppression systems, and have an emergency evacuation procedure that is tested annually.

Evidence to attach

- Cloud provider environmental controls documentation
- Office fire safety certification
- Emergency evacuation procedure
- Building compliance certificates

Red flags to avoid

- Unable to describe environmental controls at any level
- No fire suppression in areas containing IT equipment
- No emergency or evacuation procedures
- Single point of failure for power or cooling

Stop copy-pasting from old questionnaires

Our TrustOps™ service answers security & due diligence questionnaires in 24 hours on your behalf. AI-assisted drafting with senior consultant, human led review. Every response verified, evidence-ready, and built to close deals.

1. Book a qualification call — 30 minutes, honest assessment

2. Experience a TrustOps™ Pilot — we respond to one real questionnaire

3. Onboard in weeks — dedicated consultant, agreed SLA, continuous improvement

Apply now at securilix.com/pilot

hello@securilix.com