The 12 Most Common Enterprise Security & Due Diligence Questions

What Enterprise & Regulated Buyers Actually Want to Know Before They Sign: Analysis From Answering 154 Questionnaires in 2025

Securilix | TrustOps™ Service
March 2026

Executive Summary

Security & due diligence questionnaires have become the single largest bottleneck in B2B sales cycles. Every service provider selling into large enterprises, financial services, healthcare, and regulated industries now faces the same reality: before a contract is signed, procurement teams send a long, intrusive security questionnaire. These documents routinely run to 60, 80, sometimes more than 100 questions, each requiring specific evidence, not just assertions. The typical response cycle takes two to three weeks of back-and-forth between your engineering team, IT leaders, compliance function, and the buyer's procurement desk. For growing companies closing four or five plus enterprise customers per quarter, that means your most senior technical leaders are spending 40 to 80 hours every three months just answering questionnaires.

The common assumption is that holding an ISO 27001 certificate or a SOC 2 Type II report should eliminate the need for questionnaires. It does not. In our experience across 154 enterprise security questionnaires collected from banks, insurance companies, government bodies, and large corporates, every single buyer still issued a bespoke questionnaire regardless of what certifications the supplier held. Certifications get your foot in the door, they signal that a baseline exists. Enterprise procurement teams have learned that a point-in-time audit certificate does not guarantee that controls are still operating six months later. Questionnaires exist to verify that what was true during the audit is still true today, and that the suppliers security programme extends into the specific areas the buyer cares about: supply chain governance, access control enforcement, incident detection speed, and data handling practices.

To give suppliers a genuine advantage, we analysed all 154 questionnaires that Securilix answered in 2025 and identified the 12 question categories that appear most frequently. These are not obscure or niche topics. They are the questions that every enterprise buyer, across every regulated sector consistently asks. Understanding them, and preparing evidence-ready answers in advance, is the difference between operational chaos to closing large customer in weeks, not watching them stall for months. This report breaks down each question category: why buyers ask it, what it reveals about their risk appetite, what evidence they expect to see, and the specific red flags that cause procurement teams to escalate, delay, or walk away from a supplier entirely.

154	12	60-100+	2-3 Wks
Questionnaires Analysed	Question Categories Identified	Questions Per Questionnaire	Answering & Preparing Time

Who This Report Is For

This report was written for technology leaders, compliance heads, and commercial teams at companies selling into enterprise and regulated buyers. If any of the following apply to you, the analysis that follows will be relevant:

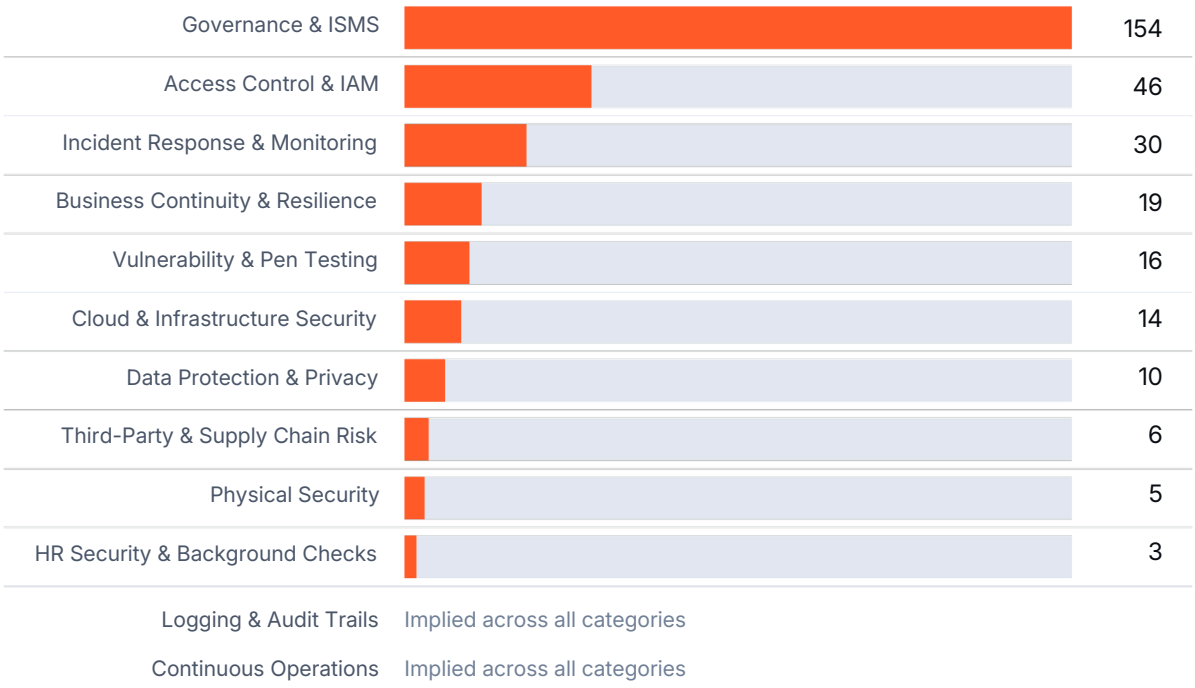
- You are a CTO / Senior Engineer, or Sales, IT, or Compliance leader who personally answers security questionnaires from enterprise buyers
- Your sales team regularly loses momentum during procurement because questionnaire responses take weeks
- You hold ISO 27001 or SOC 2 but still receive bespoke questionnaires from every new enterprise or regulated customer
- You are scaling into regulated sectors (financial services, insurance, government, healthcare, etc) and encountering enterprise security requirements for the first time
- Your team spends a combined 10–20 hours per questionnaire, pulling senior staff away from core work and role responsibilities

Methodology & Data Source

This analysis is based on 154 security questionnaires answered by Securilix during 2025. Questionnaires were received from buyers across financial services (38%), general enterprises (22%), government and public sector (16%), large corporates (14%), and healthcare and life sciences (10%). Each questionnaire was categorised by question topic, and individual question signals were tagged to one of 12 categories. A single questionnaire may generate multiple signals within one category, for example, a governance section containing three distinct sub-questions about risk treatment, executive approval, and asset inventory would be counted as three signals within the Governance & ISMS category. Signal counts reflect the total number of distinct question signals across the full dataset, not the number of questionnaires in which the category appeared. The frequency chart on the following page shows the number of questionnaires (of 154) in which each category appeared.

Question Frequency Overview

The chart below shows how often each of the 12 question categories appeared across the 154 enterprise security questionnaires in our analysis. Governance and ISMS dominates, appearing in every questionnaire and generating the highest total signal count, followed by Access Control and Incident Response. The frequency distribution reveals a clear hierarchy - Buyers prioritise structural and procedural controls above all else.



Note: "Signal count" represents the average number of distinct question signals related to each category across all 154 questionnaires. A single questionnaire may generate multiple signals within one category, for example, a governance section that asks separately about policy ownership, risk assessments, internal audits, and management review generates four signals. Categories 11 and 12 are patterns that emerge across multiple categories rather than standalone question sections.

01 Governance & ISMS

> Sample Question: "Do you have a formal Information Security Management System (ISMS)? Please provide evidence of security ownership, documented policies, risk assessment cadence, internal audit, management review, and current certifications (ISO 27001, SOC 2)."

Signal Count: 154 of 154 questionnaires

Why Buyers Ask This

Governance is the foundation of every enterprise security assessment because it tells the buyer whether your security programme is deliberate or accidental. Procurement teams have seen too many suppliers claim strong security while running ad hoc processes that depend on one person's knowledge. When a buyer asks for evidence of an ISMS, they are really asking: "If your lead engineer leaves tomorrow, do your security controls survive?" Without formal governance — a named owner, documented policies, recurring reviews, and independent audits — buyers assume controls will decay post-sale.

What This Reveals About Procurement Risk

Enterprise procurement treats security governance as a proxy for operational maturity. A supplier without an ISMS is a supplier without structure. This question had the highest signal count in our analysis by a significant margin: governance is the precondition for every other control on this list. No governance means no deal progression.

What Buyers Expect

- Named security owner (CISO, VP Engineering, or designated role) visible on the org chart with clear reporting lines
- Documented information security policy approved by leadership, reviewed at least annually
- Quarterly or annual risk assessments with documented methodology and management sign-off
- Evidence of internal audits or third-party assessments (ISO 27001, SOC 2 Type II) with remediation tracking
- Management review meetings with documented agendas, attendees, decisions, and follow-up actions

Evidence Requirements

Policies, org charts showing security ownership, risk registers, audit reports, management review minutes, and certificates of current certifications.

Red Flags

- "We're working on ISO 27001" with no auditor engaged, no timeline, and no gap assessment evidence
- Security owned by "the team" with no named individual accountable
- No evidence of recurring reviews or audits - Policies exist but haven't been reviewed since creation

02 Access Control & IAM

> Sample Question: "Is multi-factor authentication (MFA) implemented for: A) Remote access into production, B) Access to privileged systems, C) Customer data access? Are personal devices permitted to access production environments?"

Signal Count: 46 of 154 questionnaires

Why Buyers Ask This

Access control failures are the number one cause of breaches in third-party suppliers, and enterprise buyers know this from their own incident data. When a buyer asks about your IAM practices, they are running a mental model of what happens when one of your employees' credentials is compromised. Can an attacker move laterally from a developer laptop to production? Can a leaver still access customer data after their last day? These are not theoretical, they are scenarios procurement teams have seen play out in real supplier breaches.

What This Reveals About Procurement Risk

Buyers treat MFA as an absolute minimum. If you do not have it enforced universally (not just available, but enforced) procurement will question your entire security posture. The logic is straightforward: If a supplier cannot implement the most basic access control, what else have they missed?

What Buyers Expect

- MFA enforced on all production access (SSO, VPN, admin consoles) with no exceptions
- Documented least privilege access model with quarterly access reviews
- Formal joiner/mover/leaver (JML) process with verified deprovisioning on departure day
- Clear separation between development and production environments
- Defined personal device policy - MDM for BYOD or outright prohibition for production access

Evidence Requirements

MFA enforcement screenshots/exports, access review logs, JML process documentation, privilege escalation workflows, and device management policies.

Red Flags

- "Most of our users have MFA enabled" - Not enforced universally, with exceptions for legacy accounts
- No documented access review process, or reviews triggered only by audits rather than on schedule
- Developers have standing production access with no time-limited elevation or approval workflow

03 Incident Response & Monitoring

> Sample Question: "Do you have a documented incident response plan? Has it been tested in the last 12 months? Are employees with access to customer data monitored with proxy policies to detect data exfiltration attempts?"

Signal Count: 30 of 154 questionnaires

Why Buyers Ask This

Buyers are not primarily concerned with whether you have ever had a breach. They care about whether you would know if you were having one right now, and how quickly you would tell them. In regulated industries, the buyer's own obligations (GDPR's 72-hour window, FCA requirements, PRA expectations) depend on how fast their suppliers detect and report incidents. Slow incident response from a supplier creates direct regulatory exposure for the buyer.

What This Reveals About Procurement Risk

The subtext of every incident response question is: "Can we trust you to be honest and fast when things go wrong?" Procurement teams look for evidence of structured, tested, and rehearsed incident response, not a document written once and filed away. A plan that has never been exercised is a plan that will fail under pressure.

What Buyers Expect

- Documented IR plan with defined roles, escalation paths, and notification timelines
- Evidence of testing within 12 months - Tabletop exercises, simulated incidents, or after-action reviews
- Security monitoring infrastructure - SIEM, EDR, CloudTrail/GuardDuty, with defined alerting thresholds
- Contractual breach notification timelines (typically 48–72 hours)
- Incident ticketing system with historical records and root cause analysis

Evidence Requirements

IR plan, test reports, monitoring dashboard screenshots, sample security alerts, post-incident review documents.

Red Flags

- "We'd figure it out if something happened" - No documented plan, no defined roles, no rehearsed process
- No evidence of monitoring or alerting: no SIEM, no EDR, no cloud-native detection tools
- IR plan never tested, or last tested more than 18 months ago

04 Business Continuity & Resilience

> Sample Question: "What are your backup and disaster recovery procedures? What are your RTO/RPO targets? When was your last restore test? Do you have a network diagram depicting how data enters, processes, and transfers?"

Signal Count: 19 of 154 questionnaires

Why Buyers Ask This

When buyers integrate your service into their operations, your downtime becomes their downtime. For enterprises with thousands of customers, or critical service providers, service disruption triggers regulatory reporting, customer compensation, and reputational damage far exceeding the cost of the contract. Business continuity questions are about supply chain dependency. The buyer is asking: "If your data centre goes down at 3am, what happens to our operations at 9am?"

What This Reveals About Procurement Risk

Buyers treat BC/DR as a first-order supply chain risk. They are not asking whether you back up data, they assume you do. They want to know whether you have tested restoration, know how long recovery takes, and have thought through failure scenarios. Network and data flow diagrams are particularly telling: if you cannot articulate how data moves through your systems, buyers conclude you cannot predict how a failure will propagate.

What Buyers Expect

- Documented backup schedule with encrypted storage and geographic separation
- Defined RTO and RPO targets appropriate for the buyer's service level requirements
- Evidence of restore testing at least quarterly, with documented actual recovery times
- DR/BC plan covering failover procedures, communication plans, and dependency management
- Current network and data flow diagrams

Evidence Requirements

Backup logs, restore test reports with actual metrics, BC/DR plan, architecture diagrams, and service-level documentation showing RTO/RPO commitments.

Red Flags

- "We use AWS, so backups are automatic" - No restore testing, no defined RTO/RPO, no shared responsibility awareness
- No defined or documented RTO/RPO targets, or targets never validated through testing
- Network diagrams that do not exist, are visibly outdated, or do not reflect current architecture

05 Vulnerability & Penetration Testing

> Sample Question: "Are all servers and workstations that process customer data patched on a regular basis? When was your last penetration test? What is your vulnerability remediation timeline for critical/high findings?"

Signal Count: 16 of 154 questionnaires

Why Buyers Ask This

Unpatched vulnerabilities are among the easiest attack vectors, and buyers know that suppliers are disproportionately targeted because attackers assume weaker patch management. Buyers ask about vulnerability management not because they expect perfection, but because they want a disciplined, continuous process for finding and fixing vulnerabilities. The emphasis on remediation timelines is critical: finding vulnerabilities is only half the equation.

What This Reveals About Procurement Risk

Enterprise procurement increasingly expects continuous vulnerability management rather than annual pen tests. A test conducted twelve months ago says nothing about today. Buyers want ongoing scanning, defined patching cadences, and specific remediation SLAs. This shift from periodic assessment to continuous management is one of the clearest trends in our 154-questionnaire analysis.

What Buyers Expect

- Regular vulnerability scanning (weekly or monthly) across all environments processing customer data
- Documented patching cadence: critical patches within 7–14 days, high within 30, medium within 90
- Annual penetration test by a qualified third-party firm
- Defined remediation SLAs by severity with tracking and escalation for overdue findings
- Vulnerability tracking system with historical records

Evidence Requirements

Pen test reports (executive summary acceptable), patch management logs, vulnerability scan results, remediation tracking data, and patching policy documentation.

Red Flags

- "We patch when needed" - No schedule, no documented cadence, no tracking of patch compliance
- Last pen test over 12 months ago, or scope excluded production systems handling customer data
- No vulnerability scanning tool deployed, or scanning limited to a subset of the environment

06 Cloud & Infrastructure Security

> Sample Question: "If you use AWS/Azure/GCP, describe: A) Encryption at rest and in transit, B) Logging and monitoring (CloudTrail, GuardDuty), C) Configuration baselines (CIS benchmarks), D) Identity boundaries and IAM policies."

Signal Count: 14 of 154 questionnaires

Why Buyers Ask This

Cloud misconfigurations are the second most common cause of supplier breaches after access control failures. The days when "we use AWS" was an acceptable security answer are over. Buyers now expect suppliers to demonstrate active configuration and hardening of their cloud environment. The question structure (encryption, logging, baselines, identity) mirrors the shared responsibility model. Buyers are testing whether suppliers understand what they are responsible for within that model.

What This Reveals About Procurement Risk

This category reveals growing sophistication among procurement teams. Five years ago, confirming a major cloud provider was enough. Today, buyers ask about specific configurations, specific tools, and specific benchmarks. The level of technical detail reflects a procurement ecosystem that has been burned by suppliers running on default cloud configurations.

What Buyers Expect

- Encryption at rest (AES-256) and in transit (TLS 1.2+) applied consistently across all services
- Cloud logging enabled and retained — CloudTrail, VPC Flow Logs, GuardDuty or equivalent
- Configuration management via IaC (Terraform, CloudFormation) with CIS benchmark baselines
- IAM least privilege with regular review and no root/overprivileged accounts for daily operations
- CSPM tooling or regular manual audits to detect configuration drift

Evidence Requirements

Cloud security configurations/exports, encryption settings, logging evidence, IAM policies and role definitions, and CSPM scan results or manual audit records.

Red Flags

- Default cloud provider settings with no evidence of hardening or configuration review
- CloudTrail or equivalent logging disabled, or logs retained less than 90 days with no centralisation
- Encryption "depends on the service" - No consistent, documented encryption standard

07 Data Protection & Privacy

> Sample Question: "Is encryption (AES-256 or similar) implemented for customer data at rest and in transit? How are passwords protected (hashing method)? What is your data retention and deletion policy? Do you have a Data Processing Agreement (DPA)?"

Signal Count: 10 of 154 questionnaires

Why Buyers Ask This

GDPR, CCPA, and sector-specific regulations have fundamentally changed supplier procurement. Under GDPR, the buyer, as data controller, is jointly liable for how their processors handle personal data. A suppliers data protection failure becomes the buyer's regulatory fine. Enterprise legal teams routinely cite real enforcement actions when justifying the depth of their data protection questions. Buyers need both contractual protection (DPAs) and technical evidence to satisfy their own compliance.

What This Reveals About Procurement Risk

Privacy and security are now treated as a single discipline. Buyers will not accept strong technical controls paired with weak privacy governance. The inclusion of password hashing methods, asking specifically about bcrypt or Argon2 versus MD5, shows procurement teams are becoming technically literate. Weak privacy governance signals risk beyond security, into legal and regulatory territory.

What Buyers Expect

- Data classification scheme (public, internal, confidential, restricted) with handling rules per tier
- Encryption at rest (AES-256) and in transit (TLS 1.2+) with documented key management
- Password hashing using bcrypt, Argon2, or scrypt - Never MD5 or unsalted SHA1
- Documented data retention policy with automated deletion processes
- Signed DPA available before processing begins, with transparent subprocessor list

Evidence Requirements

DPA template, data classification policy, encryption documentation including key management, retention schedules with deletion evidence, and current subprocessor list.

Red Flags

- "We delete data when customers ask" - No policy, no automated process, no defined retention periods
- No DPA available, or a DPA not reviewed since GDPR came into force
- Passwords stored using MD5, unsalted SHA1, or any deprecated hashing algorithm

08 Third-Party & Supply Chain Risk

> Sample Question: "Do you conduct security assessments of your subprocessors/vendors? Are security requirements included in vendor contracts? How often do you review vendor risk?"

Signal Count: 6 of 154 questionnaires

Why Buyers Ask This

Your suppliers are their suppliers. When a buyer entrusts data to your platform or ecosystem, they are implicitly entrusting it to every subprocessor in your supply chain. The SolarWinds and MOVEit breaches demonstrated what happens when supply chain security fails. Buyers in regulated industries are now required by their regulators (FCA, PRA, OCC) to understand fourth-party risk. They need to know how you manage your own suppliers, because your suppliers' weaknesses become their exposure.

What This Reveals About Procurement Risk

Enterprise buyers treat supply chain risk as first-class risk, equal to your internal controls. A supplier who claims strong internal security but cannot demonstrate governance over their supply chain creates unquantifiable risk that regulated buyers cannot accept. The lower signal count does not indicate lower importance; supply chain questions are often embedded within broader governance sections.

What Buyers Expect

- Supplier security assessment process (questionnaires, audits, certifications) before onboarding and at defined intervals
- Security requirements in supplier contracts: data handling, incident notification, audit rights, termination provisions
- Annual supplier risk reviews based on data criticality
- Subprocessor register maintained and updated at least quarterly
- Supplier incident notification requirements enabling timely buyer notification

Evidence Requirements

Supplier risk policy, subprocessor list, sample supplier contracts with security clauses, assessment records, and evidence of annual review execution.

Red Flags

- "We trust our suppliers" - No formal assessment, no documented criteria, no ongoing review
- No subprocessor visibility: cannot produce a list of third parties with access to buyer data
- Supplier contracts contain no security requirements, audit rights, or incident notification obligations

09 Physical Security

> Sample Question: "What physical security controls are in place at your offices and data centres? Are access logs maintained? Is visitor access controlled?"

Signal Count: 5 of 154 questionnaires

Why Buyers Ask This

Physical access equals logical access. If someone can walk into your office, sit down at an unlocked workstation, and access your network, every technical control becomes irrelevant. Enterprise buyers understand defence-in-depth, and physical security is a layer that cannot be bypassed with software. For buyers in financial services and government, physical security questions are also driven by regulatory frameworks that explicitly require physical access controls.

What This Reveals About Procurement Risk

Physical security questions reveal whether a suppliers security thinking extends beyond the cloud console. The rise of remote and hybrid working has made this more nuanced, buyers now ask not just about offices, but about how suppliers manage physical security when employees work from home or co-working spaces.

What Buyers Expect

- Badge/keycard access with electronic logging of entry and exit events
- Visitor sign-in and escort procedures for non-employees in secure areas
- Data centre security - self-managed with documented controls, or SOC 2 from hosting provider
- Secure hardware disposal with verified wiping and destruction certificates

Evidence Requirements

Physical access control policy, visitor logs, data centre SOC 2 reports, hardware disposal procedures, and destruction certificates.

Red Flags

- Co-working space or shared office with no dedicated access controls and no compensating measures
- No visitor management process - Anyone can enter without sign-in or escort
- "We use AWS" offered as the sole answer, with no mention of office or endpoint physical security

10 HR Security & Background Checks

> Sample Question: "Do you conduct background checks on employees with access to customer data? Is security awareness training mandatory? How often do you run phishing simulations?"

Signal Count: 3 of 154 questionnaires

Why Buyers Ask This

People remain the weakest link, and enterprise buyers know this from decades of incident data. Social engineering, phishing, and insider threats consistently feature in breach reports. Buyers want evidence that you screen employees before granting data access and continuously train them to recognise common attack techniques. The emphasis on phishing simulations reflects a shift from compliance-driven training to effectiveness-driven training.

What This Reveals About Procurement Risk

Buyers assume insider threats and social engineering are inevitable. Background checks provide baseline trust; ongoing training builds operational resilience. The combination signals to buyers that you treat human risk with the same discipline applied to technical controls.

What Buyers Expect

- Background checks (DBS in UK, equivalent globally) for all employees and contractors with data access
- Annual mandatory security awareness training with documented completion rates
- Quarterly phishing simulations with measured metrics and evidence of improvement
- Role-based training: secure coding for devs, privileged access for admins, social engineering for executives

Evidence Requirements

HR screening policy, training completion reports, phishing simulation results showing trends, training platform screenshots, and role-based curriculum documentation.

Red Flags

- No background checks, or checks limited to senior hires while excluding contractors with equal data access
- Training is "recommended" but not mandatory - No completion tracking, no enforcement
- No phishing simulations, or simulations run once without follow-up or remediation

11 Logging & Audit Trails

> Sample Question: "Are all administrative actions logged? How long are logs retained? Are logs monitored for suspicious activity? Can logs be modified by administrators?"

Signal: Implied — Identified across all 154 questionnaires

Why Buyers Ask This
Logs are the evidence that controls work. Every other security measure (access control, incident response, vulnerability management, configuration baselines) depends on logging to prove execution and enable investigation. Without comprehensive, tamper-resistant logging, your security controls are assertions without evidence. When buyers ask about logging, they are asking about forensic readiness: if something goes wrong, can you trace what happened, who did it, and when?

What This Reveals About Procurement Risk
Logging questions reveal the buyer's need for forensic capability and evidence of control execution. The question about administrator access to logs is especially telling: buyers want to know that the people running your systems cannot quietly delete evidence of what they, or an attacker using their credentials, have done.

What Buyers Expect
- Centralised logging (SIEM: Splunk, Elastic, CloudWatch etc) aggregating logs from all critical systems
- Log retention of at least one year; up to seven years for regulated industries
- Integrity protection - Write-once storage, separate access controls, or cryptographic verification
- Active monitoring and alerting on critical events: failed auth, privilege escalation, data access anomalies

Evidence Requirements
Log retention policy, SIEM configuration, sample audit trails, integrity protection mechanisms, and alerting rule documentation.

Red Flags
- Logs retained "for a while" - No defined retention period, no policy, no commitment
- No centralised logging: logs scattered across systems with no aggregation, correlation, or alerting
- Administrators can modify or delete log entries, undermining forensic integrity

12 Continuous Operations Over Point-in-Time Audits

> Key Insight: Across all 154 questionnaires, buyers consistently demand evidence of ongoing processes: quarterly access reviews, ongoing vulnerability scanning, recurring vendor assessments, regular phishing simulations, and tested backups - Not just scheduled ones.

Signal: Implied — Identified across all 154 questionnaires

Why Buyers Ask This
This is the overarching pattern across every question category. ISO 27001 and SOC 2 prove controls existed at a point in time, during the audit window. Questionnaires answer a different question: Are those controls still operating today? Enterprise buyers have learned that a suppliers security can deteriorate significantly between audit cycles. Staff leave, configurations drift, tools expire, and processes followed during audit preparation are quietly abandoned once the certificate is issued. Questionnaires force suppliers to demonstrate continuous execution, not periodic compliance.

What This Reveals About Procurement Risk
This is the most important finding in our analysis. It explains why certifications do not stop questionnaires, they start them. Certifications establish a baseline. Questionnaires verify the baseline is maintained. The shift from "do you have this?" to "prove this is still running" represents the maturation of enterprise third-party risk management.

What Buyers Expect
- Evidence of recurring execution - Dated logs, completed tickets, periodic reports, scheduled reviews
- Clear ownership and accountability with named individuals and escalation paths
- Metrics showing control effectiveness over time: vulnerability counts, phishing rates, patch compliance
- Management visibility - Dashboards, periodic leadership reports, management review minutes

Evidence Requirements
Review schedules with execution evidence, recurring reports with historical comparisons, dashboards showing metrics over time, and management review minutes documenting oversight.

Red Flags
- "We did this once for ISO" - Controls implemented for certification but not maintained continuously
- No evidence of ongoing execution: policies exist but no logs, tickets, or reports prove they are followed
- Controls not monitored or measured - No way to determine whether a control is operating or inactive

Readiness Self Assessment

Use the table below to assess your current readiness across each of the 12 question categories. For each area, mark yourself as Green (evidence ready and current), Amber (partially addressed or out of date), or Red (not in place). Any category marked Amber or Red represents a potential delay or objection during enterprise procurement.

Category	Green	Amber	Red	Your Rating
01. Governance & ISMS	ISMS documented, certified, reviewed annually	Policies exist but reviews overdue	No ISMS, no named owner	
02. Access Control & IAM	MFA enforced, access reviews quarterly	MFA available but not enforced everywhere	No MFA, no access review process	
03. Incident Response	Plan tested within 12 months, monitoring active	Plan exists but untested	No documented plan or monitoring	
04. Business Continuity	RTO/RPO defined, restores tested quarterly	Backups exist but no restore testing	No backup strategy or recovery plan	
05. Vulnerability Mgmt	Weekly scans, patching SLAs, annual pen test	Scans run but no remediation SLAs	No scanning, no pen testing	
06. Cloud Security	Encryption, logging, CIS baselines enforced	Partial encryption, logging gaps	No documented cloud security controls	
07. Data Protection	DPA in place, classification, key management	DPA exists but not current	No DPA, no data classification	
08. Supply Chain Risk	Vendor assessments, contract clauses	Vendor list exists but not reviewed	No vendor risk process	
09. Physical Security	Badge access, visitor logs, cameras	Some controls but gaps exist	No physical access controls	
10. HR Security	Background checks, training, phishing sims	Training available but optional	No checks, no training	
11. Logging & Audit	Centralised, immutable, retained 1yr+	Logging exists but not centralised	No logging strategy	
12. Continuous Ops	Recurring evidence, drift detection, dashboards	Some recurring processes documented	Point-in-time only	

If you scored Amber or Red in three or more categories, your next regulated or enterprise customer questionnaire is at risk. The Securilix TrustOps pilot includes a full RAG Gap Report — See the final page for details.

About Securilix

Securilix is a UK-based cybersecurity, risk, and compliance consultancy. We have answered more than 150 enterprise security questionnaires for clients selling into banks, insurers, government bodies, and large corporates. TrustOps combines AI-assisted drafting with senior consultant review — every answer is fast, accurate, and defensible. We are not an AI-only tool. Every response is verified by security practitioners who understand both the technical controls and the commercial stakes.

The Real Cost of Slow, Weak Questionnaire Responses

Security & due diligence questionnaires are not going away. If anything, they are getting longer, more detailed, and more technically demanding. The days of a procurement team accepting a certificate and moving on are behind us. Every enterprise buyer now issues bespoke questionnaires that demand specific evidence of specific controls. ISO 27001 and SOC 2 get your foot in the door, solid questionnaire responses close the deal.

The cost of slow, reactive questionnaire responses is significant and often invisible. When your CTO, VP Engineering, IT Leader, or Sales Ops team spends 10 to 20 hours per questionnaire, that is time not spent building your product or service, closing other customers, or managing the team. Multiply that across four or five enterprise deals per quarter and you are looking at a full-time headcount consumed by questionnaire responses. Meanwhile, every day a questionnaire sits unfinished is a day the buyer's confidence erodes. Procurement teams track response times. Slow responses signal operational immaturity, and that perception is difficult to reverse.

Securilix analysed 154 enterprise security questionnaires to understand exactly what buyers ask and why they ask it. The 12 question categories in this report are the definitive patterns that emerge when you study enterprise procurement at scale. We built TrustOps on this foundation: A managed service that takes questionnaires off your team's desk and returns complete, evidence-ready answers within 24 hours. Every response is verified by security professionals who have seen the same questions hundreds of times and know exactly what buyers need to see.