

Sample security questionnaire

Prepared by Polaris Cybersecurity | polariscybersec.com/security-questionnaires

What this is

A completed security questionnaire for Tallyfern Inc., a fictional 14-person B2B SaaS company with no SOC 2 report. It shows the kind of answers, gap responses and answer library a Polaris client receives.

Tallyfern is not a real company. Every answer, date and figure in this file is invented for illustration. Subprocessor names are real services used only as examples.

The questions were written by Polaris to cover topics buyers commonly ask about. This is not an official CSA CAIQ, SIG or other standard questionnaire.

How to read it

Questionnaire tab (rows with an open gap are shaded yellow): each question with an answer (Yes, No, Partial or N/A), the full response, the evidence available on request, and for every gap, what covers it today and the target date.

Answer library tab: the approved answers, their owners and review dates, so the next questionnaire can be answered by copying from here.

Summary tab: answer counts and the list of open gaps with target dates.

Why the gaps are left in

Buyers check answers. An honest Partial or No with a compensating control and a date is more credible than a Yes the company can't back up, and it keeps the answers safe to put in a contract.

General information only, not legal advice. Each client reviews and approves every answer before it goes to a buyer.

#	Domain	Question	Answer	Response	Evidence available on request	Gap: what covers it today and target date
1.1	Company and compliance	Describe your company and the service in scope for this review.	N/A	Tallyfern Inc. is a 14-person company based in Toronto, Canada. The service in scope is the Tallyfern web application, which routes supplier invoices to the right approvers and records each approval.		
1.2	Company and compliance	Do you hold a current SOC 2 report or ISO/IEC 27001 certificate?	No	Tallyfern does not hold a SOC 2 report or ISO/IEC 27001 certificate today. This questionnaire, our written policies and the evidence listed in each answer describe the controls in place now.	Policy set, answer library	Tallyfern plans to start SOC 2 Type 1 readiness work in Q2 2027 and will share the report when it is issued.
1.3	Company and compliance	Do you have documented information security policies approved by management?	Yes	Yes. Tallyfern maintains written policies for acceptable use, passwords and MFA, remote work and personal devices, and incident reporting. The CEO approved them in October 2026, and they are reviewed every year.	Policy documents with approval dates	
1.4	Company and compliance	Is a named person responsible for information security?	Yes	The CTO owns information security and reports on it to the CEO each month. There is no dedicated security team; security tasks are assigned to named owners in the answer library.	Org chart, answer library owners	
1.5	Company and compliance	Do you perform a formal information security risk assessment at least annually?	Partial	Tallyfern tracks known security risks in a risk register reviewed by the CTO and CEO. A full, documented risk assessment has not yet been completed.	Risk register	The first documented annual risk assessment will be completed by December 31, 2026.
2.1	People	Do all employees and contractors complete security awareness training?	Partial	All new staff complete security onboarding in their first week, covering phishing, passwords, MFA and incident reporting. Completion is recorded.	Onboarding completion records	Annual refresher training with phishing simulations starts in January 2027.
2.2	People	Do you perform background checks on employees with access to customer data?	No	Tallyfern does not currently run background checks. Production access is limited to 3 engineers, granted by role and reviewed every quarter.	Access review records	Tallyfern is evaluating background checks for new hires with production access, with a decision by June 30, 2027.
2.3	People	Do employees and contractors sign confidentiality agreements?	Yes	Yes. Every employee and contractor signs a confidentiality agreement before receiving system access.	Signed agreements on file	
2.4	People	Is access removed promptly when someone leaves the company?	Yes	Yes. An offboarding checklist disables the person's Google Workspace account on their last day, which ends single sign-on to company tools. Production and AWS access are removed the same day.	Offboarding checklist records	
3.1	Access control	Is multi-factor authentication required for all workforce accounts?	Yes	Yes. MFA is enforced in Google Workspace for every account, and company tools use Google single sign-on. AWS, GitHub and Stripe also require MFA.	MFA enforcement settings screenshots	
3.2	Access control	Does each person have a unique account, with no shared logins?	Yes	Yes. Each person has a named account. The AWS root account is locked away, protected by a hardware security key, and used only for emergencies.	Account list	
3.3	Access control	Is access granted on a least-privilege basis and reviewed regularly?	Yes	Yes. Access is granted by role. The CTO reviews access to production, AWS and GitHub every quarter and removes anything no longer needed.	Quarterly access review records	
3.4	Access control	Is administrative access to production systems restricted and logged?	Yes	Production access uses individual AWS IAM Identity Center accounts with MFA and short-lived credentials. Only 3 engineers hold production access, and changes are logged in AWS CloudTrail.	IAM configuration, CloudTrail logs	
3.5	Access control	Do customers have options to secure their own user accounts?	Yes	Yes. Customer admins can require MFA for their users, sign in with Google or Microsoft accounts, and assign roles that limit what each user can see and approve.	Product documentation	
4.1	Data protection	What customer data do you store?	N/A	Tallyfern stores invoice files and invoice details, approval history, and user names, email addresses and roles. Tallyfern does not store payment card numbers or bank login credentials.	Data inventory	
4.2	Data protection	Is customer data encrypted at rest?	Yes	Yes. The database and file storage are encrypted at rest with AES-256 using AWS Key Management Service.	AWS encryption settings screenshots	
4.3	Data protection	Is customer data encrypted in transit?	Yes	Yes. All connections to the application use TLS 1.2 or higher. Unencrypted HTTP requests are redirected to HTTPS.	TLS configuration scan	
4.4	Data protection	Where is customer data stored and processed?	N/A	Customer data is stored and processed in the AWS Canada (Central) region. Some subprocessors handle limited data outside Canada, as listed on the subprocessor list.	Subprocessor list	
4.5	Data protection	Is customer data logically separated from other customers' data?	Yes	Yes. Every record is tagged with the customer's account ID, and the application checks that ID on every request. Automated tests check that one customer cannot read another customer's data.	Test suite results	
4.6	Data protection	What happens to customer data when a contract ends?	Yes	Customers can export their data at any time. After a contract ends, Tallyfern deletes customer data within 30 days, and it ages out of backups within a further 35 days.	Data deletion procedure	
4.7	Data protection	Is production customer data ever used in development or test environments?	No	No. Development and testing use generated sample data. Production data stays in production.	Environment configuration	
5.1	Infrastructure	Where is your service hosted?	N/A	The service runs on Amazon Web Services in the Canada (Central) region, using managed containers and a managed PostgreSQL database. Tallyfern does not operate its own data centres.	Architecture diagram	

5.2	Infrastructure	Are production systems protected from direct internet access?	Yes	Production systems run in private subnets with no direct internet access. Only the load balancer is public, and security groups allow only the traffic each service needs.	Network diagram, security group configuration	
5.3	Infrastructure	Are employee laptops centrally managed and encrypted?	Partial	Company laptops require full-disk encryption, a screen lock and automatic updates, and Google endpoint management checks these settings before allowing access.	Endpoint management report	Full mobile device management with remote wipe will be in place by March 31, 2027.
5.4	Infrastructure	Do you use anti-malware or endpoint protection on company devices?	Yes	Yes. Built-in operating system protection is enabled and kept up to date on all company laptops, and the endpoint management report confirms it.	Endpoint management report	
6.1	Application security	Do you follow a secure development process?	Yes	Yes. Every code change requires a pull request and review by a second engineer before it can be merged. Automated tests and dependency checks run on every change.	GitHub branch protection settings	
6.2	Application security	Do you scan code and dependencies for vulnerabilities?	Yes	Yes. GitHub dependency alerts and code scanning run on every change. Critical findings block the merge until they are fixed.	Scan results	
6.3	Application security	Has the application had an independent penetration test in the last 12 months?	No	Not yet. Tallyfern runs automated scanning of the application and its dependencies, but no independent penetration test has been completed.	Automated scan results	An independent penetration test is booked for Q1 2027. A summary letter will be available to customers afterward.
6.4	Application security	Do you have defined timeframes for fixing security vulnerabilities?	Yes	Target fix times are 7 days for critical, 30 days for high and 90 days for medium vulnerabilities. Progress is tracked in the engineering issue tracker.	Vulnerability tracking records	
7.1	Logging and monitoring	Are security events logged and retained?	Yes	Yes. Application, infrastructure and AWS account activity logs are collected in Amazon CloudWatch and AWS CloudTrail and kept for 1 year.	Log retention settings	
7.2	Logging and monitoring	Are security logs monitored, with alerts for suspicious activity?	Partial	Alerts for suspicious activity, such as root account use and unusual login attempts, are sent to the engineering on-call channel. Amazon GuardDuty is enabled. There is no 24/7 security operations centre.	Alert configuration	Tallyfern will review alert coverage against its incident response plan by December 31, 2026.
8.1	Incident response	Do you have a documented incident response plan?	Yes	Yes. The plan names an incident lead, sets out steps for containment, investigation and recovery, and includes contact lists.	Incident response plan	
8.2	Incident response	Has the incident response plan been tested?	Partial	The team walked through the plan once in September 2026 using a lost-laptop scenario.	Exercise notes	A ransomware tabletop exercise is scheduled for February 2027, then once a year after that.
8.3	Incident response	Will you notify customers promptly of a security breach affecting their data?	Yes	Tallyfern will notify affected customers without undue delay after confirming a breach affecting their data, and within any time limit set in the customer's contract. Notices go to the customer's named security contact by email.	Incident response plan	
8.4	Incident response	Have you had a security breach in the last 24 months?	No	No. Tallyfern has had no security breaches affecting customer data.		
9.1	Business continuity	Is customer data backed up regularly?	Yes	The database is backed up automatically, with point-in-time recovery for the last 35 days. Daily copies are also kept in a separate AWS account that production staff cannot delete.	Backup configuration	
9.2	Business continuity	Are restores from backup tested?	Yes	Yes. A full database restore was tested in September 2026 and completed in 47 minutes. Restore tests run every 6 months.	Restore test record	
9.3	Business continuity	Do you have a documented business continuity and disaster recovery plan?	Partial	Recovery steps for the database and application are documented in the engineering runbook. A complete continuity plan covering people, suppliers and communication has not yet been written.	Engineering runbook	A full business continuity and disaster recovery plan will be approved by November 30, 2026.
10.1	Vendors and subprocessors	Do you maintain a list of subprocessors with access to customer data?	Yes	Yes. The current list is AWS (hosting), Stripe (billing), Postmark (transactional email) and Sentry (error monitoring). Customers receive 30 days' notice before a new subprocessor is added.	Subprocessor list	
10.2	Vendors and subprocessors	Do you assess the security of vendors before using them?	Partial	Tallyfern reviews each subprocessor's published security documentation and certifications before signing up. The review is not yet recorded in a standard format.	Subprocessor list	A written vendor review checklist will be in use by December 31, 2026.
11.1	Privacy	Do you have a privacy policy and a named person responsible for privacy?	Yes	Yes. Tallyfern publishes a privacy policy, and the CEO is the named privacy officer.	Public privacy policy	
11.2	Privacy	Will you sign a data processing agreement?	Yes	Yes. Tallyfern offers a standard data processing agreement and will review a customer's own agreement on request.	Standard data processing agreement	

Rows shaded yellow have an open gap, with what covers it today and a target date.

Library ID	Topic	Approved answer	Used for questions	Evidence	Owner	Last reviewed	Next review
A-01	Company overview	Tallyfern Inc. is a 14-person company in Toronto, Canada. Its web application routes supplier invoices to approvers and records each approval.	1.1		CEO	2026-10-10	2027-04-10
A-02	Certifications	No SOC 2 or ISO/IEC 27001 today. SOC 2 Type 1 readiness starts Q2 2027.	1.2	Policy set	CEO	2026-10-10	2027-04-10
A-03	Policies	Written policies for acceptable use, passwords and MFA, remote work and personal devices, and incident reporting. Approved October 2026, reviewed yearly.	1.3	Policy documents	CTO	2026-10-10	2027-04-10
A-04	Security ownership	The CTO owns information security and reports monthly to the CEO.	1.4	Org chart	CEO	2026-10-10	2027-04-10
A-05	Risk management	Risk register reviewed by CTO and CEO. First documented annual risk assessment due December 31, 2026.	1.5	Risk register	CTO	2026-10-10	2027-04-10
A-06	Training	Security onboarding in week 1 for all staff. Annual refresher and phishing simulations start January 2027.	2.1	Completion records	CEO	2026-10-10	2027-04-10
A-07	Background checks	Not performed today. Production access limited to 3 engineers and reviewed quarterly. Decision on checks by June 30, 2027.	2.2	Access reviews	CEO	2026-10-10	2027-04-10
A-08	Offboarding	Google Workspace disabled on the last day, ending SSO. AWS and production access removed the same day.	2.4	Offboarding records	CTO	2026-10-10	2027-04-10
A-09	MFA	MFA enforced on Google Workspace, AWS, GitHub and Stripe. Company tools use Google SSO.	3.1	MFA settings	CTO	2026-10-10	2027-04-10
A-10	Access reviews	Role-based access. Quarterly review of production, AWS and GitHub access by the CTO.	3.2, 3.3, 3.4	Review records	CTO	2026-10-10	2027-04-10
A-11	Encryption	AES-256 at rest with AWS KMS. TLS 1.2 or higher in transit.	4.2, 4.3	Encryption settings, TLS scan	CTO	2026-10-10	2027-04-10
A-12	Data location	Stored and processed in AWS Canada (Central). Subprocessor list shows data handled elsewhere.	4.4, 5.1	Subprocessor list	CTO	2026-10-10	2027-04-10
A-13	Data deletion	Deleted within 30 days of contract end; ages out of backups within a further 35 days.	4.6	Deletion procedure	CTO	2026-10-10	2027-04-10
A-14	Secure development	Peer-reviewed pull requests, automated tests, dependency and code scanning on every change. Critical findings block merges.	6.1, 6.2	GitHub settings	CTO	2026-10-10	2027-04-10
A-15	Penetration testing	No independent test yet. Booked for Q1 2027, summary letter to follow.	6.3	Scan results	CTO	2026-10-10	2027-04-10
A-16	Logging	CloudWatch and CloudTrail logs kept 1 year. GuardDuty enabled. Alerts to engineering on-call. No 24/7 SOC.	7.1, 7.2	Log settings	CTO	2026-10-10	2027-04-10
A-17	Incident response	Documented plan with named lead. Walkthrough September 2026; ransomware tabletop February 2027.	8.1, 8.2, 8.3	Incident response plan	CTO	2026-10-10	2027-04-10
A-18	Backups	Automated backups with 35-day point-in-time recovery, plus daily copies in a separate AWS account. Restore tested September 2026 (47 minutes).	9.1, 9.2	Backup settings, restore record	CTO	2026-10-10	2027-04-10
A-19	Subprocessors	AWS, Stripe, Postmark, Sentry. 30 days' notice before adding a new one.	10.1	Subprocessor list	CEO	2026-10-10	2027-04-10
A-20	Privacy	Published privacy policy, CEO is privacy officer, standard DPA available.	11.1, 11.2	Privacy policy, DPA	CEO	2026-10-10	2027-04-10

Next review is set 6 months after the last review. Update Last reviewed whenever an answer is checked.

Answer summary

Answer	Count	Share
Yes	26	62%
Partial	7	17%
No	5	12%
N/A	4	10%
Total questions	42	100%

Open gaps and target dates

Question	Answer	Gap: what covers it today and target date
1.2 Do you hold a current SOC 2 report or ISO/IEC 27001 certificate?	No	Tallyfern plans to start SOC 2 Type 1 readiness work in Q2 2027 and will share the report when it is issued.
1.5 Do you perform a formal information security risk assessment at least annually?	Partial	The first documented annual risk assessment will be completed by December 31, 2026.
2.1 Do all employees and contractors complete security awareness training?	Partial	Annual refresher training with phishing simulations starts in January 2027.
2.2 Do you perform background checks on employees with access to customer data?	No	Tallyfern is evaluating background checks for new hires with production access, with a decision by June 30, 2027.
5.3 Are employee laptops centrally managed and encrypted?	Partial	Full mobile device management with remote wipe will be in place by March 31, 2027.
6.3 Has the application had an independent penetration test in the last 12 months?	No	An independent penetration test is booked for Q1 2027. A summary letter will be available to customers afterward.
7.2 Are security logs monitored, with alerts for suspicious activity?	Partial	Tallyfern will review alert coverage against its incident response plan by December 31, 2026.
8.2 Has the incident response plan been tested?	Partial	A ransomware tabletop exercise is scheduled for February 2027, then once a year after that.
9.3 Do you have a documented business continuity and disaster recovery plan?	Partial	A full business continuity and disaster recovery plan will be approved by November 30, 2026.
10.2 Do you assess the security of vendors before using them?	Partial	A written vendor review checklist will be in use by December 31, 2026.