

The week after your SOC 2 report lands

Seven templates to answer enterprise buyers before they ask

Your SOC 2 report gets you into a buyer's security review. These templates answer the six questions reviewers usually ask next, so you can send them with the report.

	Template	Answers the buyer's question
1	Cover note to the buyer	What's in this packet?
2	Pentest scope summary	Can we see your pentest report and its scope?
3	SOC 2 scope statement	What's outside the report?
4	Agent access register	What can your agents reach?
5	Model and subprocessor disclosure	Which models touch our data, and where do they run?
6	Named owners and security contact	Who's the human?
7	Bridge letter and change log	Is it still true today?

How to use this kit

- Fill in the bracketed fields. Gray text in brackets is guidance; delete it when you're done.
- Each template has an example for Northwind AI, a made-up company that sells Northwind Assist, an AI assistant that drafts support replies for business software companies.
- Date every page, name every owner, and say plainly what's out of scope. A buyer who sees the edges believes the middle.
- Share the packet under your NDA or on your trust center, and link it from the cover note.

These templates are general guidance, not legal advice. Adapt them to your contracts, your auditor's guidance and what is actually true at your company. Free to use and adapt.

Cover note to the buyer

HOW TO USE THIS TEMPLATE

Send this with the SOC 2 report. It tells the reviewer what's coming, names the person who owns the answers, and saves you the first round of follow-up emails.

Only list the documents you're actually attaching. If one isn't ready, give the date it will be.

Subject: [Company] SOC 2 Type 2 report and security packet

Hi [first name],

Attached is our SOC 2 Type 2 report from [audit firm], covering [period start] to [period end]. To save your team time, I've included the documents reviewers usually ask for next:

- Penetration test letter and scope summary ([testing firm], [test dates])
- SOC 2 scope statement: what the report covers, the vendors we rely on and what sits outside it
- Agent access register: each AI agent and integration, its owner and what it can reach
- Model and subprocessor disclosure, including our change-notice promise
- Named owners and how to reach our security team
- Bridge letter covering [period end] to [today] [only if your period ended more than about three months ago]

Everything is shared under our NDA. If anything is missing, reply here or call me at [phone]. I own these answers, and I'm glad to join a call with your security team.

[Name]

[Title], [Company] · [email]

Example

Northwind AI, sent October 12, 2026:

Hi Dana, attached is our SOC 2 Type 2 report from Example CPA Firm LLP, covering April 1 to September 30, 2026. I've included our pentest letter and scope summary (Example Security LLC, August 3 to 14), our scope statement, agent access register, model and subprocessor disclosure, and our named owners. Everything is under our NDA. I own these answers; call me any time at the number below. Priya Shah, Head of Security, Northwind AI.

Pentest scope summary

HOW TO USE THIS TEMPLATE

Send this one-page summary with your testing firm's attestation letter. Offer the full report under NDA only if a buyer needs it.

The out-of-scope row is the one reviewers read hardest. If something wasn't tested, say why and when it will be.

Field	What to write	Example: Northwind AI
Testing firm	[Firm name, accreditation such as CREST]	Example Security LLC, CREST accredited
Testers	[Number of testers, names or certifications]	Two named testers, certifications listed in the letter
Dates and effort	[Start and end dates, tester-days]	August 3 to 14, 2026, 16 tester-days
Environment	[Production or staging; if staging, how it differs]	Production, with a dedicated test tenant
In scope	[Each web app, API, mobile app, cloud account]	Web app, public API, admin console, AWS configuration
AI features	[Prompts, agents, tools, MCP servers tested, or a dated plan]	Assistant prompts, three agent tools, one MCP server
Out of scope, and why	[What wasn't tested, why, and when it will be]	Mobile app, test scheduled November 2026; marketing site, holds no customer data
Method	[Standards followed]	OWASP ASVS 5.0; OWASP top tens for LLM and agentic applications
Findings	[Count by severity]	0 critical, 1 high, 3 medium, 5 low
Retest	[Status of every critical and high finding]	High finding fixed and retested August 28, 2026
Next test	[Date or trigger]	August 2027, or before any major release
Full report	[Who to ask, and on what terms]	Available under NDA from security@northwind.example

SOC 2 scope statement

HOW TO USE THIS TEMPLATE

One page: what your report covers, the vendors you rely on (name your AI model providers), what sits outside it, and what you need from the customer.

1. What the report covers

Item	Your answer
Report type and period	[SOC 2 Type 2, period start to period end]
Audit firm and opinion date	[CPA firm name, date of the opinion]
Trust services criteria	[Security, plus Availability or Confidentiality if included]
Products in scope	[Product names exactly as your buyer knows them]
Environments and regions	[Production accounts, regions]
Teams and processes	[Engineering, support, people operations, incident response]

2. Vendors we rely on

Vendor	What it does for us	Touches customer data?	Their report
[Cloud provider]	[Hosting, storage]	[Yes/No]	[Their SOC 2, where to get it]
[AI model provider]	[Which feature uses it]	[Yes/No]	[Their report or terms]
Example: Anthropic, through Amazon Bedrock	Drafts support replies	Yes	AWS and Anthropic reports

3. What's outside the report, and why

Outside the report	Why	Other evidence
[Marketing site]	[No customer data]	[Pentest, separate hosting]
[Internal tools]	[No customer data, or limited access]	[Access reviews, SSO]
[Test and staging environments]	[Synthetic data only]	[Separate accounts, no production keys]
[Laptops]	[Covered by device management]	[MDM enrollment, disk encryption]

4. What we need from you

Your complementary user entity controls, in plain words:

- [Turn on single sign-on for your users.]
- [Remove departed employees from your account promptly, and keep your API keys out of code.]

Agent access register

HOW TO USE THIS TEMPLATE

One row per AI agent or AI integration that can reach company or customer data. Every row needs a named owner.

The best answer in the identity column is the agent's own credential. A borrowed user credential or a shared account is the first thing to fix.

The same columns are in week-after-agent-access-register.csv, ready for a spreadsheet.

Agent	Job	Owner	Identity	Can read	Can write	Model	Logs	Revoke	Last tested
[Name]	[What it does]	[Person]	[Own / borrowed / shared]	[Systems, data]	[Systems, data]	[Model, provider]	[Where, how long]	[Who, how, how fast]	[Date, what]
Example: Reply drafter	Drafts support replies for agents to review	Priya Shah	Own service identity	Ticket, help center	Draft reply only	Anthropic via Amazon Bedrock	Audit log, 1 year	Support lead disables it in the admin console, under 5 minutes	Prompt injection tests, Sept 2026
Example: Ticket triage	Labels and routes new tickets	Marcus Lee	Own service identity	Ticket text	Ticket labels	Self-hosted open-weight model	Audit log, 1 year	Revoke token in identity provider, under 5 minutes	Sept 2026
Example: Coding agent	Opens pull requests	Ana Ortiz	Own GitHub app, repo-scoped	Source code	Branches and pull requests, no production	Anthropic API	GitHub audit log	Uninstall the app, under 5 minutes	Aug 2026

Model and subprocessor disclosure

HOW TO USE THIS TEMPLATE

One row per model that touches customer data. Say who made it, who hosts it, where, what data reaches it and what the host keeps. If a router or gateway can switch hosts, pin your approved providers and regions, and say so. Add your change-notice promise at the bottom. The same columns are in week-after-model-disclosure.csv.

Model	Maker	Host and region	Routing	Customer data that reaches it	Retention	Training on customer data	Fallback
[Model name and version]	[Who built it]	[Who runs it, where]	[Direct / gateway, pinned?]	[Content, metadata, none]	[How long, by contract or setting]	[No, by contract / by setting]	[Approved alternative]
Example: Claude model for reply drafts	Anthropic	Amazon Bedrock, US East	Direct	Ticket text and help center articles	Not stored by the provider for this use	No, by contract	Second approved model on Bedrock
Example: open-weight triage model	Open-weight, documented model card	Self-hosted in our AWS account, US East	Direct	Ticket text	Our logs only, 1 year	No	Rules-based routing

Our change-notice promise

[We give customers at least [30] days' notice before adding or replacing a subprocessor or model provider that processes customer data, by email to subscribers and on our trust center. We may remove a provider at any time.]

Subscribe at: [link]

Named owners and security contact

HOW TO USE THIS TEMPLATE

Every answer in your packet should have a person's name next to it. A fractional or advisory title is fine; an empty row isn't.

Publish a security.txt file so researchers can reach you. The Contact field is required by RFC 9116.

Role	Name	How to reach	Response time
Security owner	[Name, title; fractional is fine]	[Email, phone]	[Business hours]
Incident contact	[Name or rotation]	[security@ address, phone]	[Acknowledge within X hours]
Agent sponsors	[One name per agent, from template 4]	[Email]	[Business hours]
Questionnaire answers	[Who approves them]	[Email]	[Business days]
Bridge letters	[Officer who signs]	[Email]	[On request]

security.txt

Publish at [https://\[your domain\]/.well-known/security.txt](https://[your domain]/.well-known/security.txt)

Contact: [mailto:security@\[your domain\]](mailto:security@[your domain])

Expires: [a date within the next year]

Policy: [https://\[your domain\]/security/disclosure](https://[your domain]/security/disclosure)

Preferred-Languages: en

Hiring and identity

[One sentence on how you verify identity before granting production access, for example: We verify identity with a live video check against a government ID and a reference call before granting production access.]

Bridge letter and change log

HOW TO USE THIS TEMPLATE

Send a bridge letter when your report's period ended more than about three months ago. Management signs it, not your auditor, so keep it short and accurate.

Attach a dated change log. It turns "is it still true?" into a two-minute read.

[Company letterhead]

[Date]

To [customer name]:

This letter covers the period from [day after your report period ended] through [today's date].

Our most recent SOC 2 Type 2 report, issued by [audit firm] on [opinion date], covered [period start] to [period end] for [system name] under the [trust services criteria] criteria.

Management confirms that, to the best of our knowledge:

- There have been no material changes to the system or its controls described in that report, other than those listed in the attached change log.
- No security incidents affected the system during this period. [Or: describe any that did.]
- Our next SOC 2 Type 2 report, covering [next period], is expected by [date].

This letter is provided by management and has not been examined by our auditor.

[Name], [Title]

[Signature]

Change log since our last report

Date	Change	What it affects	Where it's documented
[Date]	[What changed]	[System, vendor, control]	[Document or link]
Example: Aug 4, 2026	Added a second approved model for reply drafts	AI subprocessors	Model disclosure, row 2
Example: Sept 2, 2026	Moved application logs to a new vendor	Logging, subprocessors	Subprocessor list

A last check

1. Every page is dated, and every row has an owner's name.
2. Product names match what your buyer calls them.
3. Your AI model providers are named, in the scope statement and the model disclosure.
4. Out-of-scope items say why, and when they'll be covered.
5. If your period ended more than about three months ago, the bridge letter is signed.
6. The cover note ends with a person who can be reached.

Want a second pair of eyes?

We'll read your packet the way your buyer's reviewer will and tell you what we'd add or cut. Book a free 15-minute security strategy call:

cal.com/ysecurity/15min

The full guide, with the seven-day plan and the evidence behind every template:

ysecurity.io/blog/week-after-your-soc-2-report

YSecurity is the on-demand cybersecurity team. This kit is general guidance, not legal advice. Northwind AI and every name in the examples are made up.