contact@namiq.io · namiq.io

NamiQ

NAMIQ GUIDE

Surviving the Security Questionnaire

Eight moves for a founder with no security team, no SOC 2 and a quarter they cannot afford to lose

What the rows are really for, which you can answer today from artefacts, the two answers that end deals, and the documents to fill in: the one-page position, the reviewer email, the answer sheet.

PREPARED BY	Hung Le, NamiQ	DATE	31 October 2026
FACTS AS OF	31 October 2026	EDITION	1.0
FOR	Founders with no security team	INSIDE	8 moves, 8 appendices, 4 figures

NamiQ © 2026 NamiQ. All rights reserved. This guide may be shared unaltered, with attribution. Free to read and share.
Web edition: namiq.io/resources/security-questionnaires

START HERE

The questionnaire on a page

The reader is not trying to work out whether you are secure. They are working out whether they can explain buying you. Most rows need an artefact, not a certificate. Eight moves, cheapest first, each ending in something they can put in a file.

Eight moves, cheapest first. The first three cost a day between them.

#	Move	Why	First step	Proof for the file	§
1	**Ask the reviewer two questions**	Which rows are mandatory at your tier and data scope, and what the exception path is	One email the day the spreadsheet arrives	The reply, in writing	7.1
2	**Generate a dated dependency and licence inventory**	The most commonly missing artefact, and one of the easiest	An hour with tooling you already have	The inventory, with the tool, the date and its output	7.1
3	**Write the process down in a page and a half**	The audit tests what you do, not what you aspire to	Describe what you actually do, including what you are not proud of	The page, dated	7.1
4	**Assemble one change's evidence end to end**	You find the gap in your own time, not theirs	Pick a change from last week: ticket, checks, results, approver	The pack for a change you did not choose	7.1
5	**List who can reach production, and remove whoever should not**	The date of the review is half of what is asked for	Write the date at the top of the list	The list with its review date	7.1
6	**Write the incident runbook and rehearse it once**	A rehearsed process beats an elegant one nobody has run	An hour, then write it up with times	The runbook and one write-up	7.1
7	**Answer honestly, with dates against every no**	A documented no with a date is something they can process	Send the one-page position with the spreadsheet	The spreadsheet and the position	7.1
8	**Start the SOC 2 clock and tell the buyer the date**	It saves the next four deals, not this one	Name the start date	The date, in writing	7.1

Where to start, for what you have today

The spreadsheet arrived today	Page 2, then Appendix B: send the two questions the same day
The deal is this quarter and you hold no SOC 2	Chapter 2, then Appendix A: the one-page dated position
You are about to answer "yes"	Chapter 5, then Appendix F: answers that lose and answers that survive
You do not know what to attach	Chapter 4.2 and Appendix D: the evidence pack index
You have ten minutes	Page 2, then Chapter 1.3: write the artefact beside the first twenty rows
Somebody is selling you a fix	Chapter 6: ask what they would attach

Edition 1.0, 31 October 2026. The only figures in this guide are published industry figures, directional rather than audited, with their sources, and one of ours with its date.

Contents

How to use this guide 4
1. The questionnaire is a proxy, and not for your security 5
2. Your deal is this quarter; the report is next year 6
3. Most of the spreadsheet does not need a certificate 7
4. A delivery record lets you answer from evidence 8
5. Two answers that end deals 9
6. What we do not hold 10
7. What to do on Monday 11

APPENDICES

Appendix A. The one-page dated position 13
Appendix B. The email to the reviewer 13
Appendix C. The answer sheet 13
Appendix D. The evidence pack index 14
Appendix E. The incident write-up 14
Appendix F. Answers that lose, and answers that survive 14
Appendix G. Glossary 15
Appendix H. Sources, and what this guide does not claim 15

How to use this guide

The contract was two weeks from signature. Then it went to their security team, and back came a spreadsheet with a hundred and eighty rows, half of which assume you employ someone whose whole job is answering them. You do not. This guide is what the rows are actually for, which of them you can answer today, and the two answers that lose the deal outright.

It is written for a founder with no security team, no SOC 2 and a quarter they cannot afford to lose. Page 2 is the whole guide on one page: the eight moves, cheapest first, each with the proof the reviewer can put in a file. The appendices are the documents themselves, ready to fill in: the one-page dated position, the email to the reviewer, an answer sheet, an evidence pack index and an incident write-up.

What the reviewer is really asking.

What the row says

"Is every change reviewed and tested before production?"

The reviewer cannot tell whether you are secure from a spreadsheet.

What the reviewer is asking

"If this vendor causes an incident, what will I be able to show that I checked?"

An answer with an artefact beats a true answer on your word alone.

How the guide is laid out

Chapter	The question it answers
1	What is the reviewer really doing, and why does it take so long
2	Your deal is this quarter and the report is next year: what do you do
3	Which rows do not need a certificate
4	How a delivery record lets you answer from evidence
5	The two answers that end deals
6	What we do not hold
7	What to do on Monday
Appendices A to H	The position page, the reviewer email, the answer sheet, the evidence pack index, the incident write-up, answers that lose and answers that survive, a glossary, the sources

What this is not

It is not a certification, not an attestation and not a substitute for one where the buyer's policy names one. It is not legal advice. The three figures in it are published industry figures, directional rather than audited. And it does not say that doing the eight moves passes a review: it says what moves the most rows, in the order that costs least.

Conventions

- "The reviewer" is the person on the buyer's side who reads your answers.
- An "artefact" is something the reviewer can attach to a file: a document, a list, a log, with a date. A statement that something is true is not an artefact.
- Nothing here quotes a price.

1. The questionnaire is a proxy, and not for your security

YOU WILL	read every row as the reviewer does: what will I be able to show that I checked?
KEY IDEA	the reader is not trying to work out whether you are secure, because nobody can from a spreadsheet. They are working out whether they can explain the decision to buy you.
PROOF IT WORKED	for each row you intend to answer, you can name the artefact you would attach.

1.1 What the reviewer is doing

The person reading your answers cannot establish whether you are secure, and they know it better than you do. What they are working out is whether they can explain the decision to buy you to their auditor, to their risk committee, and to whoever asks the question after an incident.

That changes what a good answer looks like. A reviewer can forward a document. They cannot forward your confidence. An answer that is true but rests only on your word gives them nothing to put in a file, so it scores worse than a modest answer with an artefact attached, even when the modest answer describes a weaker control.

> Read every row as: if this vendor causes an incident, what will I be able to show that I checked?

1.2 Why it takes as long as it does

Figure	Source
36% of companies lost a deal because they lacked a required certification, up from 29% the year before	SOC 2 industry survey, 2026
4 to 6 weeks for a typical vendor security assessment, once you have supplied everything asked for	Vendor assessment benchmarks, 2026
10 to 11 months: the common path to a SOC 2 Type 2 report, with Type 1 at month four and then a six-month observation window	SOC 2 timing benchmarks, 2026

Published industry figures, directional rather than audited. Treat them as the shape of the problem, not as a forecast of your deal.

Note what the first figure is measuring. It is not that insecure vendors lost deals. It is that vendors without the paperwork lost deals, and the share doing so is rising. The review is a documentation exercise wearing a security title, and the good news buried in that is that documentation is something a small team can actually produce this month.

1.3 Check it worked

Take the spreadsheet. For the first twenty rows write the artefact you would attach to the answer. Count the rows where the honest entry is "nothing". That count is the work, and Chapter 3 says which of it needs no certificate.

2. Your deal is this quarter; the report is next year

YOU WILL	do four things in order while the SOC 2 clock runs, so that this deal and the next four are both covered.
KEY IDEA	SOC 2 is not the instrument that saves this deal. It is the instrument that saves the next four. Start it, and separately go and win this one.
PROOF IT WORKED	the reviewer has your dated position in writing, and a named start date for the audit.

2.1 The gap

SOC 2 Type 2 takes roughly four months to the Type 1 report, then a six-month window during which an auditor observes that your controls actually operate, then the Type 2 report itself: ten to eleven months on the common path, for something your buyer wants before the quarter closes.

The clock: your deal against the report. Published benchmark, directional.

Today	Month 4	Months 4 to 10	Month 10 to 11
your deal is this quarter	SOC 2 Type 1 report (common path)	a six-month observation window	Type 2 report

SOC 2 saves the next four deals. This one is won with a dated position, an exception path and artefacts.

Founders respond to that gap in one of two bad ways. They stall, hoping the buyer relents, and the deal quietly ages out. Or they write something on the website with the word "compliant" in it and hope nobody asks for the report. Chapter 5 is about why the second one is worse than losing the deal.

2.2 Four things to do in the meantime, in this order

1. **Ask for the actual control list.** Much of what arrives is the reviewer's default template, not a contractual requirement. Asking which rows are mandatory for a vendor at your tier and your data scope frequently removes a third of them, and it takes one email (Appendix B).
2. **Ask what the exception path is.** Nearly every enterprise vendor programme has one, usually a conditional approval with a remediation date and a review. It exists because the programme would otherwise be unable to buy from anyone under fifty people. Nobody will offer it unprompted; asking is not a sign of weakness, it is a sign you have read their process.
3. **Send a dated position, not a promise.** One page: what is true today, what is not yet true, and the date each gap closes, signed by a named person. This is the artefact the reviewer has been trying to extract from you all along, because it is the one they can attach to the file (Appendix A).
4. **Start the clock anyway, today.** The observation window only begins when it begins. Every week you spend deciding whether to start is a week added to the end, and the next buyer will ask the same question.

2.3 Check it worked

Look at your sent mail. The two questions to the reviewer, the one-page position and a named start date for the audit should each be there, with a date. If one is missing, it is the next thing you do.

3. Most of the spreadsheet does not need a certificate

YOU WILL	sort the rows into the four things that need no report, and answer those from artefacts you can produce this month.
KEY IDEA	strip out the rows that genuinely require an external auditor and what is left is mostly four things, all within reach of a team of a dozen people.
PROOF IT WORKED	for each of the four you can attach a document with a date.

3.1 A documented process

A page and a half, not a manual. Named steps, what has to pass before a release, who is allowed to approve one, and what happens when something is rejected. Written down and actually followed beats comprehensive and aspirational, because the audit tests the second one and finds the difference in about an hour.

3.2 Evidence attached to each change

For any change the reviewer picks, you should be able to produce the ticket, the checks that ran, what each returned, and who approved the merge. If you can do that for a change they choose rather than one you choose, you have answered a large block of the spreadsheet in a single attachment.

3.3 A dependency and licence position

An inventory of everything you ship that you did not write: the versions, the licences, the known vulnerabilities, and the date the list was generated. This is the row most often missing and the cheapest one to fix: the tooling is free and the list takes an afternoon the first time.

68% of audited codebases contain open-source licence conflicts (Technical due diligence benchmarks, 2026; a published benchmark, directional rather than audited). It is a diligence figure rather than a security one, and it turns up in both reviews for the same reason: nobody generated the list.

3.4 Incident and access practice

Who can reach production, how that access is granted and removed, when the list was last reviewed, and what happens at two in the morning. One real incident written up with times (detected, contained, communicated, closed) is worth more to a reviewer than a policy nobody has ever exercised, because it proves the process survived contact with an actual event.

3.5 Check it worked

For each of the four, write the filename and the date. Appendix D is the index. Any with no filename is a gap you can close this month without a report.

4. A delivery record lets you answer from evidence

YOU WILL	answer rows by attaching what happened, not by asserting it, using a record that is a by-product of shipping.
KEY IDEA	you can assert a property, which costs a minute and buys exactly as much trust as the reviewer already had, or show it, which costs whatever it cost to have kept the record.
PROOF IT WORKED	for a change the reviewer picks, what ran, what it said and who approved it is a lookup, not an investigation.

4.1 The whole argument for keeping one

Almost every row in a security questionnaire is asking about a property of how you build software. If the record is a by-product of shipping (every item tracked, every check logged with its result, every decision written down where it was made) then it costs nothing at questionnaire time, because it already exists. If it is not, you are reconstructing six months of history under deadline while the deal ages, and the reconstruction is itself the thing an auditor will not accept.

Assert it, or show it.

Assertion

"Yes, every change is reviewed."

Costs a minute. Buys as much trust as they already had.

Artefact

The ticket, the checks that ran, each result, the approver, for a change the reviewer picks.

Costs whatever it cost to have kept the record, which is nothing at questionnaire time.

4.2 What you attach instead of an assurance

What the row asks	What you attach instead of an assurance
Do you have a documented development lifecycle?	The written process: named steps, what blocks a release, who may approve one
Is every change reviewed and tested before production?	For a change the reviewer picks at random: the ticket, the checks that ran, each result, and the approver
How do you manage vulnerabilities in third-party code?	A dated inventory of what you ship, its versions and its licences, plus the scan output from the last build
Do you have change management and segregation of duties?	Who opened the work, who approved the merge, and the record showing they were different people
Who has access to production, and how is it removed?	The current access list, the joiner and leaver steps, and the date of the last review
What is your incident process?	The runbook, and one real incident written up with times: detected, contained, communicated, closed

4.3 What "the checks that ran" can mean

Our own process puts six checks in front of every change, and the record of which passed is per change rather than per release:

Check	What it stops	When
Security and code health	Insecure code, leaked credentials and unreadable work stopped at the door.	every change
Automated tests	Every change proved against the test suite, and the bar rises as your product grows.	every change
Integration	Confirms the parts still work together, not just on their own.	on integration
Whole system	Rebuilds everything from scratch and scans the full stack for vulnerabilities.	on integration
AI output quality	What the AI produced is sampled and scored. Nothing is assumed.	before release
Real user journey	Can a real person finish the job, end to end, on the running system.	before release

You do not need six, and you certainly do not need ours. You need the answer to "what ran, what did it say, and can you show me for this particular change" to be a lookup rather than an investigation.

4.4 The awkward row stays in

A record that only produces good news is not evidence. It is marketing with timestamps, and reviewers have seen a lot of it. Ours reports that 43% of work was later redone, alongside the figures that flatter us, on the capture dated 2 August 2026. That number is embarrassing and it is the reason the rest of the board is worth reading: a reviewer who finds one uncomfortable figure in your evidence trusts the others more, not less. If you are assembling a pack this month, leave the awkward row in.

4.5 One limit, stated plainly

A delivery record does not substitute for a certification where the buyer's policy names one. If their procurement standard says the vendor holds the report, no amount of evidence changes that, and the honest move is to find out in week one rather than week six. Ask directly: is this a hard gate, or is it a control the review is trying to satisfy some other way?

4.6 Check it worked

Ask a colleague to pick any change from last week. Time how long it takes you to produce the ticket, the checks and results, and the approver. Under ten minutes is a lookup. Over an hour is an investigation, and the reviewer will notice.

5. Two answers that end deals

YOU WILL	know the two answers that cost you the buyer's ability to defend having chosen you, and the replacement for each.
KEY IDEA	these do not cost you points. A false statement made in writing during procurement cannot be fixed by a remediation plan.
PROOF IT WORKED	nothing you have sent the buyer claims a certification you do not hold, and every "yes" has an artefact behind it.

5.1 Never claim a certification you do not hold

This includes the softened versions, which are the ones founders actually reach for: describing an audit you have started as though it has concluded, saying you are "aligned with" or "compliant with" a standard you have not been assessed against, or putting a badge on a website in the belief that nobody reads the small print. Someone does. The request that follows is always the same: please send the report. And there isn't one. At that point the conversation stops being about security. Your buyer's security lead now has a vendor who made a false statement in writing during procurement, and no remediation plan fixes that.

5.2 Never answer "yes" to a control you have not implemented

Questionnaire answers are frequently pulled into the contract as representations, which means a hopeful yes is a warranty. It gets discovered in one of two places: at the audit, where a tester asks for the evidence behind the answer, or during an incident, where the answer becomes the first thing anyone reads. The second is worse than the first by a wide margin.

The replacement is not a clever form of words. It is: *no, here is what we do instead, and here is when that changes.* Reviewers accept that far more often than founders expect, because a documented no with a date is something they can process, and a yes they cannot verify is something they have to carry personally.

The one-page dated position: signed by a named person, sent with the spreadsheet.

True today	Not yet true	Not held
each control, what you do, and the artefact attached	what you do instead for now, the date it closes, and the owner	the certification you do not hold, and the date you started

5.3 A rule that prevents most of it

Whoever fills in a row must be the person who would have to produce the artefact for it. When the questionnaire is answered by whoever is closest to the commission, every ambiguous row resolves optimistically, and the optimism is discovered later by someone with more authority than you. Appendix F has the wording that loses and the wording that survives.

5.4 Check it worked

Read your last three answers to "do you hold" and "are you compliant with". For each, find the report or the assessment it rests on. Any without one is rewritten today, before anyone asks for the report.

6. What we do not hold

YOU WILL	see our own position stated plainly, and apply to us the test this guide tells you to apply to an answer.
KEY IDEA	the test is the same for a supplier as for a questionnaire answer: ask what they would attach.
PROOF IT WORKED	you know what a supplier holds, what they do not, and what they would put in your file.

6.1 Our position

We should be direct, because this guide would be worthless coming from a supplier who was vague about it.

NamiQ does not hold SOC 2. We have not been audited against it and we are not in a Type 2 observation window. Nothing on this site says otherwise, and if you ever find something that reads as though it does, it is wrong and we

want to know.

We are also not auditors, and we do not issue attestations of any kind. What we do is build software with the evidence trail attached, which happens to be most of what a vendor review asks you to produce. That is a useful thing and a narrower thing than "we get you certified", and any supplier blurring the two is worth a harder question.

6.2 Check it worked

Ask any supplier, including us, the question in 6.1: what would you attach? If the answer is a document with a date, you have something to put in the file. If it is reassurance, you have not.

7. What to do on Monday

YOU WILL	do eight things, cheapest first. The first three cost a day between them and move more rows than anything else on the list.
KEY IDEA	the part that is genuinely hard to retrofit is being able to produce the full evidence for a change somebody else picked.
TEN MINUTES	put a name and a date beside each of the eight.

7.1 The eight

1. **Email the reviewer and ask two questions.** Which rows are mandatory at our tier and data scope, and what is your exception path. Free, and it regularly removes more work than the rest of this list adds (Appendix B).
2. **Generate a dated dependency and licence inventory.** An hour with tooling you already have. It is the most commonly missing artefact and one of the easiest to produce.
3. **Write the process down in a page and a half.** Describe what you actually do, including the parts you are not proud of. Aspirational documents fail audits; accurate ones pass with findings.
4. **Pick one change from last week and assemble its evidence end to end.** Ticket, checks, results, approver. If you cannot, you have found the gap in your own time instead of theirs, which is the entire point of doing it on a Monday.
5. **List who can reach production and remove whoever should not.** Then write the date of the review at the top of the list, because the date is half of what is being asked for.
6. **Write the incident runbook and rehearse it once.** An hour. A rehearsed process with a written record beats an elegant one nobody has run (Appendix E).
7. **Answer the spreadsheet honestly, with dates against every no.** Send the one-page position alongside it rather than after it (Appendices A and C).
8. **Start the SOC 2 clock, and tell the buyer the date.** A named start date does work for you immediately, months before the report exists.

None of this needs our tooling, and most of it needs no tooling at all.

7.2 Where to start

If you would rather the full evidence for a change were a by-product of how the work ships than a project of its own, that is what our delivery process does. And if the eight steps get you through the review without speaking to us, that is a good outcome and the reason this is not behind a form. If you are stuck on a review right now, give us read access to one system and we come back with what is actually in it (dependencies, licences, where the evidence trail breaks) and what a reviewer would find first. The write-up is yours whether or not we work together.

7.3 Ten minutes

Copy the eight onto a page. Beside each write who does it and by when. A step with no name will not happen.

APPENDICES

Appendix A. The one-page dated position

The artefact the reviewer has been trying to extract from you all along. One page, signed by a named person, sent with the spreadsheet and not after it.

```
Position of <company> on <date>, for <buyer> security review

Signed by:   <name and role>

True today (each with the artefact attached)
  - <control>: <what we do>, evidence: <file, date>
  - ...

Not yet true (each with the date it closes and the owner)
  - <control>: <what we do instead for now>, closes <date>, owner <name>
  - ...

Not held
  - We do not hold <certification>. We started <audit> on <date>. The Type 1 report is expected
<date>.

Contact for questions: <name, email>
```

Date every line. A gap with a date is something the reviewer can process; a gap with no date is something they have to carry.

Appendix B. The email to the reviewer

Send it the day the spreadsheet arrives. Two questions, nothing else.

```
Subject: <buyer> security review: two questions before we start

Hello <name>,

Thank you for the questionnaire. Before we fill it in, two questions so we answer
what you need rather than the whole template:

1. Which rows are mandatory for a vendor at our tier and data scope?
2. If we cannot meet a control by the signing date, what is your exception path
   (for example a conditional approval with a remediation date)?

We will send our answers with a one-page dated position, so you have something
to put on file.

<name, role>
```

Appendix C. The answer sheet

One row per question. "Yes" only when you can attach the artefact. Whoever fills a row is the person who would produce its artefact.

Question	Answer (yes / no / partly)	Artefact attached	If no or partly: what we do instead	Date it changes	Owner

Appendix D. The evidence pack index

What to have ready, with the date each was made. If a line has no filename, it is the next thing you do.

Pack item	What it is	Filename	Date
Process	The development process in a page and a half: steps, what blocks a release, who approves, what happens on rejection		
One change, end to end	Ticket, checks that ran, each result, approver, for a change the reviewer can pick		
Dependency and licence inventory	Versions, licences, known vulnerabilities, generated by a tool, dated		
Access list	Who can reach production, how access is granted and removed, date of the last review		
Incident runbook and one write-up	The steps, and one real incident with times		
The position	The one-page dated position (Appendix A)		

Appendix E. The incident write-up

One real incident, written up with times, is worth more to a reviewer than a policy nobody has exercised. If you have had none, rehearse one and write that up, and say it was a rehearsal.

```
Incident:        a title that says what happened
Date and times:  detected <time>, contained <time>, communicated <time>, closed <time>
Detected by:     how we found out
What happened:   two or three sentences
Impact:          who and what was affected, and for how long
What we did:     the steps, in order
Told:            who we told, and when
Changed after:   what we changed so it is less likely or less damaging
```

Appendix F. Answers that lose, and answers that survive

The question	An answer that loses	An answer that survives
Are you SOC 2 compliant?	"Yes, we follow SOC 2 principles"	"No. We have not been audited. We started the audit on <date>; the Type 1 report is expected <date>. Here is our dated position."
Is every change reviewed before production?	"Yes" (and nothing attached)	"Yes. Here is a change you can pick: the ticket, the checks and results, and the approver."

Do you do penetration testing?	"Yes" (when you have not)	"Not yet. We run <scans> on every change, evidence attached. A penetration test is planned for <date>."
Do you encrypt data at rest?	"Yes" (without checking)	"Yes for <systems>, evidence attached. Not yet for <system>; it closes <date>, owner <name>."
Who can access production?	"Only the team"	"These <n> people, reviewed on <date>. Leavers are removed by <step>."
Have you had a security incident?	"No" (when you do not know)	"None recorded. Here is how we would find out, and the write-up of the rehearsal we ran on <date>."
Do you have an incident response plan?	"Yes" (and no runbook)	"Yes. The runbook is attached, and one write-up with times."
Do you hold an ISO or SOC attestation?	"We are working towards it" with no date	"No. We started on <date>."

Appendix G. Glossary

Artefact. Something the reviewer can attach to a file: a document, a list or a log, with a date.

Attestation. A statement by an independent auditor about your controls. We do not issue them.

Exception path. The route a vendor programme provides for approving a vendor that cannot meet every control by the signing date, usually with a remediation date.

Observation window. The period, in a SOC 2 Type 2 audit, during which an auditor watches your controls operate. Six months on the common path.

Representation. A statement made in a contract or a questionnaire that the other party relies on. A hopeful "yes" can be treated as one.

SOC 2. A report by an independent auditor on a company's controls. Type 1 reports the design of the controls at a point in time; Type 2 reports that they operated over a period.

Vendor security review. The buyer's assessment of a supplier before signing, often a spreadsheet of questions.

Appendix H. Sources, and what this guide does not claim

Sources.

- SOC 2 industry survey, 2026: 36% of companies lost a deal for lack of a required certification, up from 29%, at soc2auditors.org/insights/soc-2-compliance-for-startups
- Vendor assessment benchmarks, 2026: four to six weeks for a typical assessment, at getagency.com/vendor-security-review
- SOC 2 timing benchmarks, 2026: ten to eleven months to a Type 2 report, at hub.causo.ai/guides/soc2-for-seed-startups-enterprise-deals-2026
- Technical due diligence benchmarks, 2026: 68% of audited codebases contain licence conflicts, at hypernestlabs.com/guides/technical-due-diligence-checklist

What this guide does not claim.

- It is not a certification, an attestation or legal advice, and it does not replace a certification where the buyer's policy names one.
- The four figures are published industry figures, directional rather than audited, and are not a forecast of your deal.

- It does not say that doing the eight moves passes a review. It says what moves the most rows, in the order that costs least.
- NamiQ does not hold SOC 2, and nothing here says otherwise.