Five Whys worksheet

Score every answer against the four tests before you ask the next why. T = True (we can show it). E = Enough on its own (no 'and'). N = Names a person (should be No). O = Ours to change. Stop at the first answer that passes all four and names a rule, check, tool or owner you can change.

Problem statement: what, where, when, how much (no causes, no names)

Incident / ticket ID: _____ Priority: ____ Date: _____ Facilitator: _____

Chain A

Step	Answer: why did the line above happen?	Evidence	T	E	N	O
0	(the problem, or the branch you split off)					
1						
2						
3						
4						
5						
6						

Root cause A: _____

Chain B (split off from chain A, step ___)

Step	Answer: why did the line above happen?	Evidence	T	E	N	O
0						
1						
2						
3						
4						

Root cause B: _____

© Garrould Limited · CC BY-NC 4.0 · Share for non-commercial use with a link to https://www.itmanagement101.co.uk/five-whys-template/

Actions: one per root cause, at the right depth

Restore = today's fix. Contain = stops a repeat while the real fix is built. Prevent = removes the root cause. Every root cause needs a Prevent action with an owner and a date.

Action	Chain	Restore / Contain / Prevent	Owner	Due	Done

The four tests

Test	Ask	If it fails
True	Can we show it? A log, a ticket, a record or a screenshot, not a memory.	Mark it unverified and find the evidence before you ask the next why.
Enough	On its own, would this answer have caused the line above? If it needs an 'and', it is two answers.	Split it: give each part its own chain.
Not a name	Is the answer a person ('Sam forgot')? People are where the interesting part starts, not where it ends.	Reframe it: what made the slip possible, likely or invisible?
Ours	Is it a rule, a check, a tool or an owner we can change?	If not, ask why we were exposed to it. If yes and the first three pass, stop: this is a root cause.

Read it back. Start at the root cause and read up the chain with 'and so' between each line. If a step does not follow from the one below it, a link is missing or a guess has crept in.

Which tool?

Situation	Use	How
One-off P3 or P4	No analysis	A closing note in the incident log. If it happens again, it is no longer one-off.
A P3 or P4 that keeps coming back	Five Whys	One chain, 15 to 30 minutes, the person who fixed it plus one other. Split the chain wherever an answer needs an 'and'.
Any P2	Five Whys, branched	Run it in the post-incident review if the incident lasted more than four hours or repeats a recent cause.
Every P1, and any personal data or security incident	Fishbone first, then Five Whys on each confirmed cause	Inside the post-incident review. The fishbone stops you following the first plausible chain and missing the others.
Someone hurt, a regulator involved, or several organisations' systems interacting	A fuller root cause analysis	A trained investigator and a method built for many interacting causes (a causal tree or fault tree). For workplace accidents, follow the HSE's investigation guidance.

© Garrould Limited · CC BY-NC 4.0 · Share for non-commercial use with a link to https://www.itmanagement101.co.uk/five-whys-template/

Worked example: Harbour Lane IT Ltd (fictional)

Harbour Lane IT Ltd is a 22-person managed service provider (fictional). The outage, people and figures are invented to show the method; the same incident is written up on our IT incident report and fishbone diagram template pages.

Not this: "Portal down Monday. Sam forgot the certificate."

This: On Monday the client support portal was unreachable for 3 h 40 min (07:55 to 11:35) for all 41 client organisations, because browsers rejected its expired TLS certificate.

Chain A: Why was the certificate not renewed?

Step	Answer: why did the line above happen?	Evidence	T	E	N	O
0	Browsers rejected the portal from 07:55					
1	Browsers refused the connection because the portal's TLS certificate expired at 07:55	Certificate record; web server log	Y	Y	N	N
2	Nobody renewed the certificate before its expiry date	Certificate authority account: no renewal request until 09:55	Y	Y	N	N
3	The only renewal reminder was in one engineer's calendar, and he was on leave; the authority's warning emails went to a mailbox nobody read	Calendar entry; leave record; mail log	Y	N	N	N
3, split	The only renewal reminder was in one engineer's calendar, and he was on leave	Calendar entry; leave record	Y	Y	N	N
4	Certificates were not in the asset register, so nothing else flagged the date	Asset register export	Y	Y	N	N
5	The register process covered hardware and licences only, and was not extended when the portal launched	Register procedure; portal go-live record	Y	Y	N	Y

Root cause A: The asset register process did not cover certificates

Chain B: Why did nobody read the warnings?

Step	Answer: why did the line above happen?	Evidence	T	E	N	O
0	The certificate authority's warning emails went unread					
1	The warnings went to the mailbox of an engineer who had left	Certificate authority account contact; leaver record	Y	Y	N	N
2	The account was opened with that engineer's own address when the portal launched	Account history	Y	Y	N	N
3	Supplier accounts have no rule requiring a shared mailbox, and the leaver checklist does not check supplier contact addresses	Supplier procedure; leaver checklist	Y	Y	N	Y

Root cause B: No rule that supplier and certificate accounts use a shared mailbox

Chain C: Why did it take 51 minutes to declare a P1?

Step	Answer: why did the line above happen?	Evidence	T	E	N	O
0	Logged as P3 at 08:24, raised to P2 at 08:45, declared P1 at 09:15					
1	Each caller described one login failure, so three calls became three one-client tickets	Tickets 08:20 to 08:31	Y	Y	N	N
2	Each ticket was graded on its own: one client affected, so Limited impact	Ticket priority history	Y	Y	N	N
3	The grading guide asks how many users a ticket affects, not how many people are reporting the same fault	Service desk grading guide	Y	Y	N	Y

Root cause C: The grading guide counts users per ticket, not reports of the same fault

In chain A, step 3 failed the Enough test: it held two answers joined by 'and'. The calendar half stayed in chain A, rewritten as step 3 on its own line (3, split); the mailbox half became chain B.

© Garrould Limited · CC BY-NC 4.0 · Share for non-commercial use with a link to https://www.itmanagement101.co.uk/five-whys-template/

Example actions

Action	Chain	Depth	Owner	Due (days)
Install a new certificate and confirm logins from outside networks	A	Restore	Lead engineer	Done
Check the expiry date of every certificate the firm runs, this week	A	Contain	Lead engineer	3
Register every TLS certificate with owner, expiry date and renewal route	A	Prevent	Service manager	14
Move the portal certificate to automatic renewal	A	Prevent	Lead engineer	30
Shared mailbox for certificate authority and supplier notices; add a supplier-contact check to the leaver checklist	B	Prevent	Office manager	7
Grading rule: three or more clients reporting the same fault = Widespread impact	C	Prevent	Service desk lead	7

Example 2: the backup that kept failing

The nightly backup of the file server failed on three nights in two weeks (all three logged as P4).

Step	Answer: why did the line above happen?	Evidence	T	E	N	O
0	Nightly backup failed 3 times in 2 weeks					
1	The backup target disk was full	Backup job log: 'insufficient space'	Y	Y	N	N
2	Backups older than 30 days were no longer being deleted	Disk listing: copies going back 11 weeks	Y	Y	N	N
3	The clean-up job that deletes them was switched off	Scheduler: job disabled	Y	Y	N	N
4	It was switched off during the storage move and not switched back on	Change record for the storage move	Y	Y	N	N
5	The migration checklist has no step to re-enable and test scheduled jobs	Migration checklist	Y	Y	N	Y

Root cause: The migration checklist has no step to re-enable and test scheduled jobs. One chain was enough: every answer passed the Enough test, so nothing needed splitting.

Running it in the post-incident review

- Before the meeting: the facilitator drafts the problem statement and a first chain from the incident report, with the evidence for each answer.
- In the room: read the problem statement aloud; correct it before anyone offers a cause.
- Test each answer as you go. Mark guesses as unverified and give someone the job of checking them.
- Split at every 'and'. Three short chains beat one long one that skips a step.
- When an answer names a person, ask what made the slip possible. Write the answer about the system, not the person.
- Finish with one Prevent action per root cause, an owner and a date, and agree when the action list will be checked.

Instead of	Ask
Why did you forget?	What would have reminded anyone at all?
Who set up the account?	How does a supplier account get its contact address, and who checks it later?
Why was it graded P3?	What did the desk know at 08:24, and what would have shown it more?
Why didn't anyone spot it?	What did the monitoring check, and what did we assume it checked?

Full guide and the Excel version: https://www.itmanagement101.co.uk/five-whys-template/

© Garrould Limited · CC BY-NC 4.0 · Share for non-commercial use with a link to https://www.itmanagement101.co.uk/five-whys-template/