Follow-Up, and the Closure the Auditor Did Not Design

GUIDING QUESTION *Look at the last three findings your internal audit closed. For each one, ask who designed the fix, who decided it was working, and what they looked at to decide. If the same person appears in the first two answers, or the third answer is a report produced by the fix itself, the finding was closed by its author, on its author's evidence.*

Property: _____ Completed by: _____ Date: _____

How to use this sheet: work through the five parts with the people who own the process. The text in the left-hand columns comes from the book; the empty columns are for what is true in your property.

1. Verification Pact: what is commonly believed, what actually holds, and your property

What is commonly believed	What actually holds	In our property
«The auditor knows the finding best, so should check the fix.»	The auditor knows the finding. If they also designed the fix, somebody else should judge it.	
«Implemented as planned means effective.»	Implementation is what was done. Effectiveness is whether the risk went down.	
«The system report shows full compliance.»	It shows compliance among what the system knows about. The hotel may hold more.	
«Check soon after the fix, while it is fresh.»	Early checks confirm installation. Workarounds appear after weeks of normal work.	
«Closed findings are finished.»	Controls decay in a hotel. Important ones need a later look after closure.	

2. What the standard requires, and what demonstrates it

From Table 3.14.a. The third column of the book (what is method, not requirement) is left out here: write what your property actually holds as evidence.

What is required	What demonstrates it in a hotel	In our property
Objectivity and impartiality	A record of who designed each remedy and who verified it, never the same person for significant findings	
Effectiveness of corrective action reviewed	A test of whether the risk went down, not only whether the action was done	
Monitoring determined	For important controls, what will be checked after closure, how and when	
Independent review	A colleague, peer hotel or outside person verifying remedies the auditor helped design	
Endpoint devices protected	All devices holding guest information protected in practice, as observed on the floor	
Inventory of assets	A count of devices from purchasing and departments, reconciled with the management console	

3. The instrument: Table 3.14.b, The follow-up sheet

The instrument of this subchapter. One sheet for each finding whose remedy is meant to reduce a risk, completed at the follow-up and kept with the finding.

Question	Implementation check	Effectiveness check	In Bordeaux
Who verifies?	Whoever designed or installed the fix	Somebody who did not design it and has no stake in it	Designed and verified by Camille; reverified by Nadia

Question	Implementation check	Effectiveness check	In Bordeaux
Against what?	The design of the remedy	A criterion agreed before the fix, describing the outcome	Console compliance, set by the designer
On which population?	What the fix reports on	What the hotel actually holds, from independent sources	Twenty-three on the console; thirty-one in the hotel
With what evidence?	Records produced by the fix	Records plus observation of the control in use	Console only; codes on trolley labels never seen
When?	Soon after installation	After two to three months of normal working	Two weeks after rollout
What remains?	Nothing: finding closed	Residual risk stated and accepted, or further action	Eight devices unprotected; erasure untested
What next?	Nothing until the next audit	A stated later check on the control	Quarterly comparison of purchases with enrolments

The rows above are the book's; the empty rows are for lines your property needs to add.

4. Common mistakes: self-check

Common mistake	Present here? (Yes / Partly / No)	Where we see it
Letting the auditor who designed a remedy verify it.		
Checking that the remedy was implemented instead of whether the risk went down.		
Sampling from the population the fix reports on.		
Relying on the fix's own reports without observing the control in use.		
Following up too soon for workarounds to have appeared.		
Letting the designer set the criterion for closure.		
Applying full effectiveness tests to every finding until the open list is unreadable.		

5. Action plan

Step from the book / gap found	Action in our property	Owner	Deadline
Classify each finding when raised: closure on implementation or on effectiveness.			
Agree, before the fix is designed, what outcome will show the risk has been reduced.			
Record who designed each significant remedy; never let them verify it.			
Count the real population from sources independent of the fix.			
Observe the control in use, not only the reports it produces.			
Schedule effectiveness tests two to three months after implementation.			

Step from the book / gap found	Action in our property	Owner	Deadline
State, on closure, what will be checked again and when.			
Keep the full discipline for findings that matter, and close the rest simply.			

In brief

Follow-up tests whether the risk has gone down, not whether the fix was installed. The auditor classifies each finding when it is raised, agrees the criterion for closure before the remedy is designed, keeps design and verification in different hands, counts the real population from independent sources, observes the control in use, waits long enough for normal work to test it, and states what will be looked at after closure. In a small company the independence comes from a colleague at another property, not from a new department.

Source: The Helm and the Lens, Volume 5b: The Lens, subchapter 3.14. This sheet does not reproduce the text of the standard; work with your own copy of ISO/IEC 27001:2022 from an authorised source.