What the Internal Audit Owes the Management Review

GUIDING QUESTION *Find the minutes of your last three management reviews and read what they say about internal audit. If each says something like «audit programme completed, no major nonconformities, results noted», ask what top management learned from the audit that it did not know before, and what it decided because of it. If the answer is nothing, the review heard that the audit happened, not what it found.*

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
«Programme completed as planned means the audit did its job.»	It means the plan was followed. Whether the plan was adequate is a separate question.	
«No major nonconformities means the system is effective.»	It means none were found in what was audited. What was not audited is unknown.	
«Three years of audits cover the whole system.»	Only if the programme was built to cover it. Programmes drift towards what is easy.	
«Auditors report findings, not opinions.»	The review needs a judgement. The auditor is best placed to give one, labelled as such.	
«The audit programme is the auditor's business.»	Top management owns it: its scope, its resources and the gaps it accepts.	

2. What the standard requires, and what demonstrates it

From Table 3.15.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
Audit programme established	A programme approved at the review, stating scope, days and responsibilities	
Importance and previous results considered	A programme visibly weighted towards high-risk areas and recurring findings	
Audit results as review input	Coverage, trends, recurrence and an opinion presented and discussed	
Trends in nonconformities considered	Recurring findings tracked under the same identity across years	
Decisions on improvement	Minutes recording what the review decided about the audit and the system	
Resources ensured	Audit days set by the review according to need, not habit	

3. The instrument: Table 3.15.b, The audit's account to the review

The instrument of this subchapter. The structure of the internal audit's input to the management review, one or two pages, presented and discussed each year.

Section	What it answers	Brussels before	Brussels after
Activity	What the audit did this year	Programme completed; 18 findings; 15 closed	The same, in one line
Coverage	What has and has not been audited in the cycle	Not reported	Sixty-two of ninety-three controls audited; thirty-one never, listed by name
Trend and recurrence	Whether the system corrects itself	Not reported	Five findings recurring in all three years, with their history

Section	What it answers	Brussels before	Brussels after
Opinion	What can be relied on, what cannot, what is unknown	Not given	Access and awareness reliable; suppliers and continuity unknown; recurrences show weak correction
The audit's own effectiveness	Whether the audit looked in the right places	Not considered	Programme built on convenience; four days insufficient for the risks
Proposed programme	Where to look next, and what will not be covered	Last year's, repeated	Suppliers, cloud, continuity, delegate data first; seven days
Decisions requested	What top management must decide	None	Approve programme and days; owners for the five recurrences; accept remaining gaps

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
Reporting to the review what the audit did rather than what it can vouch for.		
Presenting each year's results alone, with no trend.		
Renumbering recurring findings so that recurrence cannot be seen.		
Never telling top management which parts of the system have not been audited.		
Building the programme on what fits in the days available.		
Declining to give an opinion because opinions can be wrong.		
Turning the review into a platform for the audit rather than an input to management.		

5. Action plan

Step from the book / gap found	Action in our property	Owner	Deadline
Read every programme and report since the last certification as one body of work.			
Map which clauses and controls have been audited in the cycle, and which never.			
Keep the original reference for any finding that recurs.			
Write a short, signed opinion on what can be relied on and what cannot.			
Assess whether the audit itself looked in the right places.			
Propose next year's programme from gaps, recurrences, incidents and changes.			

Step from the book / gap found	Action in our property	Owner	Deadline
Ask the review to approve the programme, the days and any accepted gaps.			
Keep the account to fifteen minutes and two pages.			

In brief

The internal audit owes the management review an account of assurance. The auditor reads the cycle as a whole, maps what has and has not been audited, tracks recurring findings under their original identity, gives a plain opinion on what can be relied on, assesses whether the audit itself looked in the right places, proposes the next programme with its gaps named, and asks top management to decide. The review, in return, owns the scope and resources of its own audit.

Source: The Helm and the Lens, Volume 5b: The Lens, subchapter 3.15. This sheet does not reproduce the text of the standard; work with your own copy of ISO/IEC 27001:2022 from an authorised source.