Auditing Information Nobody Can See

GUIDING QUESTION *Choose one piece of guest information your hotel received this week (a booking, a delegate list, a passport) and follow it on paper from the moment it arrived to every place it is held today. If your last internal audit could not have drawn that path, it audited the system's documents rather than the system.*

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
«An internal audit checks conformity to the standard.»	It checks conformity to the organisation's own requirements as well, including its policy, its rules and its Statement of Applicability.	
«A good quality auditor can audit any system.»	Only if competent in what this system protects. Auditing information requires knowing where information goes.	
«The documents show how things are done.»	Documents show how things should be done. Observation, records and people show how they are.	
«Suppliers are outside the audit because they are outside the scope.»	The hotel's controls over what it sends to suppliers are inside the scope, and they are where flows most often fail.	
«No major findings means the system works.»	It means nothing major was found in what was examined. The report should say what was not examined.	

2. What the standard requires, and what demonstrates it

From Table 3.1.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
Audits at planned intervals	A programme covering the whole system within the certification cycle, with dates	
Conformity to the organisation's own requirements	Audit criteria that include the policy, topic rules and the Statement of Applicability	
Effective implementation	Evidence from observation, records and interviews where the work is done	
Importance of processes considered	Audit time weighted towards the flows that carry guests' information	
Criteria and scope defined for each audit	A one-page plan naming the flows, the criteria and what is left out	
Objectivity and impartiality	An auditor who did not build or run what is audited	
Competent auditors	Training or pairing so that the auditor recognises how information moves in a hotel	

3. The instrument: Table 3.1.b, Following one piece of information

The instrument of this subchapter. One page per flow, filled in during the audit, with the evidence beside each step.

Step on the trail	Where it is, who touches it	What the hotel promised here	Evidence found
Received	Events office inbox; the events coordinator	Personal data received only through agreed channels, and only what is needed	The client's email with passport numbers; no one asked for less
Stored	Shared events folder; three people who need it	Access limited by role	Folder open to the whole sales team
Used	Registration at the desk; transfer planning	Identity data used only for registration	Passport numbers also used to label transfer lists
Sent	Transfer company, by public link	Sent only through approved, protected channels	Link without password or expiry, still open
Held by supplier	Transfer company's drivers' phones	Agreement requires deletion after the service	No agreement found; drivers keep lists
Deleted	Nowhere yet	Delegate lists deleted ninety days after the event	All lists since the certification still present
Reported	The audit report	Findings reported to management with what was not examined	This trail was not in the programme

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
Organising the internal audit by clause and department rather than by flow of information.		
Accepting documents and the word of their authors as evidence of practice.		
Auditing samples chosen by the people being audited.		
Assigning an auditor who does not know how information moves in a hotel.		
Leaving the hotel's own rules and Statement of Applicability out of the audit criteria.		
Stopping the audit at the boundary of the certificate instead of at the edge of the hotel's control.		
Concluding effective implementation without saying what was not examined.		

5. Action plan

Step from the book / gap found	Action in our property	Owner	Deadline
List the six to ten flows of information that matter most in this hotel, starting from the information register.			
Make each flow a unit of the audit programme within the certification cycle.			
Follow one real item forwards along each flow, and one backwards from where information ended up.			

Step from the book / gap found	Action in our property	Owner	Deadline
Use the policy, topic rules and Statement of Applicability as criteria alongside the standard.			
Collect a record, an observation and a conversation at each step.			
Draw the sample from complete lists, never from examples offered by the auditee.			
Follow flows to the edge of the hotel’s control, including the handover to suppliers.			
Add a paragraph on what was not examined to every audit report.			

In brief

An internal audit of an information security system establishes whether the hotel keeps its own promises where its information actually goes. It follows the important flows of guest information from arrival to deletion, uses the hotel’s own rules and statement of controls as criteria, collects records, observations and conversations, chooses its own sample, stops at the edge of the hotel’s control rather than at the boundary of the certificate, and says plainly what it did not examine.

Source: The Helm and the Lens, Volume 5b: The Lens, subchapter 3.1. This sheet does not reproduce the text of the standard; work with your own copy of ISO/IEC 27001:2022 from an authorised source.