Surveillance, and the Year the Hotel Changed Hands

GUIDING QUESTION *List everything that has changed in your hotel since the last certification audit: people in key roles, systems, suppliers, the operator, the owners, the scope of what the hotel does. Then find the letter or email in which you told the certification body about each. If the list is long and the letters are few, the certificate on your wall describes a hotel that may no longer exist.*

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 certificate is valid for three years whatever happens.»	It is valid while surveillance confirms the system still exists and works.	
«The certifier will find out at the next surveillance.»	The hotel must tell it without delay. Finding out at surveillance is itself a failure.	
«The management system belongs to whoever runs the hotel.»	It should belong to the owner, with the operator running it under agreement.	
«Migrating the guest data completes the handover.»	The handover also needs confirmation of what the old operator keeps, and its deletion.	
«A suspended certificate can still be shown.»	During suspension the certification is invalid and may not be claimed.	

2. What the standard requires, and what demonstrates it

From Table 4.9.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 through a change	In our property
Certifier informed of changes	A letter before the change, with the plan and a proposed audit	
Changes planned	A transition plan with an information security section and owner	
System continues to operate	Internal audit and management review held on schedule, even during transition	
Supplier exit addressed	Written confirmation from the outgoing operator of data returned and deleted	
New suppliers assessed	New systems and providers checked against the hotel's requirements before going live	
Surveillance allowed at required frequency	Audit dates agreed and kept, even in a year of change	

3. The instrument: Table 4.9.b, Change notice to the certifier

The instrument of this subchapter. Completed when a significant change is decided, and sent to the certification body with the transition plan.

What changes	Why the certifier needs to know	What must be in place first	Taipei in September
Operator	Changes management, organisation and often the system itself	Owners hold the system; transition plan includes it	Not reported; system left with the old operator
Key people	Roles and responsibilities change hands	Successors named and briefed before handover	Coordinator and most managers gone; roles unknown

What changes	Why the certifier needs to know	What must be in place first	Taipei in September
Property system and platform	Main processing of guest data changes	Assessment before go-live; migration planned	Migrated over a weekend; not assessed
IT provider	Key supplier with access to all systems	Contract with the hotel's security terms	No security terms
Policies and statement of controls	The certified basis of the system	Owned by the hotel; revised for new systems	Withdrawn by old operator; statement out of date
Data at the outgoing operator	Guest data custody after exit	Written list of copies; return and deletion confirmed	Unknown
Audit and review cycle	Surveillance checks both	Held on schedule through the change	Internal audit cancelled; no review since March

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
Changing operator, systems or key people without telling the certifier.		
Leaving the management system's documents and records in the operator's hands.		
Planning a transition without an information security section.		
Migrating guest data without asking what the old operator keeps.		
Connecting new suppliers without assessing them against the hotel's requirements.		
Cancelling the internal audit and management review during a transition.		
Freezing necessary change for fear of surveillance.		

5. Action plan

Step from the book / gap found	Action in our property	Owner	Deadline
Secure the owners' ownership of the management system in every management agreement.			
Include information security in any transition plan, with a named owner.			
Write to the certifier as soon as a significant change is decided.			
Obtain written confirmation of data returned and deleted by any outgoing operator or supplier.			
Assess new systems and suppliers before they go live.			
Hand over information security roles, and brief every new manager on the system.			
Hold the internal audit and management review on schedule through the change.			

Step from the book / gap found	Action in our property	Owner	Deadline
Change what the hotel needs to change, and report it.			

In brief

Surveillance confirms that the certified system still exists and still works. A change of operator, owners, key systems or key people is a change to that system, and the hotel plans it as one: the owners own the system whatever the operator, the transition plan includes information security, the certifier is told before the change, the outgoing operator returns and deletes data in writing, new suppliers are assessed before go-live, roles are handed over, and the audit and review cycle keeps running.

Source: The Helm and the Lens, Volume 5b: The Lens, subchapter 4.9. This sheet does not reproduce the text of the standard; work with your own copy of ISO/IEC 27001:2022 from an authorised source.