Recertification, and the System That Has to Stay Awake

GUIDING QUESTION *Lay your risk register, your statement of controls, your objectives and your management review minutes from three years ago beside today's. Count what has changed and ask why. If almost nothing has, ask whether your hotel has really stood still for three years, or whether your management system has simply stopped watching it.*

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
«Clean surveillance audits guarantee recertification.»	Recertification judges the whole cycle, including whether the system followed the hotel's changes.	
«A stable risk register shows a stable hotel.»	It may show a register nobody questions. Stability needs a reason.	
«Objectives met at one hundred per cent are a success.»	They usually measure activities that cannot fail. They should stretch the system.	
«The management review is fine if it is held.»	It must produce decisions. Three years without one is a finding.	
«Recertification can be completed after expiry.»	It must be completed before; otherwise the certificate lapses, with limited means of restoring it.	

2. What the standard requires, and what demonstrates it

From Table 4.15.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 at recertification	In our property
Performance over the whole cycle	A cycle account: what changed, why, and what it achieved	
Effectiveness in light of changes	Risks, controls and statement updated for each significant change in the cycle	
Context kept under review	Context analysis updated with industry events and new services	
Objectives measured and updated	Outcome objectives, raised when met, with trends	
Review produces decisions	Minutes recording changes decided and their results	
Continual improvement	Improvements traced from findings, incidents and reviews to results	

3. The instrument: Table 4.15.b, Signs of a system that is awake

The instrument of this subchapter. Completed three months before recertification, and presented to the certifier as part of the cycle account.

Sign	What a living system shows over the cycle	Waikiki before	Waikiki after correction
Risk register	Risks added, removed and rescored with reasons	Same forty-two risks, same scores	Mobile key, digital check-in and messaging supplier added; every risk questioned
Statement of controls	Versions following significant changes	Version 1.0 throughout	Version 2.0 with supplier, cloud and masking controls applied

Sign	What a living system shows over the cycle	Waikiki before	Waikiki after correction
Context	Industry events and new services considered	Unchanged since the start	Sector attacks and the sister property's incident included
Objectives	Outcome measures, raised when met	Four activity measures at one hundred per cent	Phishing reporting rate, access removal time, restore time, supplier evidence
Internal audit	Coverage extended; recurring findings resolved	Same checklist; same three findings	New areas audited; causes of recurrences corrected
Management review	Decisions recorded and followed	Minutes nearly identical for three years	Six decisions with owners and dates
Improvement	Changes traced to results	None evidenced	Cycle account showing what was learned and changed

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
Treating recertification as a longer surveillance audit.		
Reviewing the risk register by updating its date.		
Leaving the statement of controls unchanged while services change.		
Setting objectives that are always met.		
Copying management review minutes from year to year.		
Ignoring what has happened in the industry during the cycle.		
Manufacturing change to look alive instead of learning.		

5. Action plan

Step from the book / gap found	Action in our property	Owner	Deadline
Read the whole cycle three months before recertification, as the certifier will.			
List every change in the hotel and its industry, and check each against the system.			
Question every risk with its owner and record the reason for each score.			
Replace activity objectives with outcome objectives that stretch the hotel.			
Show audit coverage and findings, including recurrences, over the cycle.			
Hold a management review that decides, and record the decisions.			
Write a short cycle account of what was learned, changed and achieved.			

Step from the book / gap found	Action in our property	Owner	Deadline
Keep stable what deserves to be stable, and say why.			

In brief

Recertification judges the whole cycle, and a living management system shows what it learned. The hotel reads its own cycle before the certifier does, checks every change in the hotel and its world against the system, questions every risk, sets objectives that stretch it, shows its audit and findings over time, holds a review that decides, and writes a cycle account. Where things have stayed the same, it says why. Where they have changed, it shows what the change achieved.

Source: The Helm and the Lens, Volume 5b: The Lens, subchapter 4.15. This sheet does not reproduce the text of the standard; work with your own copy of ISO/IEC 27001:2022 from an authorised source.