Lenders, Insurers and the Certificate as Evidence

GUIDING QUESTION *Find the last three questionnaires your hotel answered about information security: one from a lender or investor, one from an insurer, one from a client or rating agency. Put the answers side by side. Were they given by the same person, from the same evidence, and do they say the same thing? If not, at least one of them is wrong, and it may be the one somebody will rely on when it matters most.*

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 answers the lender's questions.»	It shows a conforming management system within scope. Lenders also want the risks and the findings.	
«A certified hotel has all the usual controls.»	The standard requires justified choices, not specific controls. Only evidence shows what is in place.	
«Audit reports are confidential and cannot be shared.»	The certifier keeps them confidential. The hotel may share them, under its own terms.	
«Insurers only want to know the hotel is certified.»	They ask about specific controls, and the accuracy of the answers can decide the cover.	
«Each questionnaire is answered by whoever receives it.»	Answers must come from one account, reconciled by one person.	

2. What the standard requires, and what demonstrates it

From Table 4.12.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 to lenders and insurers	In our property
Interested parties and requirements determined	Lenders, insurers and investors listed, with their known requirements	
Contractual requirements identified	Policy conditions and loan covenants on information risk recorded and met	
Scope determined with interfaces	Scope stated honestly, with what lies outside and how it is managed	
Communication determined	One evidence pack and one person reconciling all answers	
Management review considers interested parties	Lender and insurer questions and the hotel's answers reviewed by top management	
Audit reports shared at the client's discretion	Reports shared under confidentiality with parties that need them	

3. The instrument: Table 4.12.b, One account, three readers

The instrument of this subchapter. The London questions as the hotel first answered them and as it answered them from evidence.

Question	What the certificate shows	What the evidence showed	Answer given from evidence
Is the hotel certified?	Yes, within scope	Yes, within scope	Yes: hotel operations; website and booking engine excluded

Question	What the certificate shows	What the evidence showed	Answer given from evidence
Are website, booking and payments covered?	Not in scope	Run by a third party on the operator's platform	Not certified; supplier's evidence provided; extension planned
Multi-factor authentication on all remote access?	Nothing specific	Staff yes; four supplier accounts no	Partly; supplier accounts completed within six weeks
Open nonconformities?	Nothing	One minor, fourteen months open, recurring	One minor, with cause, corrective action and date
Incidents in three years?	Nothing	One email compromise, reported and handled	One, described with lessons and changes made
Board oversight of cyber risk?	Top management review exists	No reporting to the fund's board	Not yet; quarterly report to the fund agreed
Backups offline and tested?	Nothing specific	Offline copy; restore tested last year	Yes, with the test record

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
Offering the certificate as the whole of the evidence.		
Answering specific control questions from the certificate instead of from facts.		
Letting different people answer different questionnaires without reconciling them.		
Leaving the owner unaware of audit findings and incidents.		
Presenting a certificate whose scope excludes what the reader cares about most.		
Failing to correct an inaccurate answer once discovered.		
Sharing detailed vulnerability reports with parties that do not need them.		

5. Action plan

Step from the book / gap found	Action in our property	Owner	Deadline
Prepare an evidence pack of scope, key controls, open findings, incidents and plans.			
Route every external questionnaire to one person who keeps all answers.			
Check every specific control with evidence before answering.			
Agree in advance what is shared with whom, under what confidentiality.			
Send the owner every audit report, finding status and significant incident.			
Document how areas outside the scope are managed, or plan to extend it.			

Step from the book / gap found	Action in our property	Owner	Deadline
Correct any inaccurate answer promptly, with the plan.			
Share vulnerability details only in summary and only where needed.			

In brief

To lenders, insurers and investors, a certificate is valuable evidence of governance and nothing more. The hotel presents it with its scope and limits, backs it with an evidence pack of key controls, open findings, incidents and plans, answers every questionnaire from that evidence through one person, shares reports under agreed confidentiality, keeps the owner informed, and corrects any wrong answer at once. It knows what its certificate proves and what it does not, and says both.

Source: The Helm and the Lens, Volume 5b: The Lens, subchapter 4.12. This sheet does not reproduce the text of the standard; work with your own copy of ISO/IEC 27001:2022 from an authorised source.