WORKSHEET 1.5

Scope, and the Boundary Drawn Around the Easy Part

Subchapter 1.5 · case in the book: Dubai

Find your certificate and read the sentence that describes its scope, word for word. Then write down the three places in your property where guests' information is most sensitive. If any of them falls outside that sentence, your certificate is accurate, and your guests would still be surprised by it.

This worksheet turns the tools of the subchapter into a form you can fill in. The texts come from the book; the empty columns are for your own property. Adapt it before use: an unadapted checklist is exactly what the book warns against.

Practical application: what to do in your property

Step (from the book)	Done?	What we found / owner
Read the scope statement on the certificate aloud, and compare it with what the website says.		
Trace the guest's information from booking to deletion, stage by stage.		
Lay the current scope over the route and mark every stage outside it.		
Write down each exclusion with its reason and the date it will be reconsidered.		
Name every out-of-scope system that touches the scope, and the control at that boundary.		
Correct every public statement about certification so that it matches the scope.		
Route every new system holding guest information through the owner of the system before signature.		
Show the full scope statement to the owner once a year.		

These steps are the book's method, not requirements of ISO/IEC 27001. Evidence can take whatever form suits the property; a separate document is needed only where an applicable requirement, or the property's own system, makes it necessary.

Verification Pact: what is believed, tested against the standard

What is commonly believed	What actually holds	Our position
«A narrow scope is a shortcut the standard does not allow.»	The standard allows any scope, provided it takes into account the context, the requirements of interested parties and the interfaces with activities outside it.	
«Scope means the IT department.»	Scope means the information and processes the system manages. In a hotel those run through every guest-facing department.	

What is commonly believed	What actually holds	Our position
«We are certified, so we can say the hotel is certified.»	A statement about certification has to reflect what the certificate covers. Anything broader invites the reader to believe something that is not true.	
«Exclusions do not need to be stated.»	The scope must be documented, and a scope whose boundary with the rest of the organisation is not stated cannot show that it has considered its interfaces.	
«Once certified, the scope is settled.»	The scope must be kept up to date as the organisation changes. New systems holding guest information are exactly the change that should prompt a review.	

Common mistakes: a self-check

Mistake (from the book)	Present here?	Action / owner
Choosing the scope that is easiest to certify rather than the one that protects the most sensitive information.		
Drawing the scope around the IT department instead of around guest information.		
Leaving exclusions unstated and unreasoned.		
Ignoring the systems at the boundary of the scope.		
Describing a certified department as a certified hotel.		
Adding systems that hold guest information without reviewing the scope.		
Never showing the scope statement to the owner.		

Operative synthesis

- **The scope is the boundary of the promise an information security system makes. Drawn around a department, it can be accurate and still mislead, because guests, clients and owners will assume it covers the places where their information actually lives. Drawn around information and the processes that handle it, with its exclusions stated and its boundaries managed, it becomes a promise the hotel can keep and describe honestly.**
- **The instrument is a page that follows the guest's information from booking to deletion and marks, at each stage, whether it is inside the scope and, if not, why and until when. Laid over the scope statement, it shows the owner in a few minutes what the certificate covers and what the hotel still has to decide.**
- **In Dubai nothing had been done dishonestly. A consultant gave sensible advice about where to begin, an IT director built a sound system inside the boundary he was given, a spa director chose the best booking system on the market, and a marketing team repeated a sentence that was true. The scope was never extended because nobody who could extend it knew what it said, and the first person outside the hotel to read it was a reporter.**
- **Which raises the question the next subchapter takes up. A great deal of the information inside any sensible scope is personal data, and personal data is governed by law as well as by the**

standard. What happens when a hotel keeps two registers of the same processes, one for the law and one for the standard, maintained by two people who never meet, is the case that follows.

Action plan for our property

Action	Owner	Due	How we will know it worked

Source: Francesco Dore, The Helm and the Lens, Volume 5a «The Helm», subchapter 1.5. Edizioni Effedore, 2026. Clause references are paraphrased; this sheet does not reproduce the text of ISO/IEC 27001. It is not legal advice: data protection and information security law is that of the place where the property operates.