WORKSHEET 1.3

Who Has an Interest in Your Guests' Data

Subchapter 1.3 · case in the book: Dublin

Find the last security questionnaire your property returned to a corporate client. Check who answered it, who approved it, and whether every «yes» on it is still true today. If nobody in the building can say, the most important interested party in your system is also the one you know least about.

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
Rebuild the list of interested parties from contracts, platform terms, bank agreements and questionnaires.		
Record each requirement in the party's own words and note where it is written.		
Mark each requirement yes, partly or no, and give every no a date or a reason.		
Route every security questionnaire to the owner of the system for review and approval.		
Read the requirements side by side and resolve conflicts between clients, suppliers and the law.		
Check contracts with security or data clauses before they are signed, not after.		
Make sure the scope of the certificate is stated accurately whenever it is mentioned to a client.		
Review the register with every major new contract and at every management review.		

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
«Interested parties are guests, staff and the regulator.»	They are whoever has written down requirements the hotel has accepted: clients, the bank, booking platforms, insurers, organisers, as well as guests and the law.	
«The questionnaire is a sales document.»	It is a written statement about the hotel's security that the client relies on. The system has to stand behind it.	

What is commonly believed	What actually holds	Our position
«Being certified means we can answer yes.»	A certificate covers a defined scope and says the system is managed. It does not make any particular control present everywhere.	
«The standard requires us to meet every requirement of every party.»	It requires the hotel to decide which requirements the system will address. Deciding not to meet one, and saying so, is allowed; pretending to meet it is not.	
«When a company books its staff with us, we process their data for the company.»	In most arrangements the hotel decides how it uses guest data and acts on its own account. A contract that describes it otherwise may not fit the facts and should be read before it is signed.	

Common mistakes: a self-check

Mistake (from the book)	Present here?	Action / owner
Listing interested parties as categories without their written requirements.		
Letting questionnaires be answered by whoever receives them.		
Answering yes when the truth is «our provider can» or «we intend to».		
Signing contracts with security clauses that the system has never seen.		
Promising a client a notification deadline shorter than the one accepted from a supplier.		
Presenting the certificate as covering more than its scope.		
Never writing no, and therefore never deciding what the hotel will not do.		

Operative synthesis

- **The interested parties that matter most to a hotel's information security are the ones who have written their requirements down and whose documents the hotel has signed or answered. They are found in contracts, platform terms, bank agreements and questionnaires, and they reach the hotel through sales, finance and reservations rather than through the system meant to meet them.**
- **The instrument is a register with one line per written requirement: the party and its words, where they are written, whether the system addresses them, and who in the hotel knows. Its third column is the one the standard added in 2022 and the one that turns a list of expectations into a set of decisions, including the decision to say no.**
- **In Dublin nothing was done dishonestly. A director of sales answered a form the way such forms are usually answered, an IT provider described what its systems could do, and a**

certificate made the rest look safe. The questionnaire became a set of promises that nobody in the system had read, and they were tested, as such promises usually are, by somebody who had bought a password.

› **Which raises the question the next subchapter takes up. Deciding what the hotel will promise, what it will protect and what it will spend is a decision for the people who run the business, not for the people who run its systems. What happens when an owner delegates information security to the IT provider and then takes, alone and for good reasons, the decision that creates the largest risk in the building 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 1.3. 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.