WORKSHEET 1.12

The Suppliers Who Hold the Keys

Subchapter 1.12 · case in the book: Tangier

List every company that can reach your property's systems from outside the building, including the ones that maintain your door locks, your lifts and your cameras. Beside each, write how many days its contract gives it to tell you about a breach on its side. If the column is empty, you will learn about it the way most hotels do: from somebody else.

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
List every supplier that can reach systems or information, from every department.		
Record what each supplier can reach and how it gets in.		
Replace permanent remote access with access opened on request, logged and closed.		
Ask key suppliers how their access is protected, whether it is separate, and who they depend on.		
Put notification, separate credentials, subcontractors, logs and exit into contracts at the next opportunity.		
Route every contract touching systems or information through the owner of the system before signature.		
Review key suppliers annually and whenever they change ownership, hosting or tools.		
Scale the effort to the access: full questions for keys to data and doors, few for the rest.		

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
«Supplier security means IT suppliers.»	It means every supplier that can reach the hotel's systems or information, including those for locks, lifts, cameras and building management.	
«Our supplier is reputable, so its access is secure.»	Reputation says nothing about how a particular access is protected. Only asking, and agreeing it in the contract, does.	

What is commonly believed	What actually holds	Our position
«The maintenance agreement covers the relationship.»	Maintenance agreements usually cover physical service levels and say nothing about access, notification or data.	
«Permanent remote access is necessary for support.»	Support can usually be given through access opened on request, logged, and closed afterwards.	
«We cannot impose terms on suppliers.»	Hotels have most influence before signature, and more influence over regional suppliers than they assume.	

Common mistakes: a self-check

Mistake (from the book)	Present here?	Action / owner
Listing only IT suppliers and ignoring those for locks, lifts, cameras and building systems.		
Choosing suppliers on design, reliability and price without asking about access and security.		
Signing maintenance agreements that say nothing about access, notification or data.		
Leaving permanent remote access open for convenience.		
Accepting notification by general email to an address nobody reads.		
Never asking suppliers who they depend on.		
Renewing agreements by invoice without reviewing what has changed.		

Operative synthesis

- **Every supplier that can reach a hotel's systems holds a key, and most modern hotel equipment, from locks to lifts to televisions, comes with a supplier who can reach it. The owner chooses those suppliers and signs their contracts, and those two moments are when the hotel can decide how its keys are held: how access is protected, how quickly incidents are reported, who else is involved, and what happens at the end.**
- **The instrument is a register of keys: every supplier that can reach systems or information, what each can reach, how it gets in, what its contract requires, and when it was last reviewed. With a short set of questions asked before selection and a few standard clauses, it gives the owner a clear view of where the hotel's security depends on others.**
- **In Tangier nothing had been chosen carelessly. The owner selected an excellent lock system, the engineering department maintained a sound agreement for twelve years, and the supplier served its clients faithfully until somebody took the one login that opened all of them. The contract had been written when locks were mechanical, and nobody had noticed that they had stopped being so.**
- **Which raises the question the next subchapter takes up. Suppliers hold keys, but so do the hotel's own staff, and in many hotels most of those staff change every season. What happens**

when the staffing model itself, decided by the owner for sound commercial reasons, sets the hotel's exposure before any system is configured, 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 1.12. 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.