WORKSHEET 2.7

Checking In Guests With the System Down

Subchapter 2.7 · case in the book: Mexico City

Imagine that at two o'clock tomorrow morning every computer in your property stops working and will not start again for four days. Write down, without asking anybody, how the night manager will know who is in which room, how tomorrow's arrivals will get keys, and who will decide what to do first. Whatever you could not write down is what your continuity plan is missing.

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 what the hotel must do without systems, and the fallback for each.		
Produce each night a list of in-house guests and arrivals and keep it off the network.		
Keep registration cards, a manual key procedure and fallback payment terminals ready.		
Keep at least one backup where an attack on the hotel's network cannot reach it.		
Restore from backup in a test at least once a year, and record how long it took.		
Name the decision-maker for any hour, with a deputy, and give them a first-hour checklist.		
Practise checking in without systems once a year, on a quiet night.		
List the dependencies of the desk, not only of the property system.		

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
«Our property system is in the cloud, so it cannot go down.»	The hosted system may survive. The desk's ability to reach it, the key encoder, the terminals and the phones may not.	
«We have backups.»	A backup the attack can reach is encrypted with everything else, and a backup never restored in a test may not restore in time.	
«The plan says recovery in eight hours.»	Recovery takes as long as it takes. Only a test tells the hotel how long that is.	

What is commonly believed	What actually holds	Our position
«The offline list is never used, so it is waste.»	Fallbacks are never used until they are the only thing that works. Keeping them ready is the plan.	
«The IT manager is in charge of system failures.»	An attack at two in the morning needs a decision-maker who is there, or can be reached, with a deputy named.	

Common mistakes: a self-check

Mistake (from the book)	Present here?	Action / owner
Writing a recovery time into the plan without ever measuring it.		
Removing the offline list and the paper fallbacks because they are never used.		
Keeping backups where the attack can reach them.		
Never restoring from backup in a test.		
Naming as decision-maker somebody who may not be reachable, with no deputy.		
Planning around the property system and forgetting the desk's other dependencies.		
Never practising a check-in without systems.		

Operative synthesis

- **A hotel's continuity after an attack is decided before it, by what the hotel keeps ready and has tested. The list of who is in the house and who is arriving, kept where the attack cannot reach it. Cards, keys and payments by hand. A backup the attack cannot reach, restored in a test so that the recovery time is known. A decision-maker at any hour. Staff who have practised. None of it is expensive, and none of it can be improvised.**
- **The instrument is a page in the night manager's office, and a copy outside the building, that lists for each essential function the fallback kept ready, who runs it and when it was last tested, together with the first-hour checklist. It is the whole of a hotel's continuity plan, and it is the part that matters at two in the morning.**
- **In Mexico City nothing had been done carelessly. A general manager reduced paper for good reasons, an IT provider kept backups faithfully, a plan was written and approved, and a night manager did everything she could with what she had. The list that would have told her who was in each room had been abolished because it was never needed, and the backup that would have restored the hotel in hours was on the same network as the attack.**
- **Which raises the question the next subchapter takes up. Some of the systems a hotel depends on are ones it chose and bought itself, and the moment of choosing them is when the hotel has most influence over how secure they will be. What happens when a new property system is chosen on features and price, and nobody asks a single question about security or about how to leave, 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 2.7. 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.