Backups That Have Never Been Restored

GUIDING QUESTION *Ask for last month's backup report and count the green lines. Then ask a different question: when did anybody last bring back one of those copies and use it, and how long did it take? If the answer is never, the green lines tell you that something was copied. They do not tell you that anything can be recovered.*

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
«Every job is green, so we are backed up.»	Green means the job ran. Only a restore shows whether the hotel could recover, for what was tested.	
«The provider backs up everything.»	The provider backs up everything on its list. The list is rarely the same as the hotel's inventory.	
«If the database is safe, the system is safe.»	Data restores in hours. The working service, with licences, interfaces and settings, can take days.	
«The cloud supplier backs up our data.»	It backs up its platform. Restoring one customer's lost records is often not in the contract.	
«Testing backups is the IT provider's job.»	Performing the restore is. Deciding what must be recoverable, and how fast, is the hotel's.	

2. What the standard requires, and what demonstrates it

From Table 3.10.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 in a hotel	In our property
Backups per an agreed policy	A short page stating what is copied, how often, for how long and where, approved by the hotel	
Backups regularly tested	Dated records of restores, with the time taken and what was found	
Readiness based on continuity objectives	For each critical system, how much data may be lost and how long it may be down, set by management	
Redundancy for availability	A second path for what cannot stop: a spare encoder, a copy off the network	
Inventory of assets	A list of systems, including those installed by other suppliers, reconciled with the backup list	
Cloud services managed	For each hosted service, what the supplier restores, for whom, and how the hotel gets its own copy	

3. The instrument: Table 3.10.b, The restore test sheet

The instrument of this subchapter. One line per system in the sample, completed during the test and signed by the auditor and the person who performed the restore.

System	What the hotel believed	What the test showed	Decision
Property system: data	Copied nightly, recoverable	Restored complete in under three hours	No change; retest yearly

System	What the hotel believed	What the test showed	Decision
Property system: service	Back in eight hours	About three days: licences, interfaces and settings not copied	Copy configuration; write the rebuild order; target one day
Lock server	Backed up with everything else	Never on the provider's list; no copy in six years	Add to backup; spare encoder; lock supplier to document recovery
Finance papers	Any file can be recovered	Only the last fourteen days	Keep copies for at least two months
Cloud sales platform	The supplier backs it up	Supplier restores its platform, not one customer's records	Monthly export held by the hotel; clause added at renewal
Database copies	Kept for safety	Kept a year, beyond the hotel's guest data rules	Retention aligned with the hotel's schedule
Encryption key	The provider has it	One engineer holds the key and the recovery order	Key in escrow; second engineer trained; procedure written

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
Reading a green backup report as proof that the hotel can recover.		
Accepting the provider's list of copied systems without comparing it to the hotel's inventory.		
Testing the restore of data but never the restore of a working service.		
Leaving backup frequency and retention at the software's defaults.		
Assuming a cloud supplier's backups protect the hotel's own records.		
Letting one person hold the encryption key and the knowledge of recovery.		
Testing restores on the live system, or testing everything at disproportionate cost.		

5. Action plan

Step from the book / gap found	Action in our property	Owner	Deadline
Ask the provider to explain exactly what a green backup mark confirms.			
Reconcile the list of systems copied with the hotel's inventory, including back-of-house machines.			
Have management state, for each critical system, acceptable data loss and downtime.			
Choose a sample of restores, including one full system to a working state.			
Test in an isolated environment, at a quiet time, with success agreed in advance.			
Time each restore and record every missing key, licence, password or setting.			

Step from the book / gap found	Action in our property	Owner	Deadline
Check where the encryption keys are and who else can perform the recovery.			
Align backup retention with both recovery needs and the hotel's data retention rules.			

In brief

A backup is audited by restoring from it. The internal auditor reads the report for what it actually confirms, reconciles the list of copied systems with the hotel's own inventory, asks management how much loss and downtime the hotel can accept, chooses a sample of restores that includes a whole system brought back to working order, watches and times the test in an isolated environment, and records every key, licence and person the recovery depended on. The finding is the gap between what the hotel believed and what the test showed.

Source: The Helm and the Lens, Volume 5b: The Lens, subchapter 3.10. This sheet does not reproduce the text of the standard; work with your own copy of ISO/IEC 27001:2022 from an authorised source.