Second-Party Audit: The Software House and the Cloud

GUIDING QUESTION *Take the certificate your property system supplier sent you last year and read the scope statement on it, word for word. Then write down, in one sentence, the service your hotel actually buys from that supplier. If the two sentences do not describe the same thing, the certificate is about somebody else's business, and the assurance you have been relying on does not exist.*

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
«The supplier is certified, so our data is safe with it.»	A certificate covers a stated scope. Whether it includes your service is the first question.	
«A questionnaire answered yes shows the controls exist.»	It shows somebody answered yes. Evidence shows the controls exist.	
«We cannot audit a cloud provider.»	You can read its assurance, ask for evidence on what matters and write your needs into the contract.	
«Our supplier holds our data.»	Often a subcontractor you have never heard of holds it. Ask who.	
«An annual approval is supplier monitoring.»	Monitoring means reviewing practices and service delivery, including what the supplier's own reports say went wrong.	

2. What the standard requires, and what demonstrates it

From Table 3.7.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
Supplier risks managed	A list of the few suppliers that hold information or run critical systems, each with its risks	
Requirements agreed with each supplier	Contract terms on backups, restore times, incidents, subcontractors and assurance	
Supply chain risks managed	The names of the data centres and subcontractors behind each critical service	
Suppliers monitored and reviewed	An annual reading of scope, assurance report and exceptions, with follow-up	
Cloud services acquired, used and exited under control	Exit and data return terms, and a known restore time	
Backups tested, including by suppliers	Evidence of the supplier's last restore test for the hotel's data	

3. The instrument: Table 3.7.b, Reading a supplier's assurance

The instrument of this subchapter. One page per critical supplier, completed at each annual review.

Document or question	What to read first	What it tells the hotel	Red flag
The supplier's certificate	The scope statement, and the public register	Whether the supplier's system covers the service bought	Scope names development or an office, not the hosted service
Independent assurance report	Type of report; service and date or period covered; subcontractors; exceptions	How the service actually ran, and what failed	Exceptions on backups, access or subcontractor oversight

Document or question	What to read first	What it tells the hotel	Red flag
Restore test evidence	Date, database, result, time taken	Whether the hotel's data can come back	No test of the hotel's data in the last year
Support access	Who can reach the hotel's data, how, with whose approval	Whether support is a controlled door	Shared accounts; no record of sessions
Incident notification	The commitment in the contract and the named contact	How fast the hotel will know	No time stated; general email address only
Subcontractor list	Names of hosting and support companies	Who actually holds the data	Supplier cannot or will not name them
Exit and data return	Format, time and cost of returning the data	Whether the hotel can leave	No terms, or data returned only as a printout

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
Accepting a supplier's certificate without reading its scope.		
Sending a questionnaire and accepting the answers without evidence.		
Not knowing which company actually hosts the hotel's data.		
Never asking for the supplier's independent assurance report, or not reading its exceptions.		
Leaving backups, restore times, incidents and subcontractors out of the contract.		
Approving critical suppliers every year without follow-up.		
Spending supplier review effort on suppliers that hold nothing of consequence.		

5. Action plan

Step from the book / gap found	Action in our property	Owner	Deadline
Identify the four to eight suppliers that hold guests' information or run critical systems.			
Describe in one sentence the service the hotel buys from each.			
Read the scope of each supplier's certificate and confirm it in the public register.			
Ask for the independent assurance report on the service and read its exceptions first.			
Ask for evidence on restore tests, support access, incident notification and subcontractors.			
Speak to somebody who runs the service, not only the account manager.			

Step from the book / gap found	Action in our property	Owner	Deadline
Check the contract for each need, and send missing terms to whoever negotiates the renewal, or raise them at once where the risk or the law requires.			
Start each year’s review from the previous year’s exceptions and follow-up list.			

In brief

A second-party audit examines the service the hotel buys, not the supplier’s logo. It chooses the few suppliers that hold the hotel’s information or run its critical systems, describes each service in a sentence, reads the scope of any certificate and the exceptions in any independent report, asks for evidence on the controls that matter, identifies the subcontractors in the chain, checks the contract and follows up. It is a reading and a conversation rather than a site visit, and it takes a day.

Source: The Helm and the Lens, Volume 5b: The Lens, subchapter 3.7. This sheet does not reproduce the text of the standard; work with your own copy of ISO/IEC 27001:2022 from an authorised source.