The Penetration Test and What It Did Not Test

GUIDING QUESTION *Find your hotel's most recent penetration test report and do not read the conclusion. Turn instead to the page that says what was tested. Then list, without looking at the report, the ways somebody could reach your guests' data: through the website, the guest network, a supplier's remote access, a meeting room socket, a telephone call to the desk. Count how many of them are on the page you just read.*

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
«No critical vulnerabilities means the hotel is secure.»	It means none were found in what was tested. What was tested is on the last pages.	
«The IT provider commissions the test, so it is independent.»	The provider is testing its own work. The scope should be set by somebody who is not.	
«Last year's scope is still valid.»	Every new system, supplier or guest service changes the routes in. The scope must follow.	
«Suppliers' systems are the suppliers' problem.»	The routes through them lead into the hotel. The hotel tests its side and asks for theirs.	
«Findings marked fixed are fixed.»	A fix is confirmed by a retest. Recurring findings show what is never fixed.	

2. What the standard requires, and what demonstrates it

From Table 3.12.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
Vulnerabilities identified, exposure evaluated	A map of routes in, each marked tested, scanned, accepted or unknown	
Measures taken	Findings tracked to closure, with retests and a year-on-year comparison	
Testing of new systems	A test or review before a new guest app, lock system or supplier connection goes live	
Networks segregated	Guest, conference, staff and building networks shown to be separate, from inside	
Independent review	Scope of testing set or approved by somebody independent of the systems tested	
Internal audit	The auditor's comparison of scope with routes, recorded as a finding	

3. The instrument: Table 3.12.b, Scope over surface

The instrument of this subchapter. One line per route into the hotel, reviewed each year before the next test is ordered and whenever a significant system or supplier is added.

Route into the hotel	In last year's test?	What that means	Decision
Website, email, staff remote access	Yes, from outside	Examined well; nine medium findings recur yearly	Keep; close the recurring findings; retest highs

Route into the hotel	In last year's test?	What that means	Decision
Guest network	No	Nobody knows whether a guest can reach staff systems	Test from inside this year
Meeting room sockets	No	Installed after the scope was written	Add; confirm they reach only the conference network
Lock system and supplier's remote access	No	Supplier-managed; never examined by anybody	Ask supplier for evidence; test the hotel's side
Property system supplier's support connection	No	Permanent connection; excluded as third party	Review how it is opened and closed; include in test
Booking engine and guest app	No	Launched after the scope was written	Obtain supplier's test report; test the hotel's integration
Staff by email and telephone	No	The commonest way into hotels, never tested	An agreed, announced exercise, approved by ownership
Payment terminals	No	Covered by the card industry's own assessment	Record as covered elsewhere, with the evidence

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 test's conclusion as a statement about the whole hotel.		
Letting the party responsible for the systems set the scope of their test.		
Copying the scope from year to year while the hotel changes.		
Testing only from outside in a building full of strangers on its networks.		
Excluding suppliers' routes because the systems belong to someone else.		
Reading each year's report alone, so recurring findings go unnoticed.		
Running aggressive tests on live hotel systems without approval, timing or limits.		

5. Action plan

Step from the book / gap found	Action in our property	Owner	Deadline
Read the scope, method, effort and exclusions of every test report before its conclusion.			
Draw a map of every route into the hotel, from outside and from inside.			
Mark each route as tested, scanned, covered by a supplier, accepted or unknown.			
Have the scope approved by somebody independent of the systems tested.			

Step from the book / gap found	Action in our property	Owner	Deadline
Review the scope whenever a significant system, supplier or guest service is added.			
Compare findings across years and retest those marked fixed.			
Ask suppliers for evidence of testing, and test the hotel's side of each connection.			
Set rules, timing, limits and a stop procedure for any test on live hotel systems.			

In brief

A penetration test is audited by reading its scope before its results. The internal auditor draws a map of every route into the hotel, lays the tested scope over it, and records the routes about which the hotel knows nothing. The auditor then asks who set the scope and whether they were independent, whether it reflects the hotel as it is now, what method and effort were bought, whether findings were retested and whether they recur. None of this requires the auditor to test anything; all of it determines what the test can be relied on for.

Source: The Helm and the Lens, Volume 5b: The Lens, subchapter 3.12. This sheet does not reproduce the text of the standard; work with your own copy of ISO/IEC 27001:2022 from an authorised source.