Auditing Accounts and the Rights Behind Them

GUIDING QUESTION *Take the last access review your heads of department signed and pick one name from it. Ask the manager who signed what that person can do in the property system: not what their job is, but what the system allows them to do. If the manager cannot answer without looking it up, the signature confirmed a list of names, not a set of rights.*

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 heads of department signed, so access has been reviewed.»	A signature confirms a review only if the signer could understand what was listed.	
«No changes means everything is correct.»	No changes over many quarters usually means the review has stopped finding things.	
«The property system is where the risk is.»	Finance, payments, email, locks and booking extranets often carry as much risk, or more.	
«Technical accounts are IT's business.»	They hold the most power, and must be reviewed by somebody accountable for them.	
«Each right is justified, so the person's access is fine.»	Some rights are harmless alone and dangerous together. Combinations must be looked at.	

2. What the standard requires, and what demonstrates it

From Table 3.11.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
Access control rules	A page stating, per job, what each system should allow, in the language of the work	
Access rights reviewed	Reviews covering all critical systems, with changes recorded when needed	
Privileged rights restricted	A named owner for every administrator, supplier and technical account, reviewed like the rest	
Identity life cycle managed	New rights granted per job, not copied from a colleague; moves trigger a review	
Segregation of duties	A short list of forbidden combinations, and a check that nobody holds them	
Secure authentication	Stronger sign-in for administrator and remote accounts	

3. The instrument: Table 3.11.b, The ten-person sample

The instrument of this subchapter. One line per person or account in the sample, completed with the supervising manager and the IT coordinator, and repeated once a year. Eight of the ten Oslo lines are shown.

Person or account	What the work requires	What the systems allow	Finding and decision
Night receptionist	Small adjustments with a limit; close the day	Unlimited adjustments without approval; close the day	Conflicting pair: limit adjustments; manager approval above the limit

Person or account	What the work requires	What the systems allow	Finding and decision
Housekeeping supervisor	Room status, lost property	Room status plus rate changes, copied from a former front office colleague	Rate rights removed; new staff set up by job, not by colleague
Events coordinator	Event bookings, deposits	Refunds to any card	Refunds moved to finance with a second approval
Sales manager	Company profiles, event history	Export of all guest profiles	Export limited to company accounts; exports logged
Reservations agent (moved from front desk)	Reservations only	Reservations plus front desk cash and keys	Old rights removed; moves trigger a review
Accounts payable clerk	Enter invoices	Enter invoices, create suppliers, approve payments	Supplier creation moved to the finance manager
TRAINING account	Nothing: training ended	Full front office rights, shared password	Disabled; training accounts created and closed per course
Supplier support account	Access on request, for a ticket	Permanent access, no second sign-in	Enabled per request; stronger sign-in; named owner at the hotel

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 signed access reviews without testing whether the signers understood them.		
Reviewing only the system from which a user list is easy to export.		
Leaving administrator, supplier and technical accounts outside every review.		
Setting up new staff with the rights of a colleague.		
Reviewing each right alone and never looking at combinations.		
Treating many quarters without a change as proof of good control.		
Restricting rights so tightly that staff share a manager's login to serve guests.		

5. Action plan

Step from the book / gap found	Action in our property	Owner	Deadline
Ask three signers to explain what two people on their list can actually do.			
Sample ten people across departments, including technical and supplier accounts.			
Ask each supervising manager what the job requires, before consulting the systems.			
Translate every role the person holds into actions, in every system they can reach.			

Step from the book / gap found	Action in our property	Owner	Deadline
List everybody holding the five or six most sensitive rights.			
Agree a short list of forbidden combinations and check who holds both halves.			
Read the last ten access requests to see how rights are granted.			
Record the review's scope, changes and exceptions, not only the signature.			

In brief

An access review is audited by performing it again on a sample. The internal auditor tests whether the signers can read what they sign, samples ten people and asks both the manager and the systems what each can do, lists who holds the most sensitive rights, checks the combinations that should never be held together, and looks at how rights are granted in the first place. The finding is the distance between what the work requires and what the systems allow, and whether the hotel's review could ever have seen it.

Source: The Helm and the Lens, Volume 5b: The Lens, subchapter 3.11. This sheet does not reproduce the text of the standard; work with your own copy of ISO/IEC 27001:2022 from an authorised source.