Change During the Cycle: New System, New Owner, New Edition

GUIDING QUESTION *Think of the biggest change your hotel made to its systems in the past year. Find the risk assessment written for it, the update to your statement of controls, the record of what happened to the old equipment and the letter telling your certifier. If any of these does not exist, the change passed around your management system rather than through it, and the system now describes a hotel that has moved on.*

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
«A smooth migration is a secure migration.»	Smoothness concerns guests. Security concerns test data, access, disposal and the controls after the change.	
«IT projects are for IT; security reviews the result.»	Security must be in the project from its first meeting, not after go-live.	
«Real data makes the best test data.»	Real personal data in testing needs protection and authorisation, and deletion afterwards.	
«The certifier only needs to know at surveillance.»	Major changes must be notified when they happen.	
«The new edition only renumbered the controls.»	It added controls. Declaring them not applicable needs a justification that survives the next change.	

2. What the standard requires, and what demonstrates it

From Table 4.14.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 for a significant change	In our property
Changes planned	A risk assessment of the change and a review of the statement of controls before go-live	
Security in project management	A named security member of the project and a sign-off before go-live	
Test information protected	Masked or minimal test data; test environment closed and wiped after go-live	
Cloud services managed	The cloud control applied, with supplier terms and exit plan	
Secure disposal	Certificates of data destruction for every disposed storage medium	
Certifier informed; transition real	A letter to the certifier; new controls assessed against actual risks	

3. The instrument: Table 4.14.b, The change passport

The instrument of this subchapter. One page for every significant change, completed by the project team and the coordinator, signed before go-live.

Question	Relevant control	What happened in Mumbai	What should have happened
Were the risks of the change assessed?	Planning of changes; project management	No; security not on the project team	Risk assessment before contract; coordinator on the team
Was the statement of controls reviewed?	Statement of applicability; cloud services	No; cloud control still not applicable	Cloud control applied; statement updated before go-live
How was test data handled?	Test information	Full copy of real guest data; environment left open	Masked data; real data only if authorised, deleted after
Who had access during and after?	Access rights; supplier relationships	Six consultants, access never removed	Named access, removed on go-live day
Were interfaces and acceptance tested for security?	Security testing in acceptance	Tested for function only	Security checks included in acceptance
What happened to the old equipment?	Secure disposal; information deletion	Disks sent to recycler without instruction	Wiped or destroyed with certificates
Was the certifier informed?	Certification rules	No	Letter before the change, with the plan

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
Running a major system migration without the information security coordinator.		
Testing with full copies of real guest data and forgetting the test environment.		
Disposing of old storage media without secure destruction and certificates.		
Leaving the statement of controls describing systems that no longer exist.		
Telling the certifier about major changes only when asked at surveillance.		
Treating a new edition of the standard as a renumbering exercise.		
Applying heavy change control to trivial changes until people bypass it.		

5. Action plan

Step from the book / gap found	Action in our property	Owner	Deadline
Agree a short list of changes that must pass through the management system.			
Put the coordinator on every significant project from its first meeting.			
Complete a change passport and sign it before go-live.			
Test with masked data; close test environments and remove access on go-live day.			

Step from the book / gap found	Action in our property	Owner	Deadline
Wipe or destroy old storage media and keep the certificates.			
Update risk assessment and statement of controls before the change takes effect.			
Tell the certifier of major changes before they happen.			
Watch the standards, and treat each new edition as a review of real risks.			

In brief

Significant change passes through the management system before it takes effect. The hotel defines what is significant, puts security on every such project, completes a change passport, protects test data, disposes of old media securely, updates its risk assessment and statement of controls before go-live, tells the certifier of major changes, and treats each new edition of the standard as a review of real risks. Everything else is handled lightly.

Source: The Helm and the Lens, Volume 5b: The Lens, subchapter 4.14. This sheet does not reproduce the text of the standard; work with your own copy of ISO/IEC 27001:2022 from an authorised source.