Root Cause, and the Answer That Is Not the Employee

GUIDING QUESTION *Take the last three information security incidents your hotel recorded and read the cause written against each. If any of them says human error, staff error or failure to follow procedure, ask what made the error possible, and whether that has changed. If it has not, the incident is waiting to happen again with a different name beside it.*

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
«Human error is a root cause.»	It is where the search for causes begins. The cause is what made the error possible.	
«A warning to the employee is a corrective action.»	A corrective action removes a cause. A warning changes nothing about the tool, the data or the process.	
«Retraining fixes human error.»	Only if the person did not know. Most errors happen to people who know perfectly well.	
«The incident happened at one desk, so the cause is at one desk.»	The same conditions usually exist wherever the same task is done.	
«Firm consequences make staff more careful.»	They make staff less willing to report. Mistakes continue; reports stop.	

2. What the standard requires, and what demonstrates it

From Table 3.9.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
Causes determined	A cause recorded that describes a tool, process, data or condition, not a name	
Similar nonconformities looked for	A note of every other place where the same task is done, and what was found	
Corrective action appropriate to effects	At least one change for each of: possible, likely, not caught, serious	
Learning from incidents	Changes to templates, tools and rules traced to the incident	
Formal disciplinary process	A separate, communicated process for violations, decided apart from the investigation	
Events reported	The number of self-reported mistakes rises after the investigation, not falls	

3. The instrument: Table 3.9.b, From the person to the process

The instrument of this subchapter. One page per incident that appears to be human error, completed before any corrective action is agreed.

Question	Answer that stops at the person	Answer that reaches the process	Change that follows
What happened?	The agent sent the list to the wrong agency	A rooming list left the hotel addressed to a similarly named agency	None yet: this is the event
Why was it possible?	She did not check the address	The email program completes addresses; two agencies differ by one word	Autocomplete off for external addresses; agencies renamed clearly in the address book

Question	Answer that stops at the person	Answer that reaches the process	Change that follows
Why was it likely?	She was careless	Fifty lists a day, most sent at the end of a shift	Lists sent from the property system's secure transfer, not by hand
Why was it not caught?	She should have noticed	Nothing checks a list with sensitive data before it leaves	A warning when an email contains passport or health data
Why was it serious?	The list was confidential	The report included fields the agency did not need	Rooming list template limited to names, dates and room types
Where else?	Not asked	Sales, events and spa send lists the same way	Same changes applied in all four departments
What did the response teach?	Not asked	Two other misdirected emails were hidden after the first warning	Mistakes reported without disciplinary consequence unless deliberate

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
Recording human error as the root cause of an incident.		
Using a disciplinary warning as the corrective action.		
Retraining a person who already knew what to do.		
Investigating without watching the task.		
Leaving unchanged the templates and reports that send more data than needed.		
Confining the corrective action to the desk where the incident happened.		
Ignoring what the response to the incident has taught staff about reporting.		

5. Action plan

Step from the book / gap found	Action in our property	Owner	Deadline
Never record human error, staff error or failure to follow procedure as a cause.			
Keep any disciplinary question separate from the investigation of causes.			
Watch somebody doing the same task before deciding what caused the incident.			
Ask why the error was possible, why it was likely, why it was not caught and why it was serious.			
Compare what was sent or exposed with what was needed, and change the templates that send too much.			
Look for the same conditions wherever the same task is done.			

Step from the book / gap found	Action in our property	Owner	Deadline
Ask the team whether similar mistakes have happened and been hidden.			
Check some months later whether the error has become harder to make or less harmful.			

In brief

Human error is where the investigation of an incident begins. The internal auditor sets any question of discipline aside, watches the task, asks why the error was possible, likely, uncaught and serious, compares what was exposed with what was needed, looks for the same conditions wherever the same task is done, asks the team what else has happened, and checks later whether the error has become harder to make. The causes found are tools, templates, workloads and rules, and they can be changed.

Source: The Helm and the Lens, Volume 5b: The Lens, subchapter 3.9. This sheet does not reproduce the text of the standard; work with your own copy of ISO/IEC 27001:2022 from an authorised source.