The Digital Near-Miss

GUIDING QUESTION *Count the entries in your information security incident register for the last twelve months, then ask your IT provider how many phishing messages were blocked, how many logins failed and how many suspicious calls the desk refused in the same period. If the first number is close to zero and the others are in the hundreds, your register records what nobody saw, not what happened.*

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
«An empty incident register shows a safe hotel.»	It shows a hotel that records nothing. Hotels receive a continuous stream of hostile events.	
«Staff should report incidents.»	The standard asks them to report events, including suspected ones. Incidents are a decision made afterwards.	
«Blocked attacks are a sign that security works.»	They are evidence a control works, and their pattern shows where the hotel is targeted. Both need reading.	
«If there are no incidents, the incident process cannot be audited.»	It can be audited through the events that should have entered it.	
«Reporting near misses creates unnecessary work.»	A few minutes of assessment per event is the cheapest risk assessment available.	

2. What the standard requires, and what demonstrates it

From Table 3.5.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
Events reported through appropriate channels	One address or number known to every department, and reports actually received	
Events assessed and decided	A log of events with the decision beside each	
Learning from incidents	Changes to training, controls or risks traced to events	
Logs produced and analysed	Someone reads the gateway and sign-in figures and acts on patterns	
Monitoring for anomalous behaviour	Alerts on repeated failed sign-ins for sensitive accounts, received and acted on by somebody named, at any hour	
Effective implementation audited	The auditor samples the stream of events, not only the register	

3. The instrument: Table 3.5.b, Near misses as evidence

The instrument of this subchapter. One page per audit, setting what the systems and people saw beside what the hotel recorded.

Source of events	What it shows	What the auditor asks	What an absence means
Email gateway: blocked messages	Filter working; who is targeted	Which people receive the most targeted messages?	Nothing: blocked messages are normal
Sign-in records: failed attempts	Accounts under attack	Is there an alert on repeated failures for sensitive accounts?	Monitoring not configured

Source of events	What it shows	What the auditor asks	What an absence means
Front desk: suspicious callers	Staff applying the never list	What calls came last month, and were any reported?	Reporting route unknown or unused
Staff reports of odd messages	Awareness working	How many reports in the year, and from which departments?	Staff do not know what to report
Supplier remote sessions outside hours	Doors used unexpectedly	Who reviewed them, and what was decided?	Nobody reads the log
Event log with decisions	Assessment working	Was each event assessed, and by whom?	Events collected but not assessed
Changes traced to events	Learning working	What changed this year because of what was seen?	The hotel is not learning

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
Reporting zero incidents as evidence of security.		
Asking staff to report incidents rather than events.		
Publishing a reporting address that nobody knows or uses.		
Treating the count of blocked attacks as a performance figure rather than as evidence to read.		
Collecting events without assessing them.		
Learning nothing from the pattern of events.		
Concluding that the incident process cannot be audited because the register is empty.		

5. Action plan

Step from the book / gap found	Action in our property	Owner	Deadline
Set the incident and event register beside the systems' figures at the start of every audit.			
Look for patterns in blocked messages and failed sign-ins, and for alerts on sensitive accounts.			
Ask staff in each department what they have seen, and whether they reported it.			
Test the reporting route with a harmless, agreed suspicious message or call.			
Check that every recorded event has an assessment and a decision.			
Trace changes in training, controls and risks back to the events that caused them.			
Report the stream of events to management, not only the count of incidents.			

Step from the book / gap found	Action in our property	Owner	Deadline
Treat an empty register in a busy hotel as a signal, and record a finding when the events seen by systems and staff show what the register missed.			

In brief

Near misses are the evidence an internal audit most needs and most often ignores. The auditor sets the stream of events recorded by systems and seen by people beside the hotel's register, looks for patterns, asks staff what they have seen and reported, tests the reporting route, checks that events are assessed, traces what the hotel has learned, and reports the whole stream to management. An empty register in a busy hotel is a question about reporting, and a finding once the stream of events shows what it missed; it is never a sign of safety.

Source: The Helm and the Lens, Volume 5b: The Lens, subchapter 3.5. This sheet does not reproduce the text of the standard; work with your own copy of ISO/IEC 27001:2022 from an authorised source.