WORKSHEET 1.14

The Management Review That Hears Bad News

Subchapter 1.14 · case in the book: Montreal

Read the minutes of your last management review of information security and find the item that described something going wrong, nearly going wrong, or being reported by a member of staff. If there is none, the review heard only what the people presenting chose to bring, and those are rarely the people who see trouble first.

This worksheet turns the tools of the subchapter into a form you can fill in. The texts come from the book; the empty columns are for your own property. Adapt it before use: an unadapted checklist is exactly what the book warns against.

Practical application: what to do in your property

Step (from the book)	Done?	What we found / owner
List the places in the hotel where bad news is written down.		
Ask the night manager and front office manager for a monthly note of anything touching information.		
Build the review agenda from the inputs the standard lists, with a named person for each.		
Have the owner attend the discussion of inputs and ask what is missing.		
Record decisions with owners and dates, and start the next review with them.		
Tell the team what was done about the warnings they reported.		
Convene a short additional review when a serious near miss or major change occurs.		
Let the person reading the logs filter; bring decisions, not noise, to the review.		

These steps are the book's method, not requirements of ISO/IEC 27001. Evidence can take whatever form suits the property; a separate document is needed only where an applicable requirement, or the property's own system, makes it necessary.

Verification Pact: what is believed, tested against the standard

What is commonly believed	What actually holds	Our position
«The review is the IT provider's annual report.»	The review is top management's judgement on the system, drawing on a list of inputs of which the provider's report is one.	
«The owner needs only to approve the conclusions.»	Top management must review the system, which means taking part in considering the inputs, not only the outputs.	

What is commonly believed	What actually holds	Our position
«Suitable, adequate and effective is the conclusion.»	It is the purpose of the review. The required outputs are decisions about improvement and changes to the system.	
«Near misses are operational matters for the front office.»	They are feedback on performance and, often, the earliest warning of an incident. They belong among the review's inputs.	
«Nothing changed, so nothing needs deciding.»	Interested parties' requirements, suppliers, staff and threats change every year. A review that finds nothing to decide has not looked.	

Common mistakes: a self-check

Mistake (from the book)	Present here?	Action / owner
Building the review on the IT provider's report alone.		
Leaving near misses in the night log and the front office book.		
Having the owner attend only to approve the conclusions.		
Concluding that the system is suitable, adequate and effective without recording any decision.		
Failing to follow up the previous review's actions.		
Ignoring changes in insurers', clients' and platforms' requirements.		
Giving nobody the job of bringing bad news.		

Operative synthesis

- **A management review decides only on what it hears, and in a hotel the first signs of trouble are heard at the desk, on the telephone and at night, by people who are not in the room. A review built on the reports of those who run the system will hear that it runs. A review built to hear bad news, with a named person bringing each input and a route from the logs to the table, will hear the warning before the incident.**
- **The instrument is an agenda with a line for every input the standard requires and a person responsible for each, including the near misses recorded in the hotel's own logs. With minutes that record decisions and an owner who attends the discussion, it turns an annual formality into the moment when the hotel decides what to change.**
- **In Montreal nothing had been concealed. A night manager recorded a warning precisely, a front office manager read the log for what she needed from it, an IT provider reported faithfully on its tools, and an owner signed minutes that were accurate in every word. The warning and the review were three floors and several months apart, and nobody's job was to carry one to the other.**
- **Which raises the question the next subchapter takes up, the last of this chapter. Everything so far has concerned systems, registers and decisions. The oldest protection of guests' information in a hotel is none of these. It is discretion, practised by people, and what happens when it fails, in a house whose reputation rests on it, is the case that follows.**

Action plan for our property

Action	Owner	Due	How we will know it worked

Source: Francesco Dore, The Helm and the Lens, Volume 5a «The Helm», subchapter 1.14. Edizioni Effedore, 2026. Clause references are paraphrased; this sheet does not reproduce the text of ISO/IEC 27001. It is not legal advice: data protection and information security law is that of the place where the property operates.