WORKSHEET 2.14

The Alert Nobody Read

Subchapter 2.14 · case in the book: Kigali

Ask your IT provider to send a test alert from your security monitoring service, and see who receives it, and how long it takes them to call you. If nobody calls, your property is paying for a service that is watching carefully and telling nobody.

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
Follow every alert address and number to a person, and fix those that lead nowhere.		
Send alerts to roles: the provider's queue and a hotel recipient for serious alerts.		
Write triage rules for what needs action at once, by the morning and weekly.		
Tune the monitoring to the hotel's normal activity in the first month.		
Send a test alert every month and confirm it was received.		
Put the provider's monitoring duties, hours and response times into the contract.		
Add the transfer of duties, including alert receipt, to the leaving process.		
Keep evidence of the review of alerts for the internal and external audit.		

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
«We have a monitoring service, so we are monitored.»	A tool produces alerts. Monitoring requires somebody to read them and act, and the standard asks who that is.	
«The provider watches the alerts.»	Only if the contract says so, with hours and response times. Otherwise each side may assume the other is watching.	
«Alerts go to the IT manager.»	Alerts should go to a role. A person leaves, goes on holiday and sleeps.	

What is commonly believed	What actually holds	Our position
«If the service were broken, we would know.»	A broken alert path is silent. Only a regular test shows it is working.	
«More alerts means better monitoring.»	Untuned alerts bury the ones that matter. Monitoring must be tuned to the hotel's normal activity.	

Common mistakes: a self-check

Mistake (from the book)	Present here?	Action / owner
Buying a monitoring tool and assuming the monitoring is done.		
Sending alerts to one person, or to an address that forwards to one person.		
Never testing whether alerts arrive.		
Receiving hundreds of untuned alerts a week, and so reading none.		
Leaving unclear whether the provider or the hotel reads the alerts.		
Closing a leaver's accounts without transferring their duties.		
Being unable to show the auditor any review of alerts.		

Operative synthesis

- **Monitoring is somebody reading an alert, deciding what it means and acting in time. A tool, however clever, only produces the alerts. The hotel decides who reads each kind, how quickly and what they do, sends alerts to roles rather than people, tunes the tool to its normal activity, puts the provider's part into the contract and tests the path every month.**
- **The instrument is a page that says, for each kind of alert, who receives it, within what time and what they do, including the monthly test. Agreed between the hotel and its provider, it ensures that no alert lands in a closed mailbox and that the ones that matter wake somebody who can act.**
- **In Kigali nothing had been done carelessly. An IT manager set up a good monitoring service correctly, a provider delivered its alerts faithfully, and the leaving process closed a departing manager's mailbox as it should. The alerts described the attack as it happened, for four months, to an address that forwarded to nowhere.**
- **Which raises the question the next subchapter takes up, the last of this volume. Every case in it ended with something the hotel could change so that it would not happen again. What happens when the same finding is closed three times in three years, each time with a memo, and comes back each time, is the case that follows.**

Action plan for our property

Action	Owner	Due	How we will know it worked

Action	Owner	Due	How we will know it worked

Source: Francesco Dore, The Helm and the Lens, Volume 5a «The Helm», subchapter 2.14. 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.