WORKSHEET 1.10

Objectives That Predict Rather Than Count

Subchapter 1.10 · case in the book: Toronto

Look at the information security figures in the last report your owners received. For each, ask whether it could have warned you of your next incident before it happened. If every figure describes what went well, the report is measuring luck.

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
Derive each objective from a risk and its treatment.		
Retire figures that could not show the system failing.		
Count, once, the accounts of leavers, administrator accounts without a second factor and overdue updates.		
Set targets that can be reached and a plan with owner and date for each one not yet met.		
Name the person who analyses the figures and have them write a paragraph each quarter.		
Put fewer, predictive figures in the owner's report, with trend and interpretation.		
Treat a rising number of reported near misses as a healthy sign in the first year.		
Review the objectives at least annually and whenever the hotel changes significantly.		

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
«Zero incidents is the right objective.»	It rewards not reporting. The standard asks for objectives that take the risk assessment into account and show whether treatments work.	
«Blocked attacks show that the defences work.»	They show the volume of automated attacks on the internet, which would be similar whatever the hotel's controls.	
«Everybody trained means the risk is reduced.»	Completion is an activity. Whether behaviour changed has to be measured separately.	

What is commonly believed	What actually holds	Our position
«Objectives must all be green to satisfy the auditor.»	The standard asks for objectives to be monitored and evaluated. A red objective with a plan is evidence of a working system.	
«The IT provider's report is the monitoring.»	The organisation must decide what is monitored, and who analyses and evaluates the results. Collecting numbers is not analysing them.	

Common mistakes: a self-check

Mistake (from the book)	Present here?	Action / owner
Setting zero incidents as the objective.		
Reporting blocked attacks as evidence of effective defence.		
Presenting training completion as a reduction in risk.		
Choosing objectives that are easy to report instead of objectives tied to the risks.		
Collecting figures without anybody analysing them.		
Avoiding indicators that would start amber or red.		
Keeping the same objectives for years while the hotel changes.		

Operative synthesis

- **A security objective is useful when it predicts: when it measures a condition that deteriorates before an incident happens and that a decision can change. Objectives of that kind come from the risk assessment, start uncomfortably, and tell the owner something. Objectives chosen because they are easy to report (zero incidents, blocked attacks, courses completed) tell the owner that things are fine until they are not.**
- **The instrument is a page of eight to twelve indicators, each tied to a risk and its treatment, with a target, an owner, a trend and a quarterly paragraph explaining what moved and why. Placed in the owner's report, it replaces reassurance with information.**
- **In Toronto nothing had been reported falsely. Every figure on the green page was true, collected carefully by a competent provider and presented honestly by a capable general manager. None of them could have shown that forty-one people who no longer worked at the hotel could still log in, and the one figure that would have shown it was never counted because it would have been red.**
- **Which raises the question the next subchapter takes up. Indicators that start red require resources to turn green, and resources are decided in the budget. What happens when an owner, faced with the cost of the controls, buys an insurance policy instead, and the policy turns out to depend on the controls he did not buy, 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 1.10. 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.