WORKSHEET 1.11

The Insurance You Bought Instead of the Control

Subchapter 1.11 · case in the book: Sydney

Find the proposal form your property completed for its cyber insurance and read the questions about the controls in place. For each answer, ask who checked it before it was signed. If nobody did, the policy you are paying for may depend on defences you do not have.

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
Ask the IT provider to break any security proposal into elements, each with cost, risk and insurer relevance.		
Estimate, roughly, the cost of the three or four most serious risks, and set it beside the cost of the controls.		
Read the policy's sub-limits, waiting periods, exclusions and conditions before buying it.		
Answer every control question in the proposal from the Statement of Applicability, and give the true answer where it is no.		
Add the insurer and its conditions to the register of interested-party requirements.		
Treat risks in order: cheap effective controls, further controls, insurance, then signed retention.		
Review controls, declarations and cover together before every renewal.		
Keep insurance, on honest terms, as part of treatment rather than as its replacement.		

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
«Insurance treats the risk.»	It shares some of the financial consequences. The event, the disruption and the harm to guests remain the hotel's.	
«The cover limit is what the policy will pay.»	Sub-limits, waiting periods, exclusions and conditions decide what it will pay. The limit is only the ceiling.	

What is commonly believed	What actually holds	Our position
«The proposal form is paperwork for the broker.»	Its answers are the basis on which the insurer accepts the risk. An incorrect answer can reduce or defeat a claim.	
«Security spending is an IT line in the budget.»	Resources for the system are a management decision, and the standard requires top management to ensure they are available.	
«If we cut the package by half, we get half the protection.»	Protection depends on which elements are kept. The cheapest element can be the one that matters most.	

Common mistakes: a self-check

Mistake (from the book)	Present here?	Action / owner
Comparing a security package with an insurance premium on price alone.		
Treating insurance as a control rather than as a way of sharing part of the consequences.		
Completing the proposal form from last year's answers without checking them.		
Buying a policy without reading its sub-limits, waiting periods and conditions.		
Cutting a package by amount without knowing which element mattered most.		
Leaving the insurer out of the register of interested-party requirements.		
Deciding security resources without any estimate of what the risk would cost.		

Operative synthesis

- **Insurance and controls are not alternatives. Controls reduce the chance and the damage of an event; insurance shares part of its financial consequences, on conditions that increasingly include the very controls it might be thought to replace. The order that works is controls first, especially the cheap ones insurers ask about, then insurance on terms the hotel has read, then knowing acceptance of what remains.**
- **The instrument is a page that sets out, for each significant risk, the controls bought and their cost, what the insurance covers and requires, and what the hotel keeps. Together with a security budget broken into elements and a proposal form checked against the Statement of Applicability, it turns a twenty-minute budget decision into a deliberate choice of treatment.**
- **In Sydney nothing had been done recklessly. The owner compared two proposals carefully, the broker offered a competitive policy, the general manager answered a form as best she could, and the IT provider spent the budget it was given on the most visible control. The decision that mattered was which element to defer, and it was taken by amount, in a meeting where nobody had separated the element that would have stopped the attack from the ones that would not.**

› **Which raises the question the next subchapter takes up. The remote access tool that let the attacker in belonged to a supplier, and suppliers hold keys to most of the systems a hotel depends on. What happens when one of them has permanent access to a hotel's lock server and its contract says nothing about how quickly it will tell the hotel if something goes wrong, 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 1.11. 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.