WORKSHEET 1.8

# Risk Assessment, and the Risk Nobody Owned

*Subchapter 1.8 · case in the book: Istanbul*

Open your risk register and count how many risks have the same owner. Then pick the risk with the highest score and ask its owner whether they have the authority to change the activity it describes. If the answer is no, the register is a list, and the risks on it have been accepted by 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 |
|---|---|---|
| Rebuild the register from the hotel's activities and the information each depends on. | | |
| Write each risk as a scenario: who, through what, with what consequence for the hotel and its guests. | | |
| Assign each risk to the manager who can change the activity concerned. | | |
| Write acceptance criteria in terms of guests harmed, revenue lost and days disrupted. | | |
| Prefer controls that do not depend on everybody being careful all the time. | | |
| Have each owner approve the treatment and sign for the residual risk. | | |
| Make every change to an activity's use of information prompt its owner to review their page. | | |
| Give the owner of the property a one-page summary of the ten risks that matter most. | | |

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 risk owner is the person who maintains the register.» | The risk owner is the person with the accountability and authority to manage the risk, which means authority over the activity that creates it. | |
| «A complete register lists every threat in the catalogue.» | The standard requires the risks that matter to be identified and treated. A catalogue is a method, and often one that hides the specific in the general. | |

| What is commonly believed | What actually holds | Our position |
|---|---|---|
| «The score decides what is acceptable.» | The organisation's acceptance criteria decide, and an owner must accept what remains. A score is only as good as the judgement behind it. | |
| «Awareness training treats people-related risks.» | Training helps. Against well-made phishing, controls such as a second factor and named accounts do more, and they are usually decisions of the business, not of IT. | |
| «The assessment is done every year.» | It must also be done when significant changes occur, and the people making those changes must know that. | |

## Common mistakes: a self-check

| Mistake (from the book) | Present here? | Action / owner |
|---|---|---|
| Building the register from a threat catalogue instead of from the hotel's activities. | | |
| Assigning every risk to IT. | | |
| Writing threats instead of scenarios. | | |
| Letting a scoring threshold decide what nobody has looked at. | | |
| Treating every people-related risk with annual training. | | |
| Having the treatment plan approved by the department that wrote it, not by the owners. | | |
| Changing how an activity uses information without reviewing its risks. | | |

## Operative synthesis

- **A risk assessment is complete when the risks that matter have been identified in the hotel's own terms and each has been seen, treated and accepted by somebody with authority over the activity that creates it. A register that lists every threat and assigns every risk to IT can be complete in form and empty in effect, because the decisions it requires are never taken by anybody who can take them.**
- **The instrument is a page per owner: the scenarios that belong to their activity, the decision taken on each, the main controls, and their signature on what remains. Above those pages, a summary for the owner of the property shows the ten risks that matter most and who decided what about each.**
- **In Istanbul nothing had been done carelessly. A consultant ran a thorough workshop, an IT manager maintained a well-kept register, a reservations agent responded to what looked like a routine request, and a revenue manager ran a distribution strategy that brought in almost half the hotel's business. The risk that joined their work together was on the register, correctly scored, and owned by the one person who could not change it.**
- **Which raises the question the next subchapter takes up. Once risks have owners and treatments, the hotel has to record which of the standard's reference controls it uses and why**

**it does not use the others. What happens when that record, the Statement of Applicability, is copied from a template and declares a control unnecessary in a hotel that plainly needs 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 1.8. 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.