WORKSHEET 1.9

# The Statement of Applicability: Ninety-Three Reasons

*Subchapter 1.9 · case in the book: Warsaw*

Ask for your property's Statement of Applicability and read only the reasons given for the controls it excludes. If any of them could not have been written by somebody who has walked through your hotel, the document your owner signed describes some other business.

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 statement from the hotel's risk pages, not from a template. | | |
| Go through every reference control with somebody who knows the hotel, and record a reason for each decision. | | |
| Write every exclusion in a sentence that could only describe this hotel. | | |
| Mark implementation as yes, partly or planned with a date, and note the evidence for each yes. | | |
| Declare and manage the good practices the hotel already has as controls. | | |
| Give every control an owner who answers for whether it operates. | | |
| Reopen the statement whenever a new system, supplier or process changes what is needed. | | |
| Have the owner read the exclusions and open items and sign the statement knowingly. | | |

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 |
|---|---|---|
| «All ninety-three controls are mandatory.» | None of them is mandatory individually. Each must be considered, and excluded only with a genuine reason. | |
| «The Statement of Applicability is a technical annex.» | It is the organisation's record of how it has chosen to protect its information, and it is read by auditors, clients and insurers. | |
| «Not applicable is a sufficient justification.» | The standard asks for the reason. A reason must describe the hotel, not another business. | |

| What is commonly believed | What actually holds | Our position |
|---|---|---|
| «A control is implemented when a template or procedure exists.» | It is implemented when it operates. Where it does not yet, the statement should say so. | |
| «The statement is fixed at certification.» | It must reflect the controls currently necessary, and changes to systems, suppliers or processes change them. | |

## Common mistakes: a self-check

| Mistake (from the book) | Present here? | Action / owner |
|---|---|---|
| Adapting a Statement of Applicability from another organisation. | | |
| Justifying exclusions with «not applicable» or with reasons that describe another business. | | |
| Treating the reference list as a checklist rather than as a check on the hotel's own controls. | | |
| Declaring controls implemented because a template or procedure exists. | | |
| Leaving good practices undeclared, and therefore unmanaged. | | |
| Failing to update the statement when systems, suppliers or processes change. | | |
| Signing the statement without reading it. | | |

## Operative synthesis

- **The Statement of Applicability is the hotel's written declaration of how it protects its information: ninety-three decisions about the standard's reference controls, each with a reason, plus any controls of its own, each with an honest statement of whether it operates. It is read by auditors, clients and insurers, and it is persuasive only if it is recognisably the hotel's own.**
- **The instrument is the statement itself, rebuilt from the hotel's risks, with reasons in the hotel's terms, honest implementation status, an owner for each control and the owner's signature. Built that way, it becomes the most useful single document in the system, because it shows in one place what the hotel does, what it does not do, and why.**
- **In Warsaw nothing had been done in bad faith. A consultant reused a sound document from another client, a coordinator maintained it faithfully, a chief executive signed what she was told was a technical annex, and the hotel's staff protected guests' information in ways the document never mentioned. The statement described a warehouse for three years because nobody who knew the hotel had been asked to read it.**
- **Which raises the question the next subchapter takes up. Once the hotel has decided how it will protect its information, it needs to know whether the protection is working. What happens when the measure chosen is zero incidents, and the hotel counts the attacks its firewall blocks instead of the things that predict the next breach, 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 1.9. 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.