WORKSHEET 1.2

The Context, and the Server Room Below Sea Level

Subchapter 1.2 · case in the book: New Orleans

Name the room in your building where the equipment that runs your front desk is kept. Say which floor it is on, whether it is on the emergency generator, and what cools it when the power fails. If you have to ask somebody, the context of your information security system has not yet been written.

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
Rewrite the context in the hotel's own terms: this building, this city, these dependencies.		
Walk the building with the chief engineer and the IT provider together, room by room.		
Check which circuit feeds each equipment room, and whether its cooling is on the generator.		
Answer the climate question with named events, not with a category.		
List where each hosted system keeps its data, and which laws travel with the hotel's guests.		
Configure and test the backup line, the offline arrival list and the manual procedures four times a year.		
Put the capital decisions the context produces in front of the owner, as trading continuity.		
Review the context after every storm, new supplier or new market.		

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 context analysis is a PESTLE document.»	No method is required. What is required is that the issues affecting the outcomes of the system are known, and a generic threat list does not identify them.	
«Climate change belongs to the environmental standard.»	Since 2024 the organisation must determine whether climate change is relevant to its information security system. For many hotels it is, through availability.	

What is commonly believed	What actually holds	Our position
«Our system is in the cloud, so availability is the provider's problem.»	The provider's availability ends at the hotel's line, router, switch, power and desk. That part is the hotel's.	
«The generator covers the building.»	Generators are sized and wired for what somebody decided when they were installed. Whether the network and its cooling are on it is a question to check, not to assume.	
«Our legal context is the law of our country.»	The law that reaches a hotel's data follows the guests, the location of the servers and the contracts the hotel has signed.	

Common mistakes: a self-check

Mistake (from the book)	Present here?	Action / owner
Writing the context as a list of threats that would be true of any business.		
Leaving the building, the climate and the utilities out of an information security system.		
Thinking of confidentiality and forgetting availability.		
Assuming that a hosted system cannot fail because the provider's data centre does not.		
Answering the climate question with «not applicable» without looking at the city.		
Buying the fallback equipment and never configuring or testing it.		
Naming only the law of the hotel's own country as its legal context.		

Operative synthesis

- **The context is the part of the information security system that decides what the rest of it can see. Written generically, it produces a generic assessment and leaves the hotel's real exposure outside. Written in the hotel's own terms, it names the building, the city, the season, the dependencies and the laws that reach the data, and it points the risk assessment at the conditions most likely to stop the hotel handling information.**
- **The instrument is a page and a map. The page names what could stop this hotel; the map shows what each essential activity depends on, where that dependency sits, what happens when it fails and who decides what to do. Together they turn the climate question from a formality into a list of events, and the cloud from an assumption into a line, a router and a room.**
- **In New Orleans nothing had been done badly. The storm plan was good, the information security system was in order, the hosted system never went down and the staff kept the hotel open through a hard week. What had never happened was the conversation between the people who knew the building and the people who knew the systems, and the room where their two responsibilities met was on the ground floor, on the wrong circuit, in a city below the river.**

› **Which raises the question the next subchapter takes up. Among the conditions a hotel does not choose are the people and organisations that take an interest in how it handles information, from the guest to the regulator to the corporate client with a security questionnaire of a hundred and forty questions. Who they are, what they actually require, and what happens when a hotel answers yes to everything, 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 1.2. 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.