WORKSHEET 2.4

Connected Rooms and the Devices Nobody Counted

Subchapter 2.4 · case in the book: Tokyo

Ask your IT provider how many devices are connected to your property's network, and then ask your chief engineer the same question. If the two numbers are different, the difference is made up of computers that nobody manages, and some of them are in the guest rooms.

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
Scan the network and walk the building to count every connected device type.		
Divide the network into zones for guest rooms, building systems, staff and core systems.		
Change every default credential and record a standard configuration for each device type.		
Find out how long each device type will receive updates, and plan replacement or isolation.		
Put update periods, credentials, network separation and guest data into every procurement contract.		
Reset guests' accounts and data on connected devices at every departure.		
Give connected devices an owner, usually engineering with IT.		
Bring the register into the inventory, the risk pages and the Statement of Applicability.		

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 inventory lists our computers.»	It must list information and the assets associated with it. Tablets, televisions, thermostats, sensors and locks are among them.	
«In-room technology is an engineering matter.»	It is a set of computers on the hotel's network, and it must be managed as such.	
«One network is simpler to run.»	It is, and it lets any device reach any other. The standard asks for segregation.	

What is commonly believed	What actually holds	Our position
«Devices come secure from the factory.»	Many come with published default passwords and a limited period of updates.	
«Housekeeping prepares the room.»	It prepares the room physically. Guests' accounts and data on connected devices need resetting too.	

Common mistakes: a self-check

Mistake (from the book)	Present here?	Action / owner
Keeping an inventory that lists only devices that look like computers.		
Putting guest-room devices on the same network as the property system.		
Leaving default passwords on devices because the installer's contract did not mention them.		
Keeping devices in service after their supplier stops providing security updates.		
Buying connected devices without asking how long they will be supported.		
Leaving guests' accounts and histories on devices for the next guest.		
Letting engineering, IT, the integrator and the rooms division each own a part and nobody the whole.		

Operative synthesis

- **A connected hotel is full of computers that do not look like computers, in rooms used by a different stranger every night. They are bought by engineering and the rooms division, installed by contractors and forgotten by the inventory, and unless they are counted, separated from the systems that hold guests' data, configured properly and kept supported, they are the easiest way into the rest of the hotel.**
- **The instrument is a register of connected device types, with count, owner, network zone, how long each will be supported, the plan for the end, and what guest data each keeps and how it is reset. Owned by engineering with IT and reviewed twice a year, it turns the hotel's technology from an unmanaged collection of equipment into a managed part of the system.**
- **In Tokyo nothing had been bought carelessly. The developer chose excellent technology, the integrator installed it well, engineering maintained it, and guests loved it. The inventory counted sixty-two devices because it had been drawn up by the people who knew what a computer looked like, and most of the other one thousand one hundred and forty-four were in the rooms.**
- **Which raises the question the next subchapter takes up. Some of the most important devices in a hotel are not the hotel's at all. They are the phones in its staff's pockets, and the messaging groups on them through which, in many hotels, the day's work is organised. What happens when the group that runs the hotel carries guests' names, room numbers and photographs of their passports, 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 2.4. 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.