WORKSHEET 2.6

The Vendor Who Logs In at Night

Subchapter 2.6 · case in the book: Bangkok

Ask your night auditor what he would do if the cursor on his screen started moving by itself at three in the morning. Then ask your IT manager how many suppliers can make it move. If the first answer is a shrug and the second is a guess, your building has doors that open from outside and nobody on duty who knows who holds the keys.

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
Find every remote support tool on the hotel's computers and every route suppliers use.		
Set up one remote route controlled by the hotel, with named accounts and a second factor.		
Remove suppliers' own remote tools once each has moved to the hotel's route.		
Allow sessions on request, for a stated purpose and period, with a notice for any at night.		
Record every session and read the records every week.		
Agree planned supplier work in advance, including time, scope and rollback.		
Give night staff a paragraph on what to do when a screen moves by itself.		
Review supplier accounts and access every quarter.		

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
«Each supplier needs its own remote tool.»	Each needs a way in. It can be the hotel's route, with the supplier's named account, rather than six separate tools.	
«Unattended access is necessary for support in other time zones.»	Access at unusual hours can be agreed in advance and recorded. It does not require a door that opens without anybody knowing.	
«The supplier's remote access is the supplier's responsibility.»	The hotel must manage privileged access to its systems and monitor its suppliers' service, whoever holds the tool.	

What is commonly believed	What actually holds	Our position
«If the supplier is working, it is fine.»	A supplier's change to a live system at night is a change to the hotel's system, and it needs the hotel's agreement.	
«Night staff cannot be expected to deal with IT.»	Night staff are the most likely to see remote access happen, and a paragraph of instruction is enough.	

Common mistakes: a self-check

Mistake (from the book)	Present here?	Action / owner
Letting each supplier install its own remote tool.		
Allowing unattended access so that suppliers can connect whenever they like.		
Leaving remote access passwords unchanged since installation.		
Not knowing when suppliers connect, or to what.		
Keeping no records of remote sessions, or never reading them.		
Allowing suppliers to change live systems at night without agreement.		
Leaving night staff without instructions for what to do when a screen is taken over.		

Operative synthesis

- **Every supplier that supports a hotel's systems needs a way in, and left to themselves suppliers each build their own, open it when it suits them and share the keys among their own staff. The management of the hotel replaces those doors with one it controls: named accounts, a second factor, sessions opened on request, every session recorded and read, and planned work agreed in advance.**
- **The instrument is a page that sets out, from the creation of a supplier's account to the weekly reading of records, what happens at each stage and who is responsible, including what the night auditor does when the cursor moves by itself. With one remote route and a quarterly review, it gives the hotel a door with a doorman.**
- **In Bangkok nothing had been done carelessly. Each supplier installed the tool it used for all its customers, the IT manager accepted what each needed to support its system, and a supplier's engineer scheduled maintenance for a quiet hour. The hotel had six doors, four of them always open, and the only person who noticed one being used was a night auditor who did the right thing by instinct.**
- **Which raises the question the next subchapter takes up. Remote access is one of the commonest ways for ransomware to enter a hotel, and ransomware usually arrives at night. What happens when it does, at two in the morning on a Saturday, in a hotel that stopped printing its arrival list to save paper, 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 2.6. 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.