WORKSHEET 2.3

The Card Number That Should Not Be in the Building

Subchapter 2.3 · case in the book: Miami

Search the mailboxes of your reservations, sales and events teams for the word «security code». Then look in the drawers at the reservations desk for any form with a card number written on it. Every result is a card number your property holds without needing to, and each of them brings every system and person it touches into the card industry's rules.

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
Draw the journey of card data through every channel, with finance, reservations, sales and IT together.		
Replace card authorisation forms and emailed deposits with secure payment links.		
Enter telephone guarantees directly into tokenised fields, and never write card details down.		
Never record the security code after authorisation, in any form.		
Search and clean every mailbox and drawer that holds card numbers, and record the deletion.		
Delete card details received by email and reply with a payment link.		
Redo the card industry self-assessment on the basis of the real journey.		
Check every quarter that the closed doors have stayed closed.		

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
«Our terminals are secure, so our card data is secure.»	Card data also enters through the telephone, email, forms and paper. Each channel is in scope if it handles card data.	
«We need the security code to guarantee a booking.»	The card industry's rules forbid storing it after authorisation in any form. A guarantee does not require it to be written down.	

What is commonly believed	What actually holds	Our position
«The authorisation form is the only way to bill a company.»	Payment providers offer secure payment links that take the card details directly, without the hotel seeing them.	
«The annual self-assessment shows we comply.»	It is accurate only if it is based on a complete picture of how card data enters and moves through the hotel.	
«Encrypting stored card numbers solves the problem.»	Not storing them solves it better, and removes the systems that held them from the scope of the assessment.	

Common mistakes: a self-check

Mistake (from the book)	Present here?	Action / owner
Securing the terminals and forgetting the telephone, email, forms and paper.		
Recording security codes on guarantee sheets or authorisation forms.		
Sending card authorisation forms by email to corporate clients.		
Letting mailboxes become archives of card numbers.		
Completing the card industry self-assessment without a picture of every channel.		
Leaving tokenisation and payment links unused although they are in the contract.		
Letting each department manage its own channel with nobody owning the whole journey.		

Operative synthesis

- **The cheapest way to protect a card number is not to have it. A hotel can take cards through encrypting terminals, tokenised systems and payment links that keep the number out of its hands altogether, and every channel it moves in that direction removes a category of risk and a portion of the card industry's assessment at the same time.**
- **The instrument is a page that draws the journey of card data through every channel, where it used to stay, and what replaces it, with an owner for each. Checked every quarter, it keeps closed the doors that habit and pressure tend to reopen.**
- **In Miami nothing had been done out of ignorance. The finance director had secured the terminals carefully and completed an honest assessment of the channels she knew about, reservations took guarantees the way reservations always had, and the sales team used the form so many hotels used. The card numbers were exposed in the channels nobody had drawn, and the security codes had been kept by a hotel that had never needed them.**
- **Which raises the question the next subchapter takes up. Card terminals are only some of the devices connected to a hotel's network. What happens when a hotel lists some sixty connected devices in its inventory and finds, on inspection, more than twelve hundred, from**

thermostats and televisions to door locks, all sharing the network with the property system, 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 2.3. 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.