THE HELM AND THE LENS · VOLUME 5a

The Thirty Concept Cards

The Helm · ISO/IEC 27001

Each subchapter of the volume ends with a concept card that gathers its subject into a single image. All thirty are collected here with title, image and text.

Francesco Dore · Edizioni Effedore

CONCEPT CARD 1.1

The Asset That Is Not on the Balance Sheet

Subchapter 1.1 · Lisbon



A small panelled office in a heritage hotel, a wall of blue-and-white tiles behind, a closed wooden door with a brass handle. The managing director sits at a polished table with one hand over her mouth, looking at a laptop. The buyer's adviser leans in beside her and points at the screen. Between them on the table lie a closed leather folder, a room key on a heavy brass fob and two cups of coffee that nobody is drinking.

The card is about the moment an owner discovers what the business has been keeping. The screen is turned towards the two of them and away from us, and that is the right way to see it: what is on it is known only to the people in the room, and it has taken a stranger's question to make them look. In the case it was a folder of scanned identity documents, accumulated for a decade without anybody deciding to keep them. The key on the table is the other half of the hotel's information: the part the house is proud of, the welcome, the history, the guest who returns.

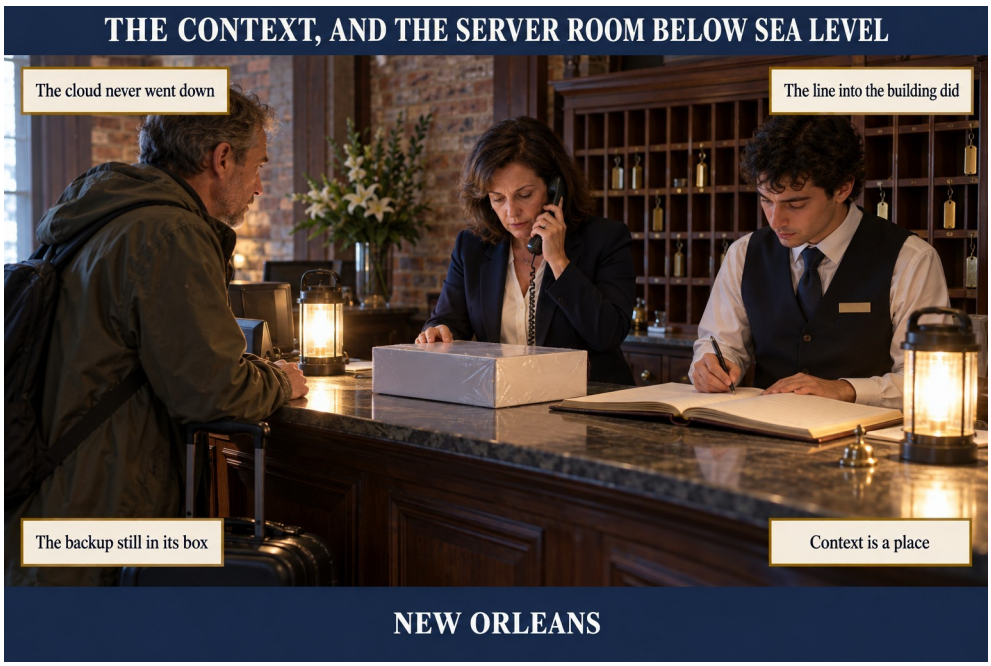
The plaques set the two values of information against each other. Worth to the business, and weight of the exposure: the same records are both, and an owner has to know both. The lower pair names how the weight arrived. Kept by default; nobody decided to keep it. Nothing on that screen was put there by a decision, and nothing will leave it until somebody takes one.

The plate is not saying that the managing director was careless. She ran a well-kept house for years and answered every question a buyer asked, until the one about personal data. It is saying that information held without a decision is carried as an exposure whether or not anybody knows it is there, and that the first act of ownership is to find out what the house holds, before somebody else asks.

CONCEPT CARD 1.2

The Context, and the Server Room Below Sea Level

Subchapter 1.2 · New Orleans



The front desk of a hotel in a converted brick warehouse, lit only by two battery lanterns and grey daylight. The general manager holds a telephone that is doing nothing, one hand resting on a white box still sealed in clear plastic. Beside her a young receptionist writes in a large bound ledger. Across the counter a tired guest in a rain jacket waits with his suitcase. Behind the desk, the pigeonholes hold their brass key tags as they have for a century.

The card is about the difference between where a system runs and where a hotel can reach it from. The property system in the case was hosted far away and never stopped. What stopped was the line into the building, and the backup that would have replaced it is the box under her hand, bought for exactly this night and never unwrapped. The ledger is the hotel's real continuity plan, improvised by the people who remembered how.

The plaques follow the chain of dependencies from the far end to the near one. The cloud never went down; the line into the building did. The backup still in its box is the conclusion nobody had written down, and the last plaque names the lesson in four words. Context is a place: the room where the equipment sits, the street outside, the height of the water, and every link between the hotel and the systems it thinks of as elsewhere.

The plate is not saying that the manager was unprepared. The windows were boarded, the generator was fuelled and the hotel stayed open through the storm. It is saying that a context written as a list of general threats misses the one that matters, and that the question a hotel should ask of every system is not whether it can fail, but what the house needs in order to reach it.

CONCEPT CARD 1.3

Who Has an Interest in Your Guests' Data

Subchapter 1.3 · Dublin



A sales office in a modern city hotel, a glass wall on the right giving onto a carpeted corridor of guest rooms. The director of sales sits at her desk, pen in hand, smiling with the satisfaction of a finished task. In front of her is a tall stack of pages, every one of them ticked in the same column. The systems coordinator stands beside the desk holding one page from the stack and looks at her with quiet alarm.

The card is about how requirements actually reach a hotel. They do not arrive through the information security system; they arrive through a client's renewal, as a questionnaire, in the inbox of whoever manages the account. Here that person has done what such forms invite: answered yes, line after line, to keep the business. The stack is the hotel's promise to a client, and the man holding one page of it is the first person who has read it as a promise.

The plaques move from the act to its consequence. Answered yes to everything; requirements arrive by contract. Nobody asked the system, which is why the answers describe the hotel the director believed in rather than the one that exists. A promise in writing is the last plaque, and it is the one that matters, because a signed questionnaire becomes part of what the client is entitled to rely on.

The plate is not saying that the director of sales lied. She answered a form the way forms are usually answered, under pressure, about matters outside her job. It is saying that a hotel must know who has an interest in its guests' information and what it has promised them, and that the only reliable way to know is to route every such promise through somebody who can check it.

CONCEPT CARD 1.4

Leadership, and Why Security Is Not the IT Department's Job

Subchapter 1.4 · Prague



A marble front desk in the foreground, a glass-walled office behind it. At the desk three receptionists work at a single computer: one types, a second reaches across to the same keyboard, the third waits with a card in her hand. There is one screen and one keyboard for all three. Behind the glass the owner and his finance manager shake hands over a closed budget binder, pleased with the meeting.

The card sets cause and effect in the same frame. The handshake behind the glass is a saving: fewer named licences for the property system, agreed in a budget meeting as a line of cost. The consequence is at the desk, where three people share one login and every refund, adjustment and change is now made by nobody in particular. Nobody at the desk chose that, and nobody behind the glass knew they had.

The plaques read as a sentence across the frame. Saved in a budget meeting; every action anonymous. A cost that was a decision is the pivot of the subchapter, and the last plaque draws the conclusion that gives it its title. Security is decided upstairs, in the room with the binder, long before anybody at the desk logs in.

The plate is not saying that the owner was reckless or the receptionists careless. The owner applied to licences the same care he applied to every cost, and the staff work as fast as the desk requires. It is saying that the decisions that most affect a hotel's information are taken by management as decisions about money, staffing and suppliers, and that leadership means recognising them as security decisions when they are taken.

CONCEPT CARD 1.5

Scope, and the Boundary Drawn Around the Easy Part

Subchapter 1.5 · Dubai



A vast resort lobby of marble and tall columns. In one corner stands a small glass office with a desk and a computer, and around it, and only around it, a line of brass stanchions and red velvet rope. Inside the rope the director of communications holds a framed certificate against her chest and a telephone to her ear, her expression guarded. Outside it, at the long front desk, a receptionist checks in a couple with their luggage; beyond them, folded towels mark the entrance to the spa.

The card is about the difference between a true statement and an honest one. The certificate is real, and it covers exactly what the rope surrounds: the office of the IT department. The guests' information lives everywhere else in the picture, at the desk, in the spa, in the sales office out of frame, and all of it is outside the boundary. The call she is taking is from somebody who has read the scope on the public register.

The plaques say it in the order a guest would discover it. True and misleading; drawn around the easy part. The guest is outside it is placed, by chance, directly beneath the couple at the desk. A scope is a promise is the last word: whatever the hotel says about its certificate, the guest assumes the promise includes her.

The plate is not saying that the certificate was obtained dishonestly or that the director has done anything wrong. The scope was drawn where the system was ready, as first scopes often are. It is saying that the boundary of an information security system is the first decision about honesty an owner makes, and that it should follow the guest's information rather than the department that was easiest to certify.

CONCEPT CARD 1.6

The Law and the Standard: Two Registers for the Same Hotel

Subchapter 1.6 · Amsterdam



An upper-floor office in a canal-house hotel, dark beams, a steep wooden staircase visible through the open doorway. At the two ends of one long table a lawyer writes in a burgundy binder and the operations director types beside a green one. They do not look at each other. In the middle of the table, at equal distance from both, lies a single unopened envelope, and in front of it an empty chair.

The card is about two careful people describing the same hotel in two books. The burgundy binder is the record the law requires, kept by the data protection officer; the green one is the risk register the standard requires, kept by whoever runs the system. Both list the same guests, the same systems and the same suppliers, in different words, and neither has ever been compared with the other. The envelope is the request that will force the comparison. The empty chair is the place where one inventory would sit.

The plaques set out the argument of the subchapter. Same guests, two books. The law asks why: on what basis each item is held, for how long, with what rights. The standard asks how: with what protection, against which risks, owned by whom. One inventory, two readings is the answer, and it is the only one of the four that describes something the room does not yet contain.

The plate is not saying that either of them has done the job badly. Each register is thorough and each keeper is competent. It is saying that when the law and the standard are kept apart they drift apart, from each other and from the hotel, and that the cheapest way to satisfy both is to describe the processing once and read it twice.

CONCEPT CARD 1.7

A Policy That Staff Can Check

Subchapter 1.7 · Kyoto



The reception of a quiet traditional inn: pale wood, paper lanterns, a plain cloth curtain in the doorway behind. A receptionist in a dark kimono-style uniform holds the telephone to her ear and looks aside, uncertain what to say. On the counter in front of her lies a beautifully bound blue booklet with a gilded edge, closed. Beside it the reservations book is open, and a small brass bell waits for the next guest.

The card is about the distance between a policy and the moment it is needed. The booklet is the hotel's information security policy, elegant, approved and never opened at the desk. The telephone is a caller with a plausible story asking whether a guest is staying. Everything the receptionist might need is twenty centimetres from her hand, and none of it tells her what to do, because nothing in it is written as a sentence she could check against the call.

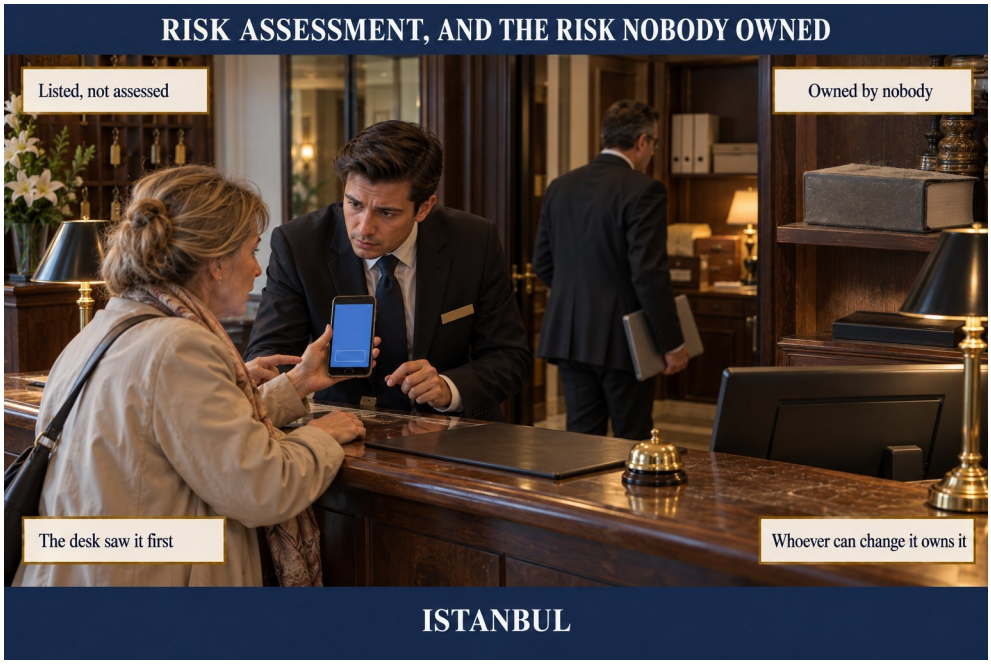
The plaques move from the document to the desk. Beautiful and unverifiable; decided at the telephone. The lower pair names what would have helped: rules staff can check, specific enough to apply in the middle of a call. Discretion needs sentences is the last plaque, and it belongs to this house in particular, whose whole reputation rests on staff who say nothing.

The plate is not saying that the receptionist was careless. She was good at her job and had once been reprimanded for being too cautious with a caller. It is saying that a policy protects guests only if it speaks in terms staff can apply at the counter, and that a hotel which wants discretion must write it down as things it does and does not do.

CONCEPT CARD 1.8

Risk Assessment, and the Risk Nobody Owned

Subchapter 1.8 · Istanbul



A front desk of dark wood and brass lamps. A worried guest shows the receptionist a phone screen: a plain blue page with a single empty button, the payment request she did not expect. He leans in, concerned. In the doorway behind the desk the IT manager walks away with a laptop under his arm. On a high shelf to the right, out of anybody's reach, lies a thick grey volume under a film of dust.

The card is about where a risk shows itself and where it is written down. The fraudulent messages reached guests through the booking platforms, and the first person to see them was the receptionist at the desk. The risk itself had been listed for years in the register on the high shelf, owned, like every other line in it, by the IT department, which could do nothing about a platform account managed by the revenue team. The man walking out of the frame is not avoiding the problem. He is simply not the person who could solve it.

The plaques trace the gap. Listed, not assessed; owned by nobody. The desk saw it first, which is almost always true in a hotel. The last plaque states the rule the subchapter is built on: whoever can change it owns it, and a risk is managed only when it reaches the person with authority over the activity that creates it.

The plate is not saying that the IT manager neglected his job or that the receptionist missed a warning. Both did what their roles allowed. It is saying that a register which assigns every risk to one department reaches nobody with the authority to act, and that a hotel whose risks reach nobody has accepted all of them by default.

CONCEPT CARD 1.9

The Statement of Applicability: Ninety-Three Reasons

Subchapter 1.9 · Warsaw



A panelled meeting room in a restored hotel, a closed door behind. The certification auditor reads a long printed table with her pen resting on one line halfway down the page. Across the table the systems coordinator watches her, hands clasped, uneasy. Between them stand a jug of water and two glasses; beside her lies a small stack of blank key cards. On the ceiling, in the centre of the room, a white dome camera looks down on them both.

The card is about the one document in the system that declares, control by control, how the hotel protects itself. The line under the auditor's pen says that monitoring the physical security of the premises does not apply. The camera above the table says otherwise. The statement was copied from a template written for another kind of organisation, and nobody in the hotel had read it with the building in mind until somebody from outside did.

The plaques describe what went wrong and what is required. Copied from a template; read line by line, as auditors read it and owners rarely do. A reason for every line is the discipline the standard asks for: each reference control included or excluded for a stated cause. The camera was there is the plaque the reader will remember, because the whole finding is visible in one glance at the ceiling.

The plate is not saying that the hotel was badly protected. In several respects it was better protected than its statement claimed. It is saying that the Statement of Applicability is the hotel's written declaration of its defences, and that a declaration nobody in the business has built, read and signed cannot be defended when it is read by somebody who knows the building.

CONCEPT CARD 1.10

Objectives That Predict Rather Than Count

Subchapter 1.10 · Toronto



A boardroom on the top floor of a city hotel, dark wood panelling, a coffee service on the table. The general manager leans over an open report and points to a page covered in a neat grid of solid green squares. The owners' asset manager sits beside her with a hand at his chin, looking at the page. On the facing page and on the table lie bar charts with no labels.

The card is about a report that is accurate in every figure and misleading as a whole. For three years the security page of the quarterly report had been entirely green, because it counted what went well: attacks blocked, systems available, courses completed. It did not count the accounts of people who had left, the administrator accounts without a second factor, or the staff who clicked on the test messages. The expression on the asset manager's face is the beginning of the right question.

The plaques set counting against predicting. Green for three years; counting what went well. Indicators that predict is the alternative the subchapter proposes: measures of conditions that make an incident more likely, so that the hotel can act before it happens. Bad news arrives late is what happens otherwise, from a client, a guest or a journalist.

The plate is not saying that the general manager hid anything. The figures on the green page were true, and she presented them in good faith. It is saying that what gets measured is what gets reported, and that an owner who sees only what goes well will learn about what goes badly when it is already expensive.

CONCEPT CARD 1.11

The Insurance You Bought Instead of the Control

Subchapter 1.11 · Sydney



The general manager's office in a harbour-side hotel. The owner, in shirt sleeves, stands holding a glossy navy folder with a round gold seal and offers it to the desk. The general manager sits with her hand at her chin and looks not at the folder but at the small sealed box on the desk between them, its plastic wrap intact. A telephone and a notepad complete the desk.

The card is about two purchases and the one that was made. The folder is the cyber insurance policy, bought at the renewal meeting. The box is the second factor for email and remote access that the IT provider had proposed at the same meeting and that was deferred to save money. The two look like alternatives on a budget sheet. They are not, because the policy was written on the assumption that the box had been opened, and the proposal form said so.

The plaques follow the decision to its end. Bought the promise; declared, not installed. Transfer is not reduction is the principle: insurance pays for some consequences of a risk and does nothing to make it less likely. Truth on the form is the last plaque, and in the case it decided the outcome, because the insurer paid only the costs the misstatement did not touch and declined the rest on the answer the hotel had given.

The plate is not saying that buying insurance was wrong. Insurance on honest terms, bought on top of the basic controls, is part of a sensible treatment. It is saying that a policy bought instead of a control is a promise conditional on a control the hotel does not have, and that the moment to discover this is the renewal meeting, not the claim.

CONCEPT CARD 1.12

The Suppliers Who Hold the Keys

Subchapter 1.12 · Tangier



A corridor of guest rooms in a restored palace hotel, carved doors, patterned tiles, warm lamps. In the foreground the general manager holds up a heavy iron ring of old brass keys, each with a blank cream tag, and studies them as if counting them for the first time. Behind her a technician from the lock company kneels at the electronic lock of a guest room door, his laptop open on the floor beside him.

The card sets the old idea of a key beside the new one. The ring in her hand is the hotel as it used to be: every door, every cupboard, held by the house. The technician is the hotel as it is: the lock server reachable from outside by the company that maintains it, with a login that in the case worked for every one of its clients. Every supplier who can reach the hotel's systems holds a key, and the ring of those keys has never been drawn up.

The plaques make the ring explicit. Every supplier holds a key; one login for every client. Nobody listed the keys, which is why the general manager learned of the compromise from a competitor at a dinner. Chosen at signature is the last plaque, because the moment the hotel has most influence over a supplier's security is the moment it chooses the supplier and signs the contract.

The plate is not saying that the lock company or the technician did anything improper. The technician is doing his job, and the supplier's contract said what engineering contracts usually say. It is saying that a hotel's security is largely the security of its suppliers, and that an owner should know who holds each key, what it opens, and what the supplier will do if it is stolen.

CONCEPT CARD 1.13

The Staffing Model Is a Security Decision

Subchapter 1.13 · Palma de Mallorca



The staff entrance of a resort in the week before opening: a service corridor, laundry trolleys, rails of pressed uniforms. At a table a woman from human resources hands a new employee an access card on a lanyard. On the tray in front of her lie many more, all identical. Two other seasonal staff wait beside her, cheerful, one already clipping her card on. Behind the table the owner's son stands with his arms folded and smiles at the efficiency of it all.

The card is about a model that works and a consequence nobody priced. The resort hires most of its summer staff in the week before it opens, which is good business. Every card on the tray was made from the same template, which gives every new person at the desk the same access to everything anybody at the desk might need, including the scans of guests' identity documents. The smile is the right expression for the model and the wrong one for what it has just decided.

The plaques describe the season from the inside. Hired the week before; copied from one template. Access set by payroll is the heart of it: the rights a seasonal employee receives are fixed by how and when the hotel hires, not by any decision about information. A security decision is the last plaque, and it names what the model has always been without being called so.

The plate is not saying that seasonal staff are a risk or that the owner's family should stop hiring them. Seasonal work is how resorts on the island run, and the people in the queue are the reason the hotel will open well. It is saying that how staff are hired, trained, given access and let go is decided by the owner, and that a staffing model is also a decision about who can reach the guests' information.

CONCEPT CARD 1.14

The Management Review That Hears Bad News

Subchapter 1.14 · Montreal



A boardroom in a converted stone warehouse, exposed walls, leather chairs. Four people sit around the table and bend over a binder held open by the representative of the IT provider: the chairman, the general manager, a younger colleague taking notes. In the foreground, on a small table by the half-open door, a large night log lies open, its page filled with handwriting, a fountain pen across it. Nobody at the table looks towards it.

The card shows the review and the report it did not receive. The binder at the table is the provider's account of the system, thorough and reassuring. The log by the door is the night manager's record of a caller who asked the night auditor to install a program and was refused, written in neat handwriting months before the same caller succeeded in the finance office. The warning existed. It was simply kept in a place the review was not built to hear from.

The plaques set the table against the door. All green at the table; the warning was in the log. Built to hear bad news is what the review should have been: an agenda that names in advance where bad news is recorded in a hotel and who will bring it. The night saw it first is the last plaque, and in a hotel it is nearly always true.

The plate is not saying that the people at the table were complacent or that the provider's report was false. The meeting was conducted properly and the report was accurate about what it covered. It is saying that a management review can decide only on what it hears, and that the people who first see something wrong in a hotel are rarely the ones invited to the table.

CONCEPT CARD 1.15

Discretion, the Oldest Control in the Building

Subchapter 1.15 · Monaco



The service pantry of a grand hotel: steel shelves, silver cloches, stacks of plates. A young waiter in a white jacket raises his phone to photograph a sheet taped to the shelf, the seating plan of a private dinner drawn as an oval with empty places. In the doorway behind him the chief concierge has just seen what he is doing and stops, his face grave.

The card is about information that never touches a system. The seating plan is the most sensitive document in the building that week: who is dining, and beside whom. It was printed so that the banqueting team could lay the table, and it leaves the building through the phone of a waiter supplied by an agency four days earlier. No firewall, register or certificate could have seen it. The only control in the frame is the man in the doorway, and he arrives one second late.

The plaques describe the oldest discipline in the trade. The oldest control in the building; paper, not systems. Four days in the house is the detail that decided the case: discretion is learned, and nobody had taught it to the newest people on the floor. Discretion can be taught is the last plaque and the argument of the subchapter, which is that the chief concierge's rules are not folklore but a control that can be written, trained and checked.

The plate is not saying that agency staff cannot be trusted, and it is not saying the concierge failed. It is saying that in a hotel the most sensitive information is who is present, with whom and when, that it travels by people and paper rather than by systems, and that a hotel which treats discretion as culture and leaves it out of its system is protecting its guests by habit alone.

CONCEPT CARD 2.1

Access Is Granted at Hiring and Forgotten at Leaving

Subchapter 2.1 · Athens



A back office in a city hotel: pigeonholes, a staff rota board, a trolley of files. The new general manager, in shirt sleeves, sits at a desk with a yellow highlighter, marking line after line on a long printed list that runs off the edge of the desk and onto the floor. Beside it lies a second list, much shorter. The IT coordinator leans over his shoulder with a laptop, a hand at her mouth.

The card is about two lists that should be the same length. The long one is every account on every system in the hotel; the short one is the payroll. The difference, marked in yellow, is people who have left, seasonal staff from summers ago, suppliers nobody can identify and one account shared at the front desk. It took a weekend of cancelled reservations, made from the account of a night auditor who had left eleven weeks before, for somebody to set the two side by side.

The plaques follow an account through its life. Granted at hiring; forgotten at leaving. More accounts than people is what the desk shows, and the last plaque states the rule that would have kept the lists the same length: access follows the person, through joining, moving and leaving, with a named person deciding at each step.

The plate is not saying that the coordinator neglected her work or that the previous management was careless. The lists grew as lists do in a hotel whose people change faster than its systems. It is saying that access which is not managed at the speed of people drifts away from the people the hotel actually employs, and that the first step is to count, once, what exists.

CONCEPT CARD 2.2

Identity Documents Over the Counter

Subchapter 2.2 · Valletta



The front desk of a baroque palazzo hotel at its busiest hour: carved stone arches, a long marble counter, luggage and a brass trolley. Two receptionists work quickly. Three guests stand at the counter, tired, bags in hand; one is handing over a document while a receptionist reaches for it. On the counter between them lie two identical dark red passports, side by side.

The card is about the moment a guest becomes data. The two passports on the counter belong to two women with the same surname and almost the same first name, and on this afternoon one of them left with the other's. Nobody at the desk made a mistake that could be called careless. The procedure worked for an ordinary afternoon and broke on the busiest one, which is exactly when an identity document is most likely to be separated from its owner.

The plaques describe the counter at that hour. The busiest hour; two identical covers. Look, record, hand back sums up the rule the subchapter proposes: the document is looked at, recorded as the law requires, and returned at once, without leaving the guest's hand for long. Where a guest becomes data is the last plaque, and it names the counter for what it is in an information security system.

The plate is not saying that the front desk was poorly run. It was one of the most admired on the island. It is saying that the handling of identity documents must be designed for the busiest hour of the week, because that is when it will be tested, and that a procedure which depends on calm will fail when the cruise passengers arrive.

CONCEPT CARD 2.3

The Card Number That Should Not Be in the Building

Subchapter 2.3 · Miami



A reservations office in a beach hotel. The finance director, in glasses, turns the pages of a thick folder of handwritten sheets. The forensic investigator beside her points to a line. In the foreground, clean and untouched, stands a modern card payment terminal with a blank screen, next to a telephone.

The card is about where the danger was and where everybody looked. The terminal is where the hotel had spent its money and its attention: devices that encrypt card data as it is read, checked every year. The folder is where the card numbers actually were: guarantee sheets filled in by hand when the system was slow, with the numbers and the security codes. The investigator found nothing wrong with the terminals, and then asked where else card numbers entered the building.

The plaques set the two against each other. The terminals were fine; the paper was not. Better not to have it is the principle of the subchapter: the cheapest and most effective protection for a card number is never to hold it. Fewer doors in is the practice that follows, taking card data through as few routes as possible and replacing it with a token wherever the hotel can.

The plate is not saying that the finance director was negligent. She completed the hotel's assessment carefully and replaced the terminals when she should. It is saying that every card number a hotel holds brings the people and systems that touch it under the card industry's rules, and that the question to ask is not whether the terminals are secure but where else card numbers come in.

CONCEPT CARD 2.4

Connected Rooms and the Devices Nobody Counted

Subchapter 2.4 · Tokyo



A modern hotel room, curtains closed. Across the whole bed, in rows, lie the connected devices removed from this one room: a bedside tablet, a speaker, a router, a small camera, a thermostat, sensors, hubs, a remote control, even the handle of the electronic lock, each with a blank white tag. The chief engineer, in overalls, shows the general manager a tablet; the general manager looks at the bed with his hand over his mouth.

The card is about counting. The hotel's inventory listed a few dozen devices for the whole building; the scan found more than a thousand, and this bed is what one room contributes. Each object looks like furniture or a gadget. Each of them is a computer with a network connection, bought by a department that did not think of it as one, and most of them were on the same network as the property system.

The plaques read as the result of the scan. Counted a few; found many more. Every device is a computer is the principle, and separate and support is what follows from it: count every device with a network address, separate them by trust, and keep them supported or replace them.

The plate is not saying that the hotel was wrong to sell itself on its technology, or that guests are better off with plastic key cards and a single remote control. Connected rooms are what many guests want, and they can be run safely. It is saying that a hotel must manage its devices as computers, and that the first step is to lay them out and count them.

CONCEPT CARD 2.5

The Messaging Group That Runs the Hotel

Subchapter 2.5 · Rio de Janeiro



A housekeeping office lined with shelves of folded linen. Five members of staff in hotel uniforms stand close together at a shift change, each looking at a personal phone full of message bubbles. At the centre a concierge holds his phone out to a colleague: on its screen is a photograph of a passport cover. In the doorway the general manager watches them all, a hand at his chin.

The card is about the real communication system of the hotel. There is a group for reception, one for housekeeping, one for maintenance and a large one for everybody, and through them pass shift changes, lost property, room numbers, guests' names and, on this morning, a photograph of an identity document sent by a guest's assistant so that the arrival could be prepared. None of it is on a system the hotel owns. All of it works, which is why everybody uses it.

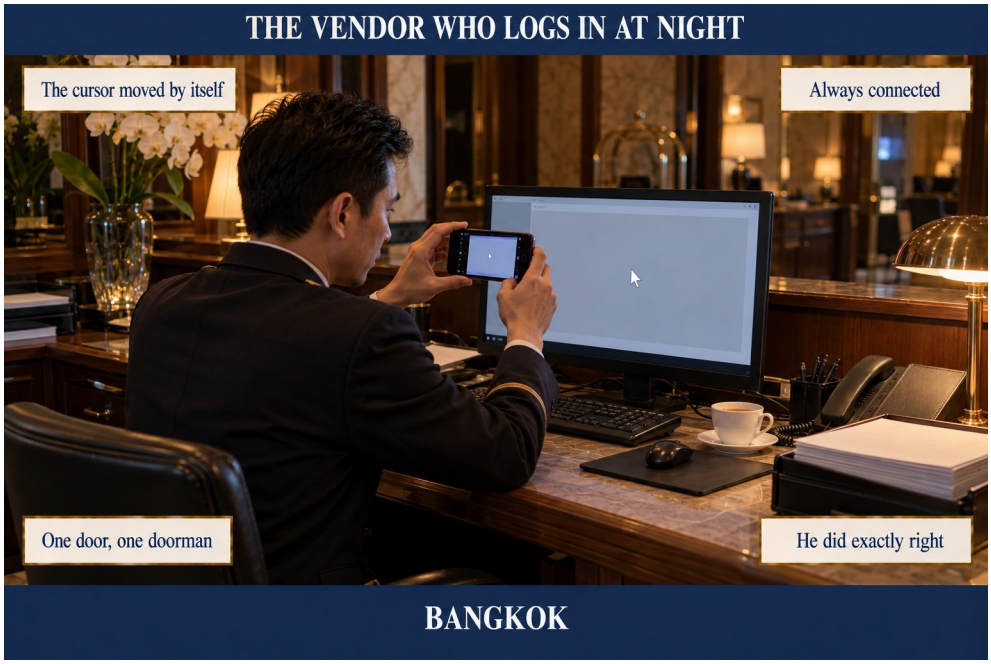
The plaques are the argument of the subchapter in four steps. The group runs the hotel; the quickest tool wins. Banning does not work, because staff away from desks will always use the tool that reaches their colleagues fastest. Offer something better is the answer: a tool the hotel controls, as quick as the one it replaces, with rules for what may pass through it.

The plate is not saying that the staff are doing anything wrong. They are running the hotel with the tool that lets them do it well. It is saying that if the hotel does not provide a quick tool that is also safe, its information will flow through channels it neither owns nor controls, and that the general manager's decision is the one still to be taken.

CONCEPT CARD 2.6

The Vendor Who Logs In at Night

Subchapter 2.6 · Bangkok



The night audit desk of a riverside hotel at three in the morning, the lobby dim behind. The night auditor sits with both hands raised away from the keyboard, holding his own phone to photograph the monitor. On the screen a plain grey window is open and an arrow cursor rests in the middle of it, moving by itself. A cup of tea and a stack of folios wait on the desk.

The card is about a door that was always open and the one person who noticed it. The cursor belongs to the supplier of the hotel's database, carrying out a maintenance nobody at the hotel had been told about, through a support tool set for unattended access with credentials known to every engineer at the supplier. This time it was the supplier. Nothing on the screen could have told the night auditor whether it was. He had never been told what to do in such a case, and did exactly the right thing: he touched nothing, recorded what he saw and called for help.

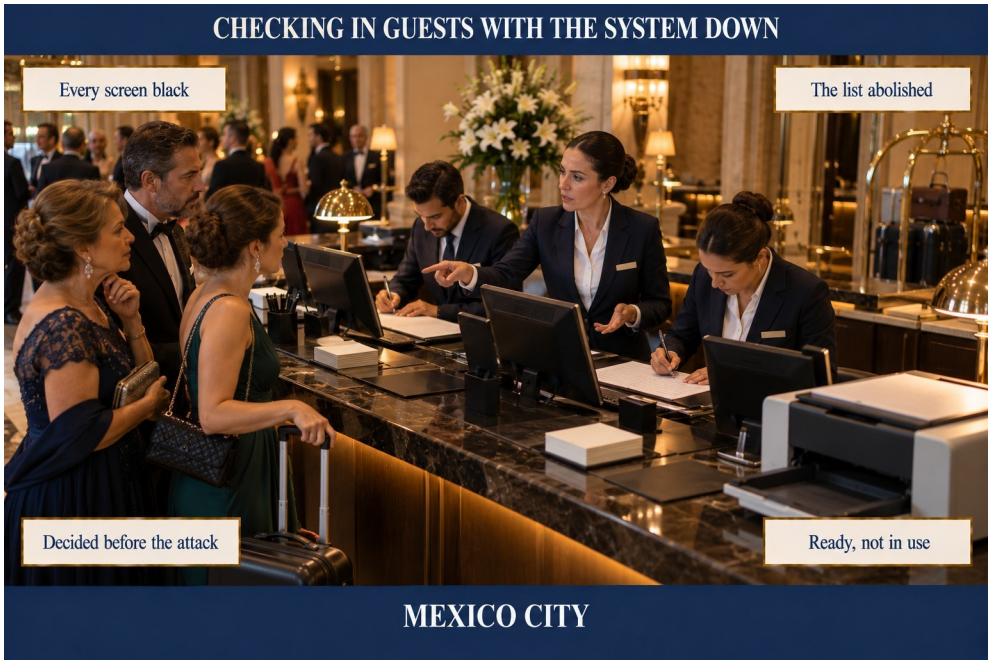
The plaques move from the event to the rule. The cursor moved by itself; always connected. One door, one doorman is the control the subchapter proposes: every supplier reaches the hotel through a single route the hotel controls, opened when the hotel agrees, for named people, and recorded. He did exactly right is the last plaque, and it belongs to him.

The plate is not saying that the supplier meant any harm or that remote support is dangerous in itself. Suppliers need to reach the systems they support. It is saying that a door opened whenever the supplier wishes, with keys held by the supplier's staff, is a door the hotel does not control, and that the person most likely to see it being used is the one person awake at three in the morning.

CONCEPT CARD 2.7

Checking In Guests With the System Down

Subchapter 2.7 · Mexico City



A large hotel lobby at two in the morning, full of wedding guests in evening clothes. At the front desk the night manager points and gives instructions, calm and decisive; two colleagues beside her write by hand on paper forms. The screens along the desk are dark. To the right, at the end of the counter, stands the printer, its tray empty. Three guests at the counter wait, patient and anxious.

The card is about continuity decided before the attack. The screens went dark at nine minutes past two, when the hotel's files were encrypted. What the desk needed at that moment was the list of who was in the house and who was arriving, printed every night for years and abolished as part of a programme to reduce paper, because nobody had ever needed it. The night manager is running the hotel on memory, paper and nerve, which is what a continuity plan should have made unnecessary.

The plaques describe the night and its lesson. Every screen black; the list abolished. Decided before the attack is the principle: a hotel's continuity after an attack is fixed by what it keeps ready beforehand. Ready, not in use is the last plaque, and the most practical one, because the fallbacks should be prepared and tested, not run every day in parallel with the systems.

The plate is not saying that the decision to reduce paper was foolish. Hotels are right to print less. It is saying that the things a hotel needs only when everything else has failed are the easiest to remove and the most expensive to lack, and that the night manager who kept the house running deserved a list, a procedure and a backup the attack could not reach.

CONCEPT CARD 2.8

Buying Software, and the Questions Nobody Asked

Subchapter 2.8 · Belgrade



A meeting room with brick walls in a converted warehouse hotel. A large scoring grid covers the wall, rows and rows of boxes all ticked. At the very bottom runs one row of empty boxes. A department head stands at the grid with a pen, still ticking near the top; two colleagues study it. In the foreground the general manager reads an email on a laptop, a hand over her mouth; on its screen is only a bright, cheerful banner.

The card is about the questions that are free before signing and expensive afterwards. The grid is the hotel's selection of a property system, two hundred and more requirements scored over three months, from rates to housekeeping to reports. The empty row at the bottom is everything nobody asked: how the supplier protects the data, what happens if it is sold, how the hotel gets its information back if it leaves. The email is the cheerful announcement that the system will be retired.

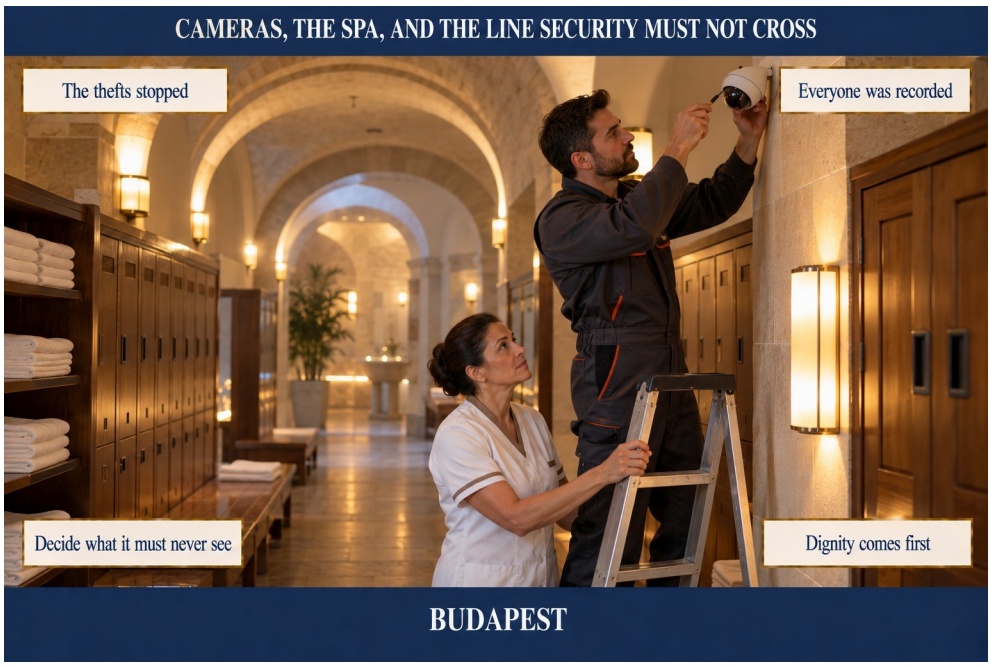
The plaques follow the selection to its consequence. Scored on functions; nobody asked how to leave. Free before signing is the moment when a supplier wants the contract and will answer any reasonable question. Expensive afterwards is what the same answers cost once the hotel depends on the system.

The plate is not saying that the committee did its work badly. By any ordinary standard the selection was thorough and the choice sound. It is saying that security and exit belong among the requirements from the start, answered in writing and carried into the contract, and that a migration is a change to be planned rather than an event to be endured.

CONCEPT CARD 2.9

Cameras, the Spa, and the Line Security Must Not Cross

Subchapter 2.9 · Budapest



The locker corridor of a hotel thermal bath early in the morning, closed and empty: stone arches, warm lamps, rows of wooden lockers, folded towels. A technician on a stepladder unscrews a small dome camera from high on the wall above the lockers. Below him the spa manager holds the ladder steady and looks up, relieved and resolute.

The card is about the camera coming down. It was installed after a spring of thefts from the lockers, and the thefts stopped. It also recorded, for ninety days, everybody who passed through the changing area of the bath, in the place where guests are most exposed and most trusting, and nobody could say who watched the recordings. The decision in the picture is the one the subchapter argues for: some places in a hotel no camera covers, whatever the problem to be solved.

The plaques set the two sides of the trade. The thefts stopped; everyone was recorded. Decide what it must never see is the principle, and it comes before any decision about where a camera should go. Dignity comes first is the last plaque, placed by chance beside the door to the changing rooms.

The plate is not saying that the spa manager was wrong to ask for help with the thefts, or that cameras have no place in hotels. They belong at entrances, in corridors, car parks and wherever cash is handled. It is saying that in a spa the cost of recording falls on every guest while the benefit is limited to a few incidents, and that the decision belongs to management, made before the camera is installed.

CONCEPT CARD 2.10

The Laptop That Left in a Taxi

Subchapter 2.10 · Singapore



The office of the director of events in a large hotel, early morning. She stands at her desk with the telephone to her ear, holding open an empty padded laptop sleeve and looking into it with alarm. On the desk lie a lanyard with a blank delegate badge, a stack of folders and her car keys. Shelves of event files fill the wall behind her.

The card is about the morning after. The laptop left the building the previous evening with the director, after a long day and a late dinner with the organiser of a regional summit, and it stayed on the back seat of a taxi. On it was the list of delegates, some of them senior officials. Whether the hotel now has a lost device or an incident to report to guests and clients depends on one thing decided months earlier: whether the laptop was encrypted.

The plaques say it as plainly as the subchapter does. Left in a taxi. Encrypted, it is lost; unencrypted, it is an incident. Report it at once is the last plaque and the only thing left in her hands this morning: the sooner the loss is reported, the sooner the device can be wiped and the questions answered.

The plate is not saying that the director was careless. She had worked on the summit for months and was tired at midnight, and devices that leave a building will be lost, left and stolen whatever anybody does. It is saying that what decides the consequence is whether the information on the device can be read by whoever finds it, and that the decision is management's, not the traveller's.

CONCEPT CARD 2.11

The First Seventy-Two Hours

Subchapter 2.11 · Barcelona



A management office on a Monday morning. Six people crowd around one desk, each with a telephone or a copy of the same printed page. One hands a sheet to the next; one telephones; one spreads her hands; the chef, in his white jacket, has been drawn in too. At the head of the desk the general manager's chair is empty, her jacket over its back.

The card is about the hours that decide an incident. The page they are passing round is an email that arrived at the hotel's general address on Friday afternoon, claiming to hold a database of its guests and demanding payment. It was read on Monday, forwarded eighteen times before eleven, and replied to by one recipient asking for proof. Nobody had yet decided whether the hotel had suffered a breach, or when the clock the law imposes had started.

The plaques describe the room and what it lacked. Read on Monday; forwarded to everyone. Who decides? is the question the whole scene is asking, and the empty chair is the only answer in it. Prepared beforehand is the last plaque and the argument of the subchapter: who decides at any hour, with deputies, a short set of first-hour questions and a way of keeping evidence can all be written in advance, and none of them can be invented under pressure.

The plate is not saying that anybody in the room behaved irresponsibly. Each of them did what seemed sensible: tell somebody more senior. It is saying that when nobody has been named to decide, telling everybody is what happens, and that the first seventy-two hours of an incident are settled by what was prepared before the email arrived.

CONCEPT CARD 2.12

Guest Wi-Fi and the Network Behind It

Subchapter 2.12 · Cartagena



The back of a conference room in a colonial hotel, white walls, dark beams, lanterns; a session is in progress, rows of delegates facing a speaker at a lectern. In the foreground a delegate with a lanyard and a laptop under his arm points into an open network cabinet on the wall. The hotel's IT manager looks where he is pointing, a hand at his chin. Inside the cabinet, bundles of blue cables and bundles of yellow cables run into the same equipment.

The card is about a network that was designed to be separate and had quietly become one. The blue cables carry the guests; the yellow ones carry the hotel, its back office, its printers and its file server. They should never meet, and here they meet in a single switch. In the case it was a bored delegate at a session on digital fraud who found it, from his seat, with the tools on his laptop, which is why it is a guest, not the hotel, who points into the cabinet.

The plaques describe the network as it is and as it should be. Strangers on the network, every night and every day of every event; one flat network behind them. Separation is easy to lose, because every event, supplier and convenience pushes towards connecting things. Somebody must own it is the last plaque, and it is the only control that keeps the separation alive after the next change.

The plate is not saying that the IT manager did not know his job, or that the delegate did anything but point out the obvious. It is saying that a hotel's guest network carries strangers and must be kept apart from everything the hotel runs, and that separation survives only if somebody owns it and checks it after every change.

CONCEPT CARD 2.13

Awareness Training That Changed Nothing

Subchapter 2.13 · Cusco



The reception of a hotel in a colonial building: stone walls, a carved counter, cushions woven in Andean patterns. The receptionist holds the desk telephone to her ear and reads aloud from her own mobile phone, where a set of empty boxes shows a code. She is helpful and unsuspecting. On the wall behind her, framed and hung with pride, is the certificate of the hotel's security training.

The card is about the difference between completing a course and changing a behaviour. Eight days earlier every member of staff had finished the online training, forty-five minutes in two languages. Now a caller claiming to be from the support team of the hotel's booking engine has asked the receptionist to read out the code that has just arrived on her phone, and she is doing it. The certificate behind her is accurate. It records that she took the course. It could not record what she would do when somebody plausible asked for something the hotel should never give.

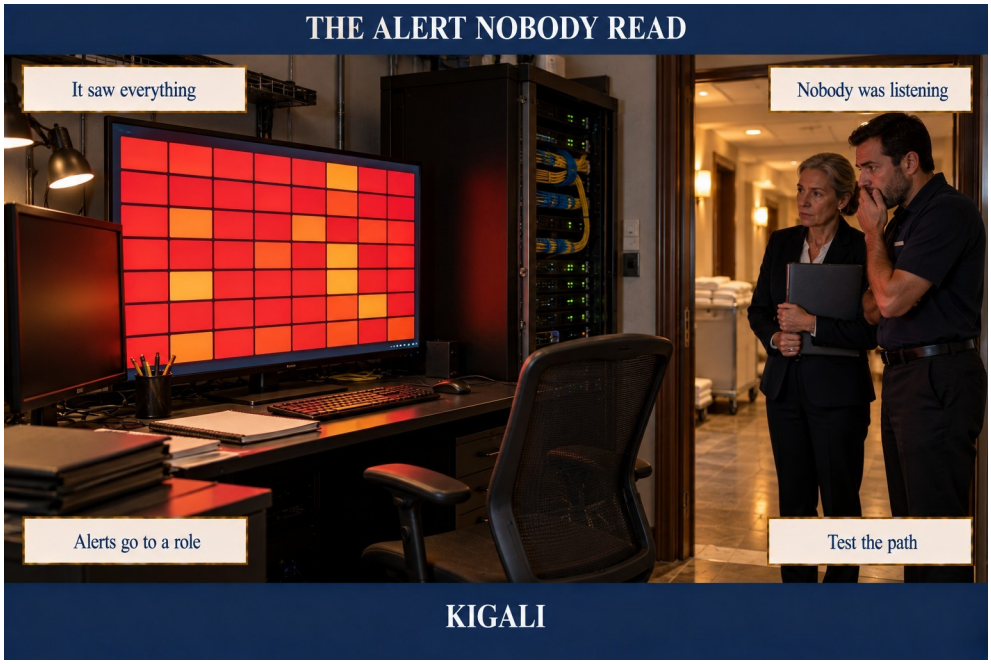
The plaques set the course against the counter. Everyone completed it; nothing changed. A short never list is the alternative: a handful of things the hotel never does, whoever asks, specific to each role. Practised until it is a reflex is the last plaque, and it names the only measure of awareness that matters, which is behaviour at the moment of pressure.

The plate is not saying that the receptionist was careless or that the general manager's training was wasted. She was trying to help, which is what a hotel trains its people to do. It is saying that awareness is formed by a few specific rules, repeated often, in the language and setting of the work, and backed by management's explicit permission to say no and to check.

CONCEPT CARD 2.14

The Alert Nobody Read

Subchapter 2.14 · Kigali



A small IT room in a conference hotel. A large monitor fills the left of the frame, covered in a grid of glowing red and amber tiles, urgent and unanswered. The chair in front of it is empty, pushed back. Beside it stands a rack of equipment with small green lights. In the doorway on the right, which opens onto a service corridor with a linen trolley, the certification auditor and the systems coordinator have just seen the screen and stopped.

The card is about a monitoring service that worked perfectly and a hotel that never heard it. The tiles are months of alerts: an unusual login to the finance system from abroad, a new administrator account, large exports of delegate lists. The service saw all of it and said so, in writing, at the time. It sent everything to an address that forwarded to the mailbox of an IT manager who had left, and his mailbox had been closed. The empty chair is the person the alerts were meant for.

The plaques follow the alert from the tool to the person. It saw everything; nobody was listening. Alerts go to a role is the first rule of the subchapter: a queue watched under contract and a named recipient at the hotel, never one person's mailbox. Test the path is the second, and it costs a few minutes a month: send a test alert and confirm that somebody received it.

The plate is not saying that anybody in the case was negligent. The IT manager set the service up correctly, the provider delivered its alerts faithfully and the leaving process closed a departing manager's mailbox as it should. It is saying that monitoring is somebody reading an alert, deciding what it means and acting, and that a hotel which buys a tool without deciding who reads it has bought a very good witness and nobody to listen to it.

CONCEPT CARD 2.15

Improvement, and the Finding Closed Three Times

Subchapter 2.15 · Wellington



The telephone room behind the front office of a waterfront hotel at two in the morning. The night auditor sits at a narrow desk and presses the power button of an old beige computer beside the grey cabinet of an ageing telephone exchange. The general manager stands behind her with his arms folded, watching. On the wall above the desk, pinned side by side, hang three identical memos in plastic sleeves.

The card is about a finding that came back because its cause never changed. The three memos are the hotel's corrective actions: each year the same computers out of support were found, and each year a memo instructed the IT provider to upgrade them. The computer she is restarting, as she does every night, runs the link to the telephone exchange and cannot be upgraded until the exchange itself is replaced, a purchase the owner had deferred for four years without being told what was waiting on it. She knew all of this. Nobody had asked her.

The plaques trace the finding to its source. Closed three times; the memo changed paper, and left everything else exactly as it was. The cause was upstairs, in the capital plan, out of reach of the manager who wrote the memos. Closed when the cause changes is the last plaque and the rule of the whole subchapter: a nonconformity is closed when the thing that produced it has changed, and the proof is looking again.

The plate is not saying that the general manager, the IT provider or the owner acted in bad faith. Each did what his position allowed. It is saying that a corrective action which stays with whoever received the finding will never reach a cause that sits in the owner's budget, and that the person who knows why a problem keeps returning is often the one restarting the computer at two in the morning.