CONCEPT CARD 3.1

Auditing Information Nobody Can See

Subchapter 3.1 · Zurich



The events office of a lakeside hotel, pale wood panelling and a vase of white flowers. At the desk a young events coordinator has turned from her laptop. The general manager stands behind her, serious. At the centre the group's auditor, grey-haired and in a dark suit, holds up a single printed sheet and, with his other arm fully extended, points through the open door to the goods entrance, where a black minivan waits with its tailgate raised and suitcases inside. On the desk, a row of blank delegate badges on lanyards.

The card is about an audit that follows the information instead of the organisation chart. The sheet in his hand is a delegate list, and his arm traces the route it actually took: from the client's email to the events office, from the office to a file-sharing link, from the link to the transfer company whose van is waiting at the door. His earlier audit had examined the server room and the procedures and found them in order. None of the places the list travelled through were on his plan.

The plaques state the method. Follow one piece of information; from arrival to deletion. Where the plan never went is the finding the case produced, and the last plaque is the lesson of the whole third chapter: the trail is the audit. Documents and procedures still matter, but an audit that never leaves the meeting room will certify the description and miss the hotel.

The plate is not saying that the auditor was careless or the coordinator reckless. He was meticulous within his plan, and she used the tool that was quickest for a busy supplier. It is saying that information in a hotel moves through people, suppliers and vehicles that no organisation chart shows, and that the internal auditor's first job is to walk the route it takes.

CONCEPT CARD 3.2

Planning an Audit Around the Hotel's Week

Subchapter 3.2 · Seville



The back office of a hotel in a converted palace: blue and yellow tiles along the wall, a studded wooden door, a lamp and paintings from an older house. The auditor, a greying man in a tweed jacket, stands before a large wall planner of coloured squares. One block is deep red and crowded; the green stickers that mark his past audit visits sit scattered in the pale, empty part of the planner. He is placing a green sticker inside the red block and holds another in his hand. The general manager watches with her arms folded. On a table beside them, an empty archive box with its lid open.

The card is about when an audit happens. The red block is the week of the city's fair, when the hotel runs full, the desk works on paper and extra staff arrive from an agency. Every earlier visit had been scheduled in the quiet weeks, when managers had time and the meeting room was free, and so every earlier report had described a hotel that existed only outside the fair. The empty box is the one that held three hundred registration cards and disappeared.

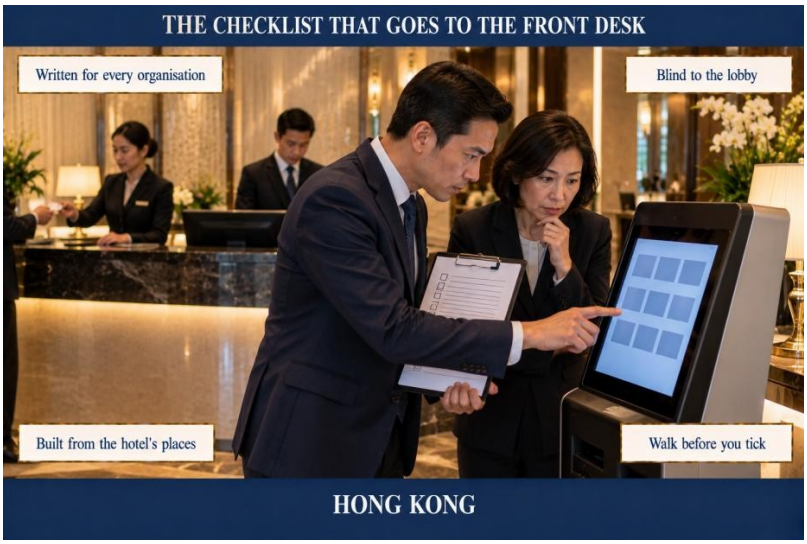
The plaques set the two calendars against each other. Audited in the quiet weeks; exposed in the busy ones. The calendar of exposure is the instrument of the subchapter, the hotel's year drawn from the point of view of its information, and go when it matters is the rule it leads to. Not every audit activity belongs in the peak, but some of them must.

The plate is not saying that the auditor avoided the fair on purpose. He planned as auditors usually plan, around availability. It is saying that a hotel's controls are tested by its busiest hours, its nights and its seasons, and that an audit programme which never sees them measures the hotel precisely when it is least like itself.

CONCEPT CARD 3.3

The Checklist That Goes to the Front Desk

Subchapter 3.3 · Hong Kong



The lobby of a large business hotel: stone floors, orchids, brass lamps and a long marble reception desk where two receptionists are working. In the foreground stands a self-service check-in kiosk. The auditor, in a navy suit, holds a clipboard with a checklist of empty tick boxes and points at the kiosk's screen, which shows a grid of small grey thumbnails. Beside him the general manager has her hand at her chin, beginning to understand.

The card is about where a checklist is written and where it is used. The auditor's list had ninety-three lines, one for each reference control, and it had been completed in a meeting room with the IT provider answering the questions. The kiosk was not on the provider's inventory and not on the checklist, and so nobody had ever stood in front of it. The thumbnails are what a guest found by pressing the wrong button: a gallery of recently scanned passports.

The plaques describe the checklist that failed and the one that replaces it. Written for every organisation; blind to the lobby. Built from the hotel's places is the method: a short list of questions organised by desk, office and floor, each asked where the work is done. Walk before you tick is the discipline behind it.

The plate is not saying that the audit firm was incompetent or the kiosk supplier negligent. A standard checklist is a reasonable tool for many organisations. It is saying that a hotel's information lives in places no generic checklist anticipates, and that the auditor who walks the lobby before writing the questions will find what the meeting room cannot show.

CONCEPT CARD 3.4

Auditing the Law Without Becoming a Lawyer

Subchapter 3.4 · Vienna



A meeting room in a nineteenth-century hotel: high mouldings, a tall green tiled stove, white double doors with brass handles. Three people sit at a round polished table. On the left, a thick stack of bound legal documents tied with ribbon. At the centre the auditor, fair-haired, places a single printed page in the middle of the table and holds her finger on it. The general manager and the data protection adviser both lean towards that one page, not towards the stack.

The card is about the difference between auditing a law and auditing the process that meets it. The bound documents are the hotel's privacy notices, consent forms and processing records, all in order, all of which the auditor had checked weeks before and declared compliant. The single page is a guest's request to stop her newsletter and delete her details, sent as a reply to an email and filed in the marketing inbox without anybody recognising it for what it was.

The plaques draw the line the subchapter draws. Not a legal opinion: the internal auditor is not the one to say whether the hotel complies with the law. Who owns the obligation, and where the request arrived, are the questions the auditor can and must ask. The process meets the law is the conclusion: the auditor tests the route by which an obligation is recognised, owned and answered, and leaves the legal verdict to those qualified to give it.

The plate is not saying that the auditor was careless or the adviser absent. She audited conscientiously what the documents said, and the adviser had never been shown the report. It is saying that an internal audit which pronounces on the law overreaches, and that one which follows the obligation to the inbox where it actually lands finds what matters.

CONCEPT CARD 3.5

The Digital Near-Miss

Subchapter 3.5 · Kuala Lumpur



The IT office of a large conference hotel, a server rack glowing green on the left and a door with a small round window at the back. The auditor, in a dark headscarf and grey blazer, sits at the desk with an open bound register whose pages are completely empty, and points at the monitor beside it, filled with rows of amber tiles. Behind her the general manager stands with his hand at his chin, unconvinced; beside him the director of sales holds her phone and looks at the screen with growing concern.

The card is about the meaning of an empty register. For three years the hotel had reported zero security incidents, and the register under the auditor's hand confirms it. The monitor tells another story: thousands of messages blocked, hundreds of failed attempts to sign in to the sales director's account, all recorded by the systems and seen by nobody. The woman with the phone is the person whose account will be compromised five weeks later.

The plaques put the two sources of evidence side by side. Zero incidents; the filter saw everything. The silence is the finding, because a register with nothing in it describes a hotel that is not looking rather than one that is safe. Near misses are evidence is the principle: the events that did no harm are the cheapest information a hotel will ever receive about where harm will come from.

The plate is not saying that the general manager was complacent or the provider negligent. The hotel had a good record and was proud of it. It is saying that an internal auditor should treat the absence of reported events as a question rather than a result, and should go to the systems and the people who see near misses every day before accepting that nothing has happened.

CONCEPT CARD 3.6

Interviewing for Awareness

Subchapter 3.6 · Lima



A guest-floor corridor: patterned carpet, wall lights, closed room doors without numbers, a narrow grey equipment cupboard set into the wall. A housekeeping trolley with folded white towels stands between two women. The auditor, in a grey jacket with a lanyard, holds a small notebook and listens. The floor supervisor, in a grey uniform with a white collar, explains with one hand on her chest and the other open towards the cupboard door.

The card is about where and how awareness is audited. The earlier audit had interviewed twelve people in the human resources office, in English, chosen by the human resources manager. None of them worked on the floors. The supervisor in the picture is the person who opened that cupboard to a man in a telecommunications vest who said he needed to check the internet for her floor, and who left a small device on the network for seven weeks. Nobody had ever asked her, at her trolley, what she would do.

The plaques describe the method of the subchapter. Asked at the trolley; in the language of the work. What would you do is the question that replaces whether she knows the policy, because she did know it, and it did not help her. Awareness is behaviour is the principle: it is measured by what people do at the moment of pressure, not by the certificate on the wall.

The plate is not saying that the supervisor failed. She was courteous to a stranger in a uniform, as the hotel had trained her to be to everyone. It is saying that an interview conducted away from the work, in the wrong language, with the wrong sample, measures how well people answer auditors, and that the internal auditor learns what a hotel really knows by asking the people on the floors, where they are.

CONCEPT CARD 3.7

Second-Party Audit: The Software House and the Cloud

Subchapter 3.7 · Manila



A back office in a business hotel, a whiteboard covered with coloured boxes and arrows, a lamp and a plant. The systems coordinator, in a light embroidered barong shirt, sits at a desk bent over a thick bound report, one page marked with a red tab. Beside him the general manager, in a dark blazer, holds up a framed certificate with a gold seal and nothing else on it, looking from the frame to the report.

The card is about two documents from the same supplier. The framed certificate is the software house's information security certificate, obtained every year and filed as proof that the hotel's property system was in safe hands. Its scope, read for the first time after an outage, covered software development at the supplier's head office and said nothing of hosting. The report with the red tab is the supplier's assurance report on its hosted service, available on request for three years and never requested. The red tab marks the exception: restore tests of client databases had not been performed.

The plaques contrast what was done with what should have been. The certificate was framed; the report was never read. Scope before seal is the rule for any certificate a supplier offers, and ask what they did not test is the question that turns a second-party audit from a collection of documents into an examination of the service the hotel actually depends on.

The plate is not saying that the coordinator was lazy or the supplier dishonest. He followed the hotel's procedure faithfully, and the supplier's certificate was genuine. It is saying that a second-party audit must read what a supplier's assurance covers and what it excludes, because the hotel's exposure usually lies in the part the certificate does not mention.

CONCEPT CARD 3.8

Retention: The Data the Hotel Believes It Deleted

Subchapter 3.8 · Stockholm



A basement equipment room with concrete walls and exposed pipes. On the left, modern server racks glow blue and green. On the right, in a dusty corner, stands an old beige tower server, visibly years older than everything else, still connected by a single blue network cable. The auditor, grey-bearded, kneels beside it and follows the cable with his hand towards the wall. Behind him the general manager holds a single printed policy page and stares at the old machine.

The card is about the difference between a retention policy and the places where data is actually kept. The page in her hand is the policy: guest profiles kept three years, then purged, and the purge worked perfectly on the new property system. The old server in the corner held every guest since the hotel opened, kept switched on after a migration so that finance could look up old invoices. When a former supplier was breached, the stolen data went back twelve years, not three.

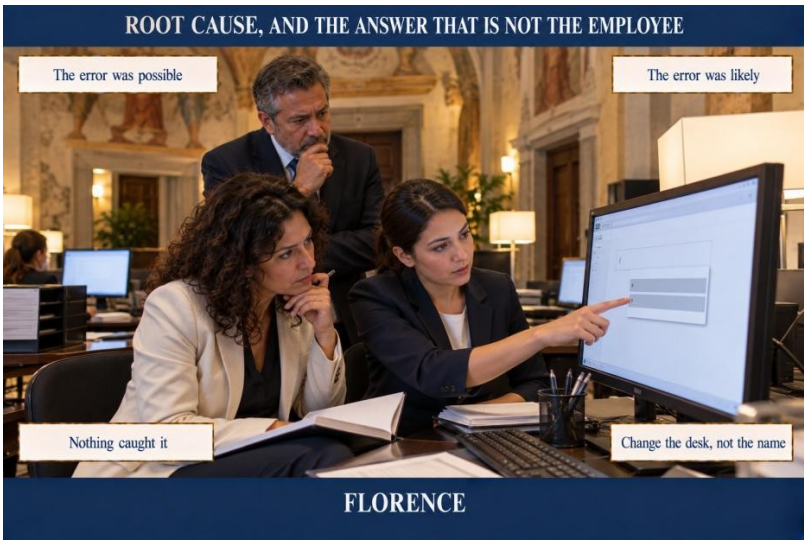
The plaques trace the gap. Deleted where the policy said; kept where nobody looked. The old server was still on is the literal finding, and retention is a hunt is the method: the internal auditor does not test a retention policy by reading the purge report, but by searching for every other place the data may still live, old systems, backups, suppliers, spreadsheets.

The plate is not saying that the general manager wrote a bad policy or that the IT provider disobeyed it. The policy was sound and the purge ran every month. It is saying that data outlives the systems it was written for, and that an audit of retention begins where the policy ends: in the corners, the backups and the suppliers nobody has asked to delete anything.

CONCEPT CARD 3.9

Root Cause, and the Answer That Is Not the Employee

Subchapter 3.9 · Florence



The reservations office of a Renaissance palazzo hotel: frescoed vaults, stone door frames, desks with monitors. A young reservations agent points at her screen, where an email drop-down offers two nearly identical grey bars. Beside her the auditor, dark curls and a cream jacket, sits with a notebook on her knee and watches closely. The general manager stands behind them, thoughtful, his hand at his chin.

The card is about where the cause of an error is found. Two rooming lists, months apart and from different desks, went to the same wrong travel agency because the email program completed the address from two agency names that differed by one word. The first incident was closed as human error, with a written warning to the agent. The auditor is doing what the first investigation did not: sitting at the desk and watching the task, until the cause is visible on the screen.

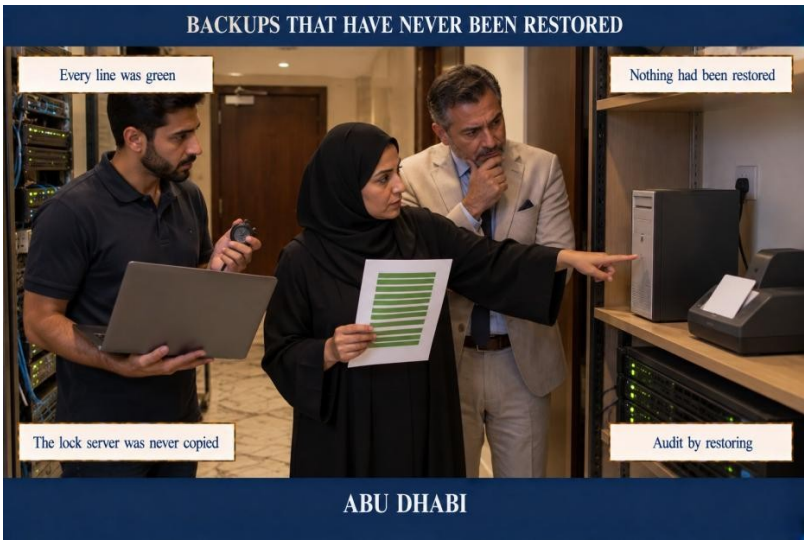
The plaques are the questions the subchapter asks. The error was possible; the error was likely; nothing caught it. Each points at something that can be changed: the tool that guessed, the fifty lists a day sent at the end of a shift, the absence of any check before sensitive data left the hotel. Change the desk, not the name is the conclusion: a corrective action must remove a cause, and a warning to one person removes none.

The plate is not saying that nobody is ever responsible for anything. Deliberate misuse and repeated carelessness belong to the disciplinary process. It is saying that human error is where an investigation begins, not where it ends, and that the internal auditor who watches the work will usually find a cause that every person at the desk shares.

CONCEPT CARD 3.10

Backups That Have Never Been Restored

Subchapter 3.10 · Abu Dhabi



A narrow room behind the front office of a luxury hotel, a server rack on the left and shelves on the right. The auditor, in a black abaya and headscarf, holds a report of solid green bars and, with her arm fully extended, points at a small grey computer tower on a shelf beside a key-card encoder. The tower is connected to nothing but power. The general manager, in a pale suit, looks at it with concern; the IT engineer holds a laptop and a stopwatch, ready for a restore test.

The card is about what a backup report proves. Every night for years the IT provider's report had shown a green line for every backup job, and every line was accurate. The small tower is the server that runs the hotel's door locks and encodes every key. It had been installed by the lock supplier's agent and never added to the provider's list, so it had never been copied. Nobody knew until the auditor asked for a restore rather than a report.

The plaques move from reassurance to evidence. Every line was green; nothing had been restored. The lock server was never copied is the finding that paid for the whole audit. Audit by restoring is the principle: a backup is a promise about the future, and the only way to check a promise is to ask for it to be kept, in a safe place, with a clock running.

The plate is not saying that the provider lied or the hotel neglected its systems. The provider copied exactly what it had been asked to copy and reported it honestly. It is saying that the internal auditor must test recovery, not reporting, and must start from the systems without which the hotel cannot trade rather than from the provider's list of what it happens to back up.

CONCEPT CARD 3.11

Auditing Accounts and the Rights Behind Them

Subchapter 3.11 · Oslo



A meeting room in a modern waterfront hotel, pale wood and a painting of a northern sea. On the table lies a long row of identical signed sheets, each with rows of grey marks and a signature at the bottom. The auditor, short blond hair and a navy sweater, points with a pen at one line on one sheet. Across from her the front office manager, in hotel uniform with a blank name badge, holds her hand to her chin and hesitates.

The card is about a control that was performed without being understood. Every quarter for two years, every head of department had signed that the access rights of their staff were correct. The sheets on the table are those signatures. The line under the auditor's pen is a role code that allowed two night receptionists to post unlimited adjustments to guests' bills and to close the day that would report them. The manager in the picture had signed eight times for rights she could not describe.

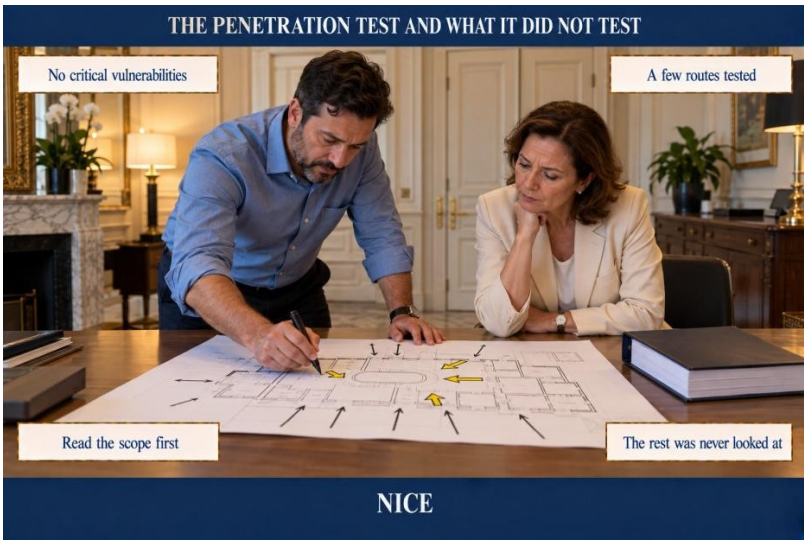
The plaques trace the finding to its method. Signed every quarter; nobody knew the codes. Compare the work with the rights is how the auditor tests a review: ask the manager what the job requires, ask the system what the person can do, and set the two side by side. A review you can read is the corrective action: rights described in the language of the work, so that a signature means something.

The plate is not saying that the managers were negligent. They did every quarter exactly what they were asked to do. It is saying that an access review sent in system codes to people who do not speak that language produces signatures without judgement, and that the internal auditor audits the review by performing it again on a sample.

CONCEPT CARD 3.12

The Penetration Test and What It Did Not Test

Subchapter 3.12 · Nice



A high-ceilinged office in a Belle Époque hotel: marble fireplace, white double doors with gilded handles, orchids, a gilt mirror. The auditor, shirt sleeves rolled up, leans over a large floor plan of the hotel spread on the table and draws with a marker. Arrows point into the building from every side; only three of them are yellow. The general manager, in a cream jacket, watches with her chin on her hand. Beside the plan lies a thick bound report, closed.

The card is about reading a test from the back. The closed report is four years of penetration tests, each concluding that no critical vulnerabilities were found, each conclusion true. The arrows are every route by which somebody outside could reach the hotel's information: the website, email and staff remote access, which the test covered, and the guest network, the meeting room sockets, the lock supplier's remote access, the booking engine, the guest app and the staff themselves, which it never did. The three yellow arrows are the only ones that had been tested.

The plaques follow the argument. No critical vulnerabilities; a few routes tested. Read the scope first is the rule for every test report, and the rest was never looked at is the finding: not a vulnerability, but a part of the hotel about which the hotel knew nothing.

The plate is not saying that the testers were incompetent or the report misleading. They tested what they were asked to test and reported it honestly. It is saying that a test answers the question it was given, and that the internal auditor's job is to lay that question over the hotel as it is now and see how much of it was never asked.

CONCEPT CARD 3.13

The Report That Ownership Will Read

Subchapter 3.13 · Chicago



A dark-panelled boardroom in a convention hotel, a polished table, a closed door and brass lamps. On the left, a thick audit report lies open in the middle. The auditor, in a grey suit, slides across the table a single sheet with three short highlighted bars. The owner's asset manager holds that sheet and reads it attentively. Beside her the general manager listens, his hand at his chin.

The card is about the page an owner actually reads. The thick report is the internal audit: sixty-two pages, forty-one findings, ordered by the clauses of the standard, the most important of them on page forty-one. The asset manager had read its first page, which said the system was broadly effective, and filed it. The single sheet is the report rewritten for her: what the hotel risks, what must be decided, by whom and by when. It is the first internal audit report she has finished.

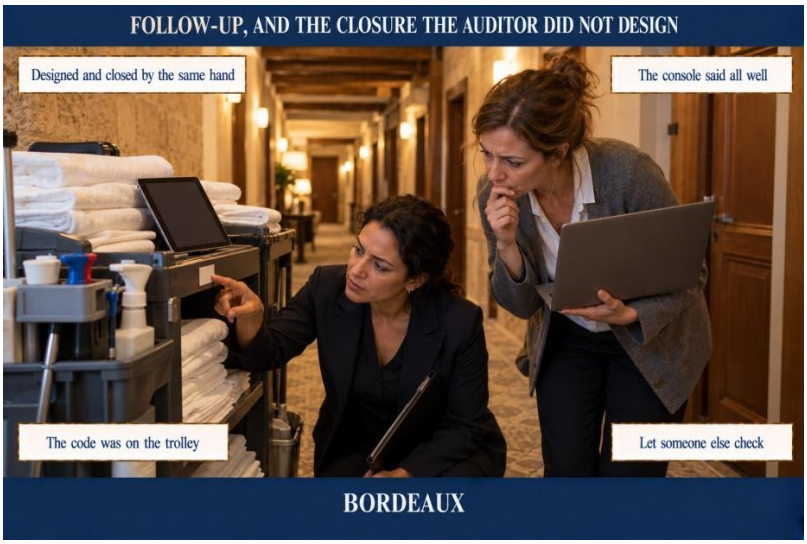
The plaques describe the two reports. A thick report; the first page is read. What must be decided is the question the first page must answer, in the owner's language rather than the auditor's. Write for the decision is the principle: the detail stays in the annex, complete, and the page on top carries only what the person with authority needs to act.

The plate is not saying that the first report was wrong or the owner inattentive. Every finding was accurate, and she read what she was given. It is saying that an internal audit produces value only when somebody with authority understands it and decides, and that the report is the only bridge between the auditor's evidence and that decision.

CONCEPT CARD 3.14

Follow-Up, and the Closure the Auditor Did Not Design

Subchapter 3.14 · Bordeaux



A guest-floor corridor in a converted wine warehouse: limestone walls, timber beams, patterned carpet, closed room doors. A housekeeping trolley stands against the wall with a tablet resting on the towels. The second auditor, dark curly hair and a black jacket, crouches beside it and points at a small white label stuck to the trolley's edge. Behind her the first auditor, in a grey cardigan, holds a laptop and covers her mouth with her hand.

The card is about who should judge a fix. The first auditor had found that housekeeping tablets held guest information without protection, designed the device management solution herself, and closed the finding two weeks later when the console showed every enrolled device compliant. The label on the trolley carries the single code every housekeeper uses, because they wear gloves and share tablets. The console could not see it, nor the eight tablets bought later and never enrolled. The colleague from a sister hotel saw both in a day.

The plaques describe the failure and the rule. Designed and closed by the same hand; the console said all well. The code was on the trolley is the evidence no record could show. Let someone else check is the principle: independence in follow-up protects not against dishonesty but against the designer's blind spot.

The plate is not saying that the first auditor was careless. She found a real problem, designed a sensible remedy and checked it honestly. It is saying that the person who builds a solution is the person least able to see what it was never built to handle, and that follow-up belongs to somebody who did not design the fix, looking at the real population, after enough time for real work to test it.

CONCEPT CARD 3.15

What the Internal Audit Owes the Management Review

Subchapter 3.15 · Brussels



A meeting room in a city hotel, panelled walls, a closed wooden door, orchids and a tray of glasses. On the long table lie three large grids side by side, one for each year of the certification cycle. In all three the same small block of squares is coloured and a large part is white. The auditor, short grey hair and a dark green jacket, stands over them and points at the edge where colour meets white. The general manager, seated, looks at the three grids with his hand at his chin.

The card is about what three years of audit add up to. Each year the auditor had reported the same slide: programme completed as planned, findings raised and closed, no major nonconformities. Each statement was true. Laid side by side, the three programmes show that the same third of the management system had been audited every year and another third never, and that five findings had returned in every year under different numbers.

The plaques set activity against assurance. Programme completed; nothing said what was missed. Coverage, trend, opinion are the three things the audit owes the management review beyond the list of findings: what has and has not been examined over the cycle, which findings recur, and what the auditor judges can be relied on. Assurance, not activity is the principle that closes the chapter.

The plate is not saying that the auditor did her work badly or that management ignored her. She did the programme she was given, and the review noted the results it was shown. It is saying that the management review needs to know what the audit can vouch for, and that only the auditor, reading the whole cycle, can tell it.

CONCEPT CARD 4.1

The Chain That Makes a Certificate Mean Something

Subchapter 4.1 · Paris



The lobby of an elegant Paris hotel, marble floors and a dark wooden reception desk in the background. On the wall behind the internal auditor, a pale rectangle with four small holes shows where a frame hung until a moment ago. He holds that frame under one arm, a certificate with a gold seal and nothing else, and in the other hand a tablet whose screen shows an empty search bar and no results. The general manager, in black, looks at the empty screen with her hand at her chin.

The card is about what makes a certificate worth anything to a stranger. The certificate had been bought with a consultancy package, after a one-day audit by video call, and carried a seal that said accredited. A client's supplier-risk analyst looked for the certification body in the accreditation directories and for the seal's issuer among the members of the international arrangement, and found neither. The empty search on the tablet is her result, reproduced by the hotel's own auditor.

The plaques follow the chain link by link. Bought with the consultancy; accredited by nobody; not in any register. A certificate is its chain is the conclusion: a certificate carries the credibility of the independent checks behind it, a certifier assessed by an accreditation body, an accreditation body evaluated by its peers, a public register anyone can consult, and nothing more.

The plate is not saying that the hotel set out to deceive anybody. It bought in good faith what it was offered as certification. It is saying that certification is not a document but a relationship with an independent body that is itself held to account, and that a hotel which can make the chain check on its own certificate, and on its suppliers', will never again frame a document that means nothing.

CONCEPT CARD 4.2

Choosing a Certification Body That Has Seen a Hotel

Subchapter 4.2 · Venice



The water entrance of a palazzo hotel: stone steps, a doorway lit from within, striped mooring poles and a polished wooden water taxi at the landing. A porter in uniform lifts a suitcase with a blank luggage tag from the boat. The certification auditor, grey-haired in a dark coat, holds an open notebook and listens to the general manager, who gestures towards the entrance as she explains how guests and their information arrive.

The card is about choosing the audit rather than the certificate. The hotel had first chosen the cheapest accredited body, and its auditor, an expert from banking, spent the better part of two of four days with the IT provider and in the equipment room and never saw the arrivals, the night or the events. The auditor in the picture is the one the owners chose at renewal, a former front office manager, who spent his first evening on the landing watching luggage and lists arrive by water taxi. His first report was the first that described the hotel.

The plaques contrast two ways of buying certification. The cheapest day; the fewest days. An auditor who knows hotels is what the rules make possible and hotels rarely ask for: the certifier must disclose the team, and the hotel may ask about their experience and object. Choose the audit is the principle: among accredited bodies, the one whose audit will see the hotel as it works.

The plate is not saying that the first auditor was incompetent or that price does not matter. He was competent in everything he examined, and the saving was real. It is saying that every accredited certificate looks alike and the audits behind them do not, and that a hotel which compares days, calculation, experience and time in operations, rather than the price of a day, buys an audit that can find what matters.

CONCEPT CARD 4.3

Stage 1: Is the System Ready to Be Audited?

Subchapter 4.3 · Cairo



A meeting room in a large riverside hotel, dark panelling, a marble sideboard and white flowers. At the round table the certification lead auditor, in a navy headscarf and grey jacket, calmly closes her folder. In front of her lies a document whose pages show only an empty grid under a pale red stamp. The general manager and the security coordinator, sleeves rolled up and tired, listen in silence with their hands at their faces. A fourth chair at the table is empty.

The card is about the moment a certifier says the system is not yet ready. The date of certification had been set by the board in January, before the system existed, and stage 1 was fixed to meet it. The document on the table is the statement of applicable controls, still a draft, with every control marked implemented. The empty chair is the internal audit and the management review, both scheduled for after the certifier's visit on a consultant's advice. The auditor has just explained that she cannot recommend stage 2.

The plaques tell the case in order. The date came first; the system came after. Not a free rehearsal is the point the hotel had missed: stage 1 decides whether stage 2 makes sense, and the certifier may say what she found but not how to fix it. A cycle must have run is the rule: risks assessed, controls operating, an internal audit and a review done, before the certifier arrives.

The plate is not saying that anybody in the hotel was careless. The board had good reasons, the coordinator worked evenings and the consultant delivered on time. It is saying that a management system cannot be hurried into having worked, and that a hotel which checks its own readiness first will hear, at stage 1, a confirmation rather than a refusal.

CONCEPT CARD 4.4

Stage 2: Does It Work at the Counter?

Subchapter 4.4 · Hanoi



The front desk of a busy city hotel at a quarter to five: a coach at the glass doors, a queue of tourists with suitcases, orchids and lamps. The certification auditor, in a dark suit, bends over a tray beneath the counter, full of photocopies. Beside him the general manager, in a black high-collared jacket, follows his gaze. A tour leader in the foreground holds a bundle of dark passports tied with a rubber band. Behind the desk a receptionist feeds another sheet into the copier.

The card is about where implementation is proved. The hotel had prepared a perfect meeting room, with binders, presentations and tea, and the auditor spent the first morning there. Then he asked to stand at the desk at the arrival peak. The tray holds forty-two passport copies from one tour group, kept overnight under the counter because the queue left no time to scan and shred them. The same afternoon a room number was given to a caller, and that night a guest list lay on a corridor printer.

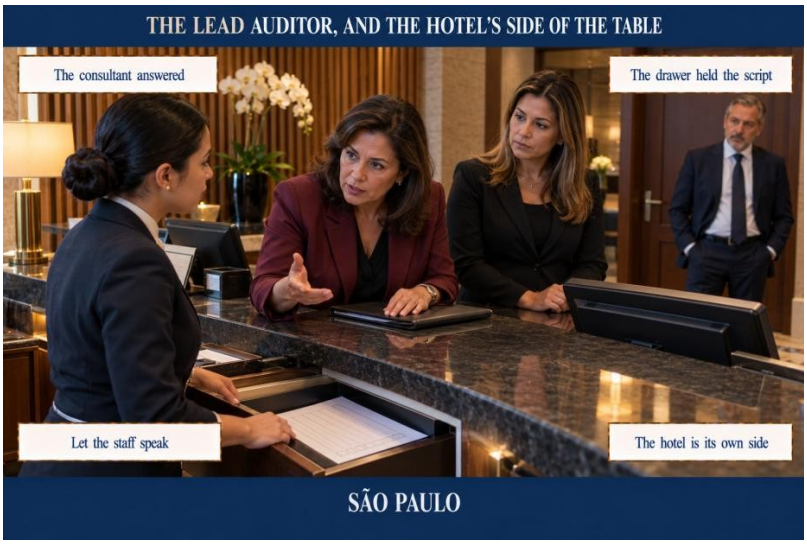
The plaques set the two audits side by side. The meeting room was perfect; the counter was not. Seen at the busiest hour is the method of stage 2 at its best: the auditor goes where and when the work is done, with the permission and ideally the invitation of the hotel. It works or it does not is what the certifier is there to find out.

The plate is not saying that the preparation was wasted or that the staff were careless. The managers understood their system and the receptionists were serving a queue. It is saying that a hotel's information security is performed, shift by shift, under pressure, and that a hotel which walks its own desk at five and its back office at two before the certifier does will know what stage 2 will find.

CONCEPT CARD 4.5

The Lead Auditor, and the Hotel's Side of the Table

Subchapter 4.5 · São Paulo



The front desk of a business hotel, dark stone counter and a wall of wooden slats behind. The certification lead auditor, in a burgundy jacket, leans on the counter and speaks directly to a young receptionist, who has just opened a drawer. Inside lies a single printed sheet of lines and boxes. Beside the auditor the security coordinator stands quietly as the guide. In the background, near the office door, a man in an expensive suit stands apart with his hands in his pockets: the consultant.

The card is about who speaks for the hotel. For the first morning of the surveillance audit the consultant who had built the system walked beside the auditor and answered every question on behalf of the staff, and his contract paid him more if no major findings were raised. After lunch the coordinator became the guide and the consultant stayed in the office. The sheet in the drawer is a script headed with the questions an auditor might ask; one of its answers described a procedure the hotel had abandoned.

The plaques trace the change of arrangement. The consultant answered; the drawer held the script. Let the staff speak is the rule the certification rules support: a guide arranges, protects and clarifies, and never answers for the person interviewed. The hotel is its own side is the principle: the people who run the system are the ones who show it.

The plate is not saying that the consultant acted in bad faith or that the receptionist did anything wrong. Each good intention put something between the auditor and the hotel. It is saying that an audit is a conversation between an independent auditor and the organisation that operates the system, and that the hotel owes the auditor its own voice, just as the auditor owes the hotel competence and respect.

CONCEPT CARD 4.6

Objective Evidence in a Business That Runs on Trust

Subchapter 4.6 · Macau



A private room in a luxury resort: dark lacquered wood, a brass lamp, orchids and a low marble table. The certification lead auditor, in a dark grey suit, points her pen at one row of a printed list in which every row is covered by a solid black bar. On her right the director of information security holds a sealed envelope. On her left the vice-president of hotel operations, in a red jacket, watches her choose.

The card is about evidence where nothing can be shown. The resort's most valuable guests are known to very few, and on the first morning the director handed the auditor a letter declaring that the controls around them were in place and could not be shown. The envelope is that letter. The list under her pen is the answer they worked out together: allocation records with every name masked, from which the auditor chooses her own sample by date and room, so that the control is seen and the guest is not.

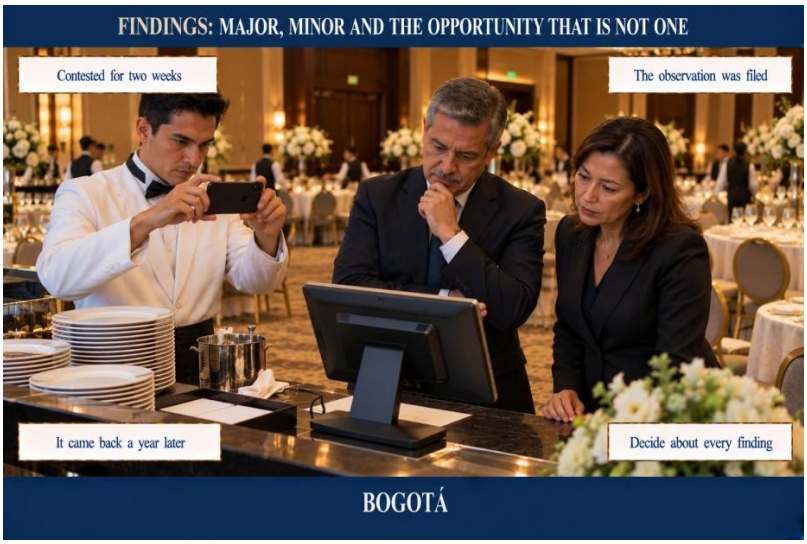
The plaques move from refusal to method. Nothing could be shown; a letter is not evidence. Masked, sampled, tested names the techniques: masked records, samples chosen by the auditor, negative tests of access, logs by user without guests' names. Show the control, not the guest is the principle, and it is also how the hotel should be able to check its own protection.

The plate is not saying that the resort was hiding a failure. Its instinct to protect its guests was sound. It is saying that a control no one can see working cannot be trusted by anyone, the owners and the guests included, and that evidence must be designed into the control so that its working can be demonstrated while what it protects stays hidden.

CONCEPT CARD 4.7

Findings: Major, Minor and the Opportunity That Is Not One

Subchapter 4.7 · Bogotá



A hotel ballroom being set for a wedding: round tables with white cloths, tall arrangements of white flowers, waiters in the distance. At the banqueting station, beside stacks of plates, stands a tablet on a stand. A young waiter in a white jacket, from an agency, holds up his own phone as if to photograph something. Across the station the certification lead auditor, grey moustache and dark suit, and the security coordinator look at the tablet, and she has just seen the waiter.

The card is about the observation nobody decided about. A year earlier the auditor had recorded an opportunity for improvement: the hotel might extend its awareness briefing and confidentiality undertakings to the agency staff in banqueting, who handled guest lists. The coordinator filed it in a spreadsheet of ideas. This year agency staff were four in ten of the banqueting team, none briefed, guest lists open on a shared tablet, and one list had appeared on a waiter's social media. The condition the observation had pointed to had become a major nonconformity.

The plaques tell the year in order. Contested for two weeks: the hotel spent its energy arguing about a minor finding it could have checked in a day. The observation was filed; it came back a year later. Decide about every finding is the rule: check the facts, answer nonconformities with cause and corrective action, and record a decision on every observation, even if the decision is to accept the risk.

The plate is not saying that the hotel was negligent. The general manager defended a system he was proud of and the coordinator kept a careful list. It is saying that a finding is a sample of a larger population and an observation is the auditor's judgement about risk given without charge, and that a hotel which files either without deciding has chosen not to hear it.

CONCEPT CARD 4.8

The Certificate, and What It Actually Certifies

Subchapter 4.8 · Casablanca



An office in a seafront hotel, green and white zellige tiles along the wall, a carved wooden door and a brass lamp. The internal auditor holds the certificate out of its frame and points at its small gold seal. Beside it an open laptop shows the hotel's homepage, where a gold badge fills most of the screen. The general manager and the marketing director look from the modest certificate to the enormous badge.

The card is about the difference between what a certificate says and what a hotel says about it. The certificate names one company, one site and a scope limited to reservations, the front office and guest data in the property system, and refers to a version of the statement of controls the hotel no longer uses. The homepage, published the day the certificate arrived, promised conference organisers that their delegates' data was fully protected. Events were not in the scope.

The plaques trace how the gap opened. Posted before it was read; one department certified, or at least a part of the hotel much smaller than the badge implied. The page promised the hotel is the problem a client's analyst found in one line. Read it as a client would is the discipline: every line of the certificate, the organisation, the site, the scope, the version, the dates, and every public statement made to match.

The plate is not saying that the marketing director meant to mislead. She celebrated a real achievement with the tools she had and nobody had shown her the scope. It is saying that a certificate is a narrow and exact document, that clients increasingly read it as one, and that somebody at the hotel must own the certificate and every claim made in its name.

CONCEPT CARD 4.9

Surveillance, and the Year the Hotel Changed Hands

Subchapter 4.9 · Taipei



The general manager's office of a modern city hotel, shelves of binders behind, a monitor on the desk. The certification lead auditor, in a grey jacket, holds open a ring binder whose coloured divider tabs are still in place but which contains no pages. The monitor shows a grey panel with a red cross: access denied. The new general manager and the owners' asset manager look at the empty binder, uneasy.

The card is about the year the management system left with the operator. In the spring the owners changed management company. The old operator took back its policies, closed the hotel's access to the intranet where the documents lived, and took its security coordinator with it. The new operator brought new systems, new suppliers and new managers. Nobody told the certification body. The binder with its tabs and no pages is what the surveillance auditor found in September.

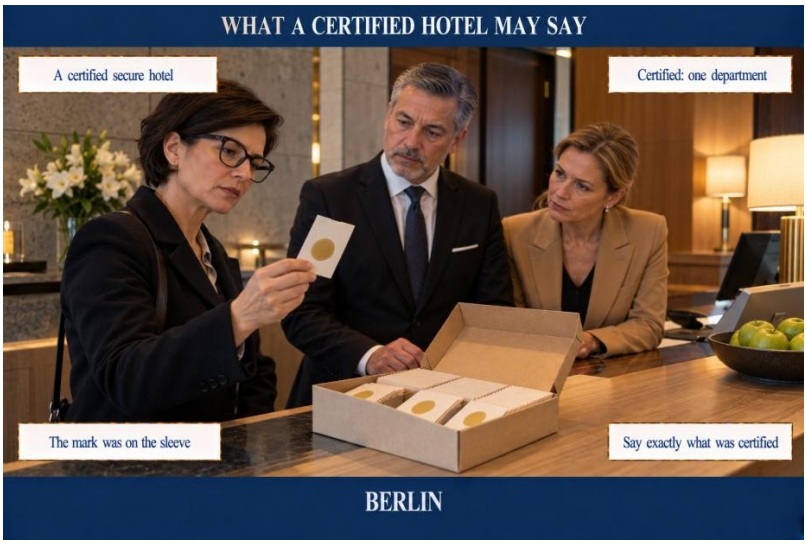
The plaques tell the case in four lines. New operator, same certificate; the system left with them. Nobody told the certifier, although the rules require significant changes to be reported without delay. Carry the system through the change is the lesson: owners should own their management system whoever operates the hotel, and a transition plan should carry it across, with the certifier informed before the change rather than after.

The plate is not saying that the transition was badly managed. For guests and staff it was handled with care. It is saying that a certificate describes a system as it was found at an audit, that surveillance checks it still exists, and that a hotel which changes hands without telling its certifier can spend months displaying a certificate for a system that is no longer there.

CONCEPT CARD 4.10

What a Certified Hotel May Say

Subchapter 4.10 · Berlin



The reception of a design hotel: concrete walls, a long oak counter, a bowl of green apples. The certification lead auditor, short dark hair and black-framed glasses, holds up a small key card sleeve printed with a gold seal. On the counter an open cardboard box holds thousands more. Behind the counter the general manager and the group's human resources director look at the sleeve with embarrassment.

The card is about the claims a certificate can carry. The group's certificate covered its central IT department and nothing else. Its human resources director used it to attract staff, with advertisements for a certified secure hotel, and the new key card sleeves carried the certifier's mark and a line promising that the guest's stay was protected to international standards. A candidate for the security coordinator's post read the scope in the register and withdrew her application. The surveillance auditor raised a finding on the use of marks.

The plaques set the claim against the certificate. A certified secure hotel; certified: one department. The mark was on the sleeve, and a management system mark may never appear on anything a guest could read as a guarantee of the service. Say exactly what was certified is the rule: the standard, the scope in plain words, the certifier, and where to check.

The plate is not saying that anybody set out to mislead. The human resources director saw a real achievement and wanted to use it. It is saying that every claim about certification borrows the credibility of the certifier and the accreditation chain, that the rules on marks exist to protect it, and that precise claims attract the people a hotel most wants to hire.

CONCEPT CARD 4.11

Integration with Quality, Environment, Safety and Privacy

Subchapter 4.11 · Lyon



A vaulted basement room with a ventilation duct along the ceiling. On the left, metal shelving holds white drums of pool chemicals in yellow spill trays. On the right stands a black server rack with green lights. Between them the certification lead auditor stands with her arms spread, one hand towards each side of the room. Beside her the quality manager holds three binders against her chest, one blue, one green, one red.

The card is about a room that three management systems had each seen and none had understood. In the environmental register it was the pool chemical store; in the health and safety register, a hazardous substances store with forced ventilation; in the information security register, the equipment room with the hotel's main server. Each register was correct. None mentioned the others, and so nobody had noticed that the pool contractor had a key to the server rack, or that the ventilation drew corrosive air across it. The three binders are the three systems.

The plaques describe the problem and the answer. Separate registers, same room; nobody saw the server. Risks sit between standards is the lesson of the subchapter: a risk that falls on the boundary between two systems belongs to neither unless they are joined. A single system for all is the answer, one management system that meets several standards, with one risk register looking through every lens.

The plate is not saying that any of the systems was badly built. Each was sound and each certificate deserved. It is saying that a hotel is one organisation in one building, that the standards share a common structure so that they can be run as one system, and that the first auditor qualified to look through all of them at once is often the first to see what lies between them.

CONCEPT CARD 4.12

Lenders, Insurers and the Certificate as Evidence

Subchapter 4.12 · London



A dark-panelled boardroom in a riverside hotel, a brass lamp and white flowers. The bank's technical adviser, silver hair and a dark suit, reads a thick audit report with more open reports beside her. The framed certificate, with its gold seal, has been pushed to the far end of the table. The fund's asset manager and the hotel's finance director wait for her verdict.

The card is about what a certificate proves to people who lend money and pay claims. The hotel had sent its certificate to the bank, the insurer and the rating agency as the answer to their questions. The adviser, a former certification lead auditor, asked for everything behind it: the scope, the statement of controls, the audit reports, the incidents. She found a scope that excluded the booking engine and payments, a finding on supplier authentication open for fourteen months, and an incident the owners had never heard of, while the insurer had been told a control was in place that was not.

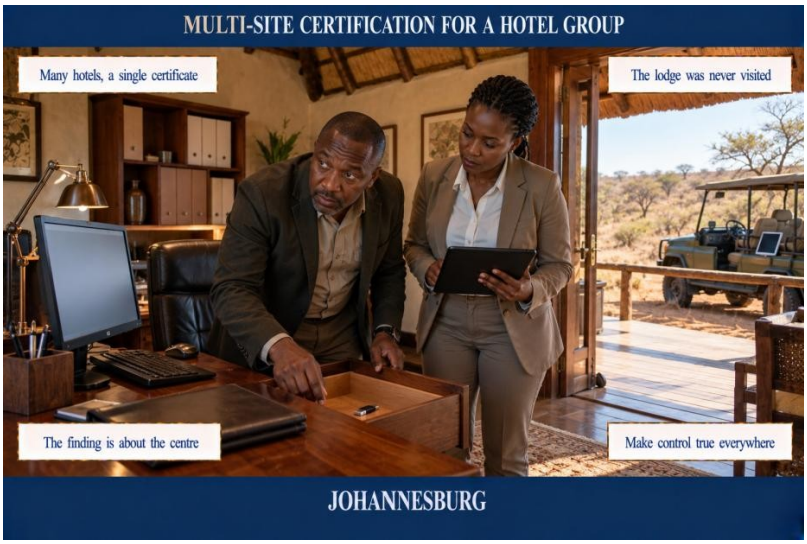
The plaques trace the change of view. The certificate was enough, the hotel believed; the lender asked for more. The same account for every reader is the discipline: one evidence pack, one person answering every questionnaire from facts, so that the bank, the insurer and the investor are never told different things. The start of the evidence is what the certificate is.

The plate is not saying that the certificate was worthless. The adviser said it had been worth a great deal, because it told her an accredited body had found a working system. It is saying that a certificate shows governance within a scope and nothing more, and that a hotel which presents it with its limits, and backs it with honest evidence, will be believed by the people who price its risk.

CONCEPT CARD 4.13

Multi-Site Certification for a Hotel Group

Subchapter 4.13 · Johannesburg



The reservations office of a safari lodge: a thatched roof, rough plastered walls, a wooden desk with a computer. The certification lead auditor, in a khaki shirt and dark jacket, bends over an open drawer in which lies a single USB stick, and looks up with a serious expression. Beside him the lodge manager holds a tablet. Through the open door, beyond the veranda, the bushveld and a game-drive vehicle with a ranger's tablet left on the seat.

The card is about the site the group never visited. Eight properties held a single multi-site certificate, with a central function at head office and a sample of sites audited each year. The lodge had been described as similar to the city hotels, and the group's own internal auditors, based three hours away, had never been there. The auditor chose it. The USB stick holds the lodge's reservation backups; the tablet on the vehicle's seat holds guests' itineraries and medical notes, with no lock.

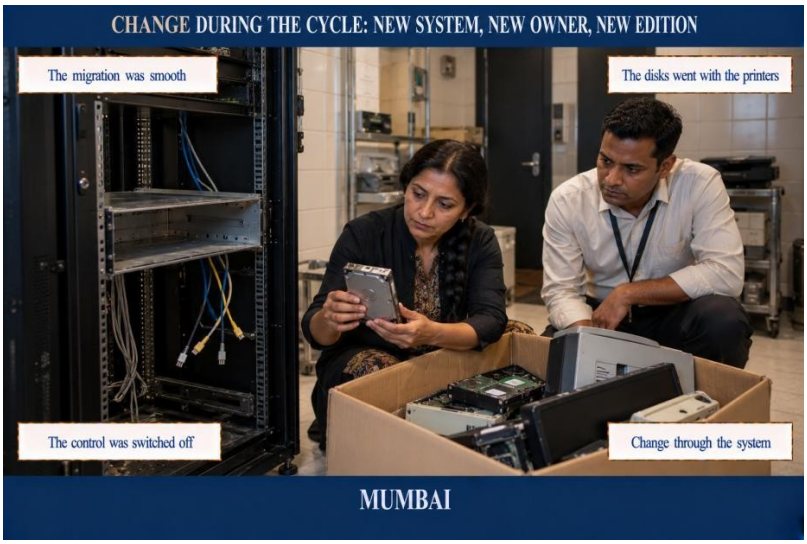
The plaques explain why one site matters to all. Many hotels, a single certificate; the lodge was never visited. The finding is about the centre, because a multi-site certificate rests on central control, and a site the centre does not reach is evidence against the whole. Make control true everywhere is the principle: honest site descriptions, internal audit of every site, and central authority over local suppliers.

The plate is not saying that the lodge manager resisted the group or that the certifier was unfair. The manager had asked head office for help and been told to find it locally. It is saying that central control that never made the journey to a remote site is not control, and that the certifier's sample is designed to find exactly such a site.

CONCEPT CARD 4.14

Change During the Cycle: New System, New Owner, New Edition

Subchapter 4.14 · Mumbai



A hotel equipment room with white tiled walls. On the left a rack stands open with an empty space where a server has been removed, loose cables hanging. On the floor beside it, a cardboard box full of old printers, circuit boards and bare hard drives waits for collection. The certification lead auditor, a long dark plait over her shoulder, crouches by the box and holds up one hard drive. Beside her the security coordinator looks from the drive to the empty rack.

The card is about a change that passed around the management system. The hotel had moved its property system to the cloud in three months, smoothly, without a single guest noticing. Nobody had assessed the risks of the migration, the supplier's test environment still held a full copy of two years of guests, and the old server's disks had been sent with the printers to an electronic waste recycler. The statement of controls still marked cloud services not applicable, a decision taken during the transition to the 2022 edition two years before.

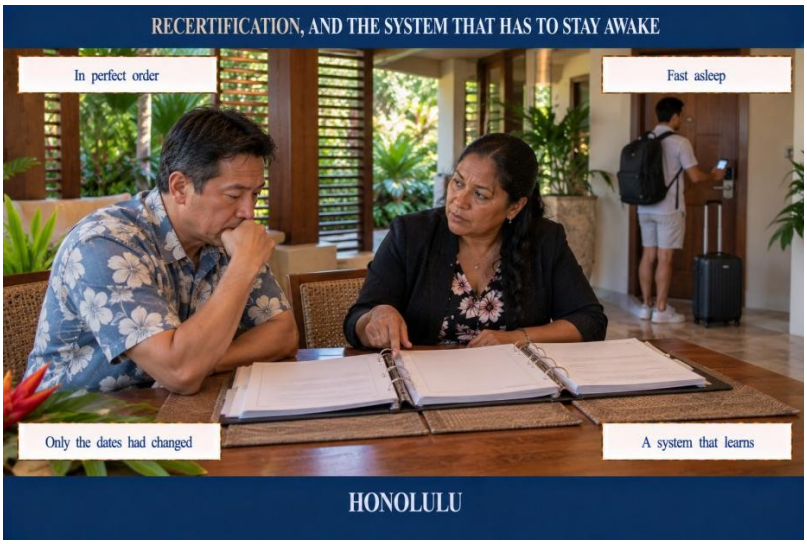
The plaques name the three failures and the rule. The migration was smooth; the disks went with the printers; the control was switched off, before the migration was even imagined. Change through the system is the principle: every significant change, a new system, a new owner, a new edition of the standard, passes through the risk assessment, the statement of controls and the certifier's knowledge before it takes effect.

The plate is not saying that the project was badly run. It was an excellent project from every point of view the project team was asked to consider. It is saying that a management system exists to absorb change, and that a change which goes around it leaves the system describing a hotel that has moved on, with its old data in a box by the door.

CONCEPT CARD 4.15

Recertification, and the System That Has to Stay Awake

Subchapter 4.15 · Honolulu



A covered lanai in a beach resort: louvred wooden walls, tropical plants, woven placemats on a wooden table. The certification lead auditor, long dark hair and a floral blouse under a dark jacket, points at three identical binders open side by side at the same page. Across from her the security coordinator, in an aloha shirt, covers his mouth with his hand. In the background a guest with a backpack and a suitcase opens his room door with his phone.

The card is about a system in perfect order and fast asleep. At recertification the auditor read the whole cycle: three years of documents in which only the dates had changed, the same risks with the same scores, the same statement of controls, objectives always met, the same audit findings each year. Meanwhile the hotel had introduced mobile keys, digital check-in with passport photographs and an automated messaging service whose supplier kept guests' conversations abroad indefinitely. The guest at the door is the change the system never saw.

The plaques read as the auditor's verdict. In perfect order; fast asleep. Only the dates had changed is the evidence. A system that learns is what recertification looks for: risks questioned, controls following the hotel's changes, objectives that stretch, reviews that decide, and a cycle account that shows what three years taught.

The plate is not saying that the coordinator neglected his work. His records were among the best the auditor had seen, and that is why their stillness was so visible. It is saying that a management system is a process of noticing and changing, that its sign of life is change with reasons, and that a hotel whose system is kept awake by everybody, not only by its coordinator, will find recertification a confirmation of what it already knows.