

A lobby remodel can change what a security camera sees without anyone moving the camera. A new reception desk may sit lower, a mirror may reflect a corridor, and a reconfigured waiting area may bring private conversations into view. The result can [blur license plates on cctv](#) be a system that captures more than it did before—or misses the entrance it was meant to monitor.

After building work, do not assume the old camera plan still works. Recheck camera angles, confirm the purpose of each view, and document any changes to access, retention or disclosure arrangements. This guide is for property managers, building teams and owners reviewing CCTV in a shared lobby.

Start with the security question

Before adjusting a camera, ask: **What security question does this camera answer?** For example, is it intended to record who enters through the main doors, help investigate damage to the reception area, or show activity at a controlled-access point? If the purpose is unclear, the answer is not simply to widen the view. A camera should not capture areas “just in case”.

Write down the specific purpose and the area needed to meet it. This gives the team a practical test for whether the current field of view is proportionate. It also helps prevent a gradual expansion of surveillance when furniture, partitions or finishes change.

Why a remodel changes what the camera captures

Small design changes can have a surprisingly large effect on a fixed camera’s view. A desk change affects capture if it blocks a doorway, exposes a previously obscured area or shifts the flow of people through the lobby. New partitions can create blind spots. Glass and polished surfaces may produce glare or reflections.

Pay particular attention to mirrors. A **mirror expands camera view** in the sense that it can reflect an area the camera cannot see directly. It may bring a lift lobby, seating area or corridor into the recording, even though the camera has not moved. Check mirrors from the camera’s actual position and review the recorded image—not just the room in person.

Who should approve CCTV changes?

Camera decisions should have clear ownership. Depending on the building and its governing documents, responsibility may sit with the owners’ association or HOA, the property manager, a managing agent, or another designated controller. The onsite team can identify operational issues, but should not make informal, undocumented changes to surveillance coverage.

Agree who can approve a change, who can adjust equipment, and who may access or export recordings. If the remodel affects shared spaces or residents’ privacy, take the proposal through the building’s established governance process. Consult the relevant privacy lead or legal adviser when needed, particularly where the proposed view would newly include areas where people may reasonably expect privacy.

A practical post-remodel field-of-view check

1. **Gather the baseline.** Find the approved camera plan, stated purpose, previous field-of-view images and any documented privacy masks. Note when the old view was last checked.

2. **Walk the remodeled lobby.** Compare the plan with the finished layout. Check doors, desk positions, seating, mirrors, screens, glass partitions and routes to lifts or amenities.
3. **Review each live and recorded view.** Confirm what the camera actually records at representative times, including when lights change or sunlight causes glare. A live monitor alone may not show the final recorded quality.
4. **Check the intended area.** Verify that the camera can answer its documented security question. Make sure entrances or relevant access points are not obscured by the new layout.
5. **Identify unnecessary capture.** Look for apartment doors, computer screens, sign-in details, payment terminals, private work areas, seating where conversations occur, or views into adjoining spaces.
6. **Adjust proportionately.** Use a narrower angle, repositioning, zoom or privacy masking where appropriate. Avoid solving a blind spot by simply capturing a much larger area.
7. **Record the result.** Save a dated image or diagram of the approved view, the reason for any adjustment, who approved it and who carried it out.

Use a simple review table

Check What to look for Action if there is a problem Camera purpose A specific, current security need Clarify the purpose before changing coverage Entrance coverage The relevant entry point is visible and usable footage is recorded Adjust position or framing without broadening the view unnecessarily Reflections Mirrors, glass or polished surfaces reveal additional areas Reposition, mask or change the reflective surface if suitable Privacy Desks, screens, seating or unrelated private areas are captured Restrict the view and document the change Access and exports Named, authorised people can access recordings Review permissions and export controls Retention A defined period and routine deletion are in place Correct settings and verify deletion works

Minimise the footage, not just the camera count

Data minimisation means collecting only the footage needed for the stated purpose. It is not enough to have a small number of cameras if each one records a broad sweep of the lobby. Review the edges of the image as carefully as the centre: incidental capture often happens at the edges or in reflections.

Use camera positioning and privacy masking to exclude areas that do not need to be recorded. Masks should be checked after any change to camera angle because a mask that once covered a desk or doorway may no longer align. If the camera is repositioned, review the full image again rather than assuming the existing settings remain effective.



Access, exports and disclosure logs

Set access by role and operational need. A person being able to view a monitor does not automatically mean they should be able to search, download or share recordings. Avoid casual viewing and prevent raw clips from being circulated by email or messaging apps.

Before any export, ask: **Where will the exported clip end up, and who can open it?** Use an approved, access-controlled method, record the reason for the export and log who authorised it, who received it, when it was shared and when it should be deleted. Keep a disclosure log in line with the building's policy and applicable legal requirements. Do not put recordings in an unrestricted shared folder with no deletion date.

Set a retention period and make deletion routine

Recordings should not be kept indefinitely by default. Set a retention period that reflects the system's purpose, building policy and applicable law. Configure routine deletion, then periodically confirm that it is operating as intended. A retention setting on a screen is not proof that old footage has actually been deleted.

If footage must be preserved for a specific incident or lawful request, isolate only the relevant material where possible, restrict access, document why it is being held and set a review or deletion date. Do not let an incident hold become a reason to retain unrelated footage indefinitely.

Common mistakes to avoid

- **Assuming the camera stayed compliant because it did not move.** The remodel may have changed sightlines, reflections and foot traffic.
- **Widening the view to fix a blind spot.** First consider whether repositioning, a narrower adjustment or a privacy mask would meet the security need with less capture.
- **Checking only the live picture.** Confirm what is recorded and whether lighting, glare or image quality affects the result.
- **Leaving approval informal.** Record who owns the decision and who authorised any change.
- **Keeping footage "just in case".** Apply a defined retention period and routine deletion.

- **Sharing clips casually.** Control exports, recipients, storage and deletion dates.

What about prices?

There are no prices listed here. The cost of a post-remodel review depends on the number and type of cameras, whether a specialist is needed, the complexity of the system and any required equipment or privacy changes. Obtain a scoped quote rather than relying on an unverified figure. Ask what the work includes: a visual inspection, recorded-image checks, angle adjustments, masking, documentation, access-control review and verification of retention settings may be separate items.

Keep a small review record

For each camera checked, record its identifier, location, purpose, review date, approved view and any changes. Include who performed and approved the work. Also note whether mirrors or other reflective surfaces affect the view, whether privacy masks were tested, and whether access and retention settings were reviewed. Store this record with the building's CCTV documentation, not in an informal email thread.

Share an approved update

If residents or occupants need to be informed, use the building's normal communications channels to explain the relevant policy or a material change. Keep the message accurate and proportionate: it should describe the camera's purpose and where to find more information without exposing sensitive system details. For social sharing, use the building's approved communications account and wording.



- [Share on Facebook](#)
- [Share on X \(Twitter\)](#)

Final check

A lobby remodel is a prompt to recheck camera angles—not a reason to expand surveillance automatically. Confirm the security question, inspect the recorded view for changed capture, minimise unnecessary footage, and

keep ownership of CCTV decisions clear. Finally, review who can access or export clips, where exports go, and whether recordings are deleted on schedule. A short, documented review can catch a changed field of view before it becomes an avoidable privacy or governance problem.