

RETAIL CCTV AUDIT CHECKLIST TEMPLATE

CCTV Audit Checklist

Use this template to review camera coverage, image quality, recording, retention, storage, access, privacy, monitoring, playback, evidence handling, maintenance, corrective actions, and management sign-off across retail locations.

STORE / LOCATION

AUDIT TYPE

DATE AND WINDOW

AUDITOR

1. Audit setup, system inventory, and ownership

- Confirm the correct store, audit type, date, approved window, and current CCTV policy version. **CRITICAL** DROPDOWN + DATE + TIME

AUDIT TYPE

Routine / targeted

DATE

Select

WINDOW

Start to end

Execution tip: Use the assigned location and latest approved checklist so results remain comparable across stores and audit periods.

- Record the CCTV system type, recorder model, software version, and monitoring arrangement. SYSTEM PROFILE

RECORDER

DVR / NVR / cloud

MODEL

Enter

VERSION

Enter

Execution tip: Capture the actual deployed configuration, including local recording, cloud recording, remote monitoring, and hybrid setups.

- Reconcile the installed camera inventory with the approved camera and device register. **CRITICAL** REGISTER RECONCILIATION

REGISTERED

Count

INSTALLED

Count

EXCEPTIONS

Count

Execution tip: Match camera IDs, locations, models, serial numbers, recorder channels, and operational status against the current register.

- Confirm the store manager, security owner, system administrator, and maintenance contact. PEOPLE PICKER

STORE OWNER

Select

SECURITY OWNER

Select

SUPPORT CONTACT

Select

Execution tip: Use named owners so faults, privacy concerns, and evidence requests can be routed without delay.

- Review previous CCTV faults, open work orders, incidents, retention failures, and repeat findings. **CRITICAL** LINKED RECORDS

OPEN FAULTS

Count

RECENT INCIDENTS

Count

REPEAT FINDINGS

Count

Execution tip: Start with overdue faults and repeat failures. Repeated camera or recorder issues should receive a higher priority.

- Capture arrival geo-location, timestamp, and an approved reference photo of the CCTV control area. **CRITICAL** GEO + TIME + LIVE PHOTO

GEO

Verified

ARRIVAL

Timestamp

Add live photo

Execution tip: Require live capture where policy allows to verify the audit occurred at the assigned location and time.

2. Camera coverage, placement, and field of view

7 Verify every approved camera is installed in the correct location and aimed at the intended zone.

CRITICAL

COVERAGE GRID

Camera ID	Approved zone	Actual view	Action

🔍 Execution tip: Compare the live view with the approved camera plan and record moved, missing, blocked, or incorrectly aimed cameras.

8 Confirm entrances, exits, cash points, high-value displays, stockrooms, and loading areas have usable coverage.

CRITICAL

CRITICAL AREA REVIEW

☐ Entrances / exits
 ☐ Cash points
 ☐ High-value stock
 ☐ Loading / stockroom

🔍 Execution tip: Prioritize areas where incidents are most likely or evidence is most important. Record every uncovered critical zone.

9 Check camera views are not blocked by signage, displays, shelving, decorations, vegetation, or stored goods.

OBSERVATION + PHOTO

Clear
Partially blocked
Blocked
Add photo

🔍 Execution tip: Inspect the current trading layout rather than relying on the original installation plan.

10 Verify camera height, angle, and distance allow useful identification and activity review.

CRITICAL

SCORED STATUS + COMMENT

Usable
Limited
Unusable

🔍 Execution tip: A wide view is not enough if faces, hands, transaction areas, or entry points cannot be identified clearly.

11 Identify blind spots created by walls, fixtures, doors, queues, fitting rooms, or seasonal layouts.

CRITICAL

BLIND-SPOT MAP

BLIND SPOTS | Count

HIGHEST RISK ZONE | Describe

ACTION OWNER | Select

🔍 Execution tip: Walk the area from likely approach routes and document blind spots with the exact location and risk.

12 Confirm privacy-sensitive areas are excluded from inappropriate CCTV coverage.

CRITICAL

PRIVACY STATUS + EVIDENCE

Compliant
Review needed
Privacy breach
Add evidence

🔍 Execution tip: Check cameras do not capture washrooms, changing areas, private offices, or other prohibited spaces beyond approved boundaries.

3. Image quality, focus, lighting, and scene usability

- 13 Confirm each sampled camera produces a clear, stable, and correctly oriented live image. CRITICAL IMAGE QUALITY RATING

Clear Acceptable Unusable

🔍 Execution tip: Check for blur, shake, tilt, distortion, frozen frames, or incorrect rotation during normal operation.

- 14 Check focus and zoom support identification at the required distance. CRITICAL FOCUS TEST + SCREENSHOT

TEST
DISTANCE || Enter

Pass Fail Add sample

🔍 Execution tip: Use a real object, face chart, or reference point at the intended capture distance rather than judging from an empty scene.

- 15 Verify day and night image quality under actual lighting conditions. CRITICAL DAY / NIGHT COMPARISON

Camera	Day image	Night image	Result

🔍 Execution tip: Review both bright and low-light footage. Record glare, reflections, overexposure, shadows, and infrared washout.

- 16 Check backlighting, sunlight, mirrors, glass, and digital displays do not obscure critical details. LIGHTING OBSERVATION

No issue Intermittent issue Material issue

TIME
OBSERVED || Enter

🔍 Execution tip: Inspect at different times where risk changes with sunlight, external lighting, or display brightness.

- 17 Confirm camera lenses, housings, domes, and protective covers are clean and undamaged. CONDITION STATUS + PHOTO

Good Cleaning needed Damaged Add photo

🔍 Execution tip: Look for dust, grease, scratches, condensation, paint, tape, impact damage, and deliberate obstruction.

- 18 Verify camera names, labels, and on-screen titles match the actual location and viewing direction. CRITICAL LABEL RECONCILIATION

CHECKED || Count

MISMATCHED || Count

CORRECTED || Count

🔍 Execution tip: Incorrect camera names delay incident review and can cause the wrong footage to be exported.

4. Recording status, date and time, retention, and continuity

19 Confirm all active cameras are recording continuously or according to the approved schedule.

CRITICAL

RECORDING TEST

EXPECTED CHANNELS

|| Count

RECORDING

|| Count

NOT RECORDING

|| Count

🔍 Execution tip: Check the recorder status and playback, not only the live view. A camera can appear online without recording.

20 Verify the displayed date, time, and time zone match an approved reference.

CRITICAL

TIME SYNCHRONIZATION

REFERENCE TIME

|| Enter

SYSTEM TIME

|| Enter

DIFFERENCE

|| Minutes

🔍 Execution tip: Compare against a trusted time source and record the difference. Even small errors can weaken incident evidence.

21 Test playback from a recent sample time for every critical camera group.

CRITICAL

PLAYBACK SAMPLE

Camera group	Sample time	Playback	Gap

🔍 Execution tip: Choose defined sample times across entrances, cash points, high-value areas, and back-of-house zones.

22 Confirm the actual footage retention period meets the approved requirement.

CRITICAL

RETENTION CALCULATION

REQUIRED

|| Days

ACTUAL

|| Days

GAP

|| Days

🔍 Execution tip: Check the oldest available footage and compare it with policy, storage design, incident risk, and legal requirements.

23 Review recording gaps, dropped frames, offline periods, and repeated reconnection events.

CRITICAL

EXCEPTION LOG REVIEW

GAPS FOUND

|| Count

LONGEST GAP

|| Duration

CAUSE

|| Select

🔍 Execution tip: Correlate gaps with power loss, network faults, storage failure, maintenance, or deliberate interference.

24 Confirm recording resumes correctly after restart, power interruption, or network restoration.

CRITICAL

RECOVERY TEST

Recovered

Partial recovery

Failed

RECOVERY TIME

|| Minutes

🔍 Execution tip: Use an approved controlled test where permitted and confirm cameras, recorder, time, and recording status recover fully.

5. Recorder, server, storage, and network health

25

Confirm the DVR, NVR, server, cloud recorder, and management software show a healthy operating status.

CRITICAL

SYSTEM HEALTH CHECK

Healthy

Warning

Fault

Execution tip: Review alarms, system logs, temperature, fan status, service warnings, and software health indicators.

26

Verify all installed hard drives or storage volumes are detected and operating normally.

CRITICAL

STORAGE INVENTORY

Drive / volume	Capacity	Status	Action

Execution tip: Record failed, degraded, missing, rebuilding, or unsupported drives and the effect on retention.

27

Check available storage capacity supports the required camera count, resolution, frame rate, and retention.

CRITICAL

CAPACITY CALCULATION

USED || %

FREE || %

ESTIMATED RETENTION || Days

Execution tip: Compare actual settings with the designed storage model. Higher resolution or frame rate can reduce retention unexpectedly.

28

Review recorder, server, and network logs for errors, restarts, disconnections, or unauthorized changes.

LOG REVIEW

PERIOD || Select

ERRORS || Count

CRITICAL EVENTS || Count

Execution tip: Use a defined review period and capture the event type, timestamp, affected device, and follow-up action.

29

Confirm camera network links, switches, PoE ports, and bandwidth are stable.

CRITICAL

NETWORK TEST

OFFLINE PORTS || Count

PACKET LOSS || %

Stable

Unstable

Execution tip: Check packet loss, flapping links, overloaded switches, damaged ports, and repeated camera disconnects.

30

Verify firmware, recorder software, and management applications are approved and supported.

CRITICAL

VERSION COMPLIANCE

CURRENT VERSION || Enter

APPROVED VERSION || Enter

STATUS || Select

Execution tip: Do not update during the audit unless authorized. Record obsolete, vulnerable, unsupported, or unapproved versions.

6. User access, cybersecurity, privacy, and governance

31 Confirm CCTV access is limited to authorized active users with a valid business need.

CRITICAL

USER ACCESS REVIEW

ACTIVE USERS || Count

AUTHORIZED || Count

EXCEPTIONS || Count

🔗 Execution tip: Match system accounts to current employees, roles, contractors, and approved monitoring responsibilities.

32 Verify shared, default, generic, dormant, and former-employee accounts are removed or controlled.

CRITICAL

ACCOUNT EXCEPTION CHECK

☐ No default accounts

☐ No leaver access

☐ Shared accounts controlled

☐ Dormant accounts removed

🔗 Execution tip: Default or shared credentials reduce accountability and increase the risk of unauthorized viewing or export.

33 Confirm strong passwords, multi-factor authentication, and account lockout are enabled where supported.

CRITICAL

SECURITY CONFIGURATION

Control	Supported	Enabled	Action

🔗 Execution tip: Record platform limitations separately from configuration failures and assign compensating controls where needed.

34 Review user permissions for live view, playback, export, deletion, configuration, and administration.

CRITICAL

ROLE PERMISSION MATRIX

Role	View	Export	Admin

🔗 Execution tip: Give users only the permissions required for their role. Restrict export, deletion, and configuration changes tightly.

35 Verify remote access, mobile access, and third-party monitoring connections are approved and protected.

CRITICAL

REMOTE ACCESS REVIEW

REMOTE USERS || Count

THIRD PARTIES || Count

EXCEPTIONS || Count

🔗 Execution tip: Confirm encrypted connections, approved devices, current accounts, logging, and termination of unnecessary access.

36 Confirm privacy notices, retention rules, subject-access handling, and footage disclosure procedures are current.

CRITICAL

GOVERNANCE CHECKLIST

☐ Notices displayed

☐ Retention approved

☐ Disclosure process

☐ Request log

🔗 Execution tip: Align signage, policy, retention, access, disclosure, and deletion controls with applicable law and company policy.

7. Live monitoring, alerts, and incident response

37 Confirm the live monitoring responsibility is defined for trading and non-trading hours.

RESPONSIBILITY SCHEDULE

TRADING HOURS || Select

AFTER HOURS || Select

ESCALATION || Select

🔍 Execution tip: Record who monitors, when monitoring is active, which alerts are reviewed, and the escalation contact.

38 Test camera offline, recorder fault, storage fault, tamper, and analytics alerts where configured.

CRITICAL

ALERT TEST MATRIX

Alert type	Generated	Received	Acknowledged

🔍 Execution tip: Confirm the alert is generated, received by the correct person, acknowledged, and recorded.

39 Verify monitoring screens show current images and are positioned to protect confidentiality.

CRITICAL

MONITOR INSPECTION

Compliant

Needs adjustment

Privacy risk

Add photo

🔍 Execution tip: Screens should support response without exposing footage to customers, unauthorized staff, or visitors.

40 Confirm employees know how to report suspicious activity and request CCTV review without delaying response.

KNOWLEDGE CHECK

EMPLOYEES SAMPLED || Count

CORRECT RESPONSES || Count

TRAINING GAP || Yes / no

🔍 Execution tip: Ask employees to explain the actual reporting path, urgent escalation, and information required.

41 Verify CCTV response procedures support theft, violence, missing persons, accidents, and emergency events.

CRITICAL

SCENARIO REVIEW

☐ Theft

☐ Violence

☐ Missing person

☐ Accident / emergency

🔍 Execution tip: Check the procedure covers immediate safety, camera identification, evidence preservation, communication, and escalation.

42 Review a recent incident to confirm footage was located, preserved, and escalated within the target time.

CRITICAL

INCIDENT TRACE

INCIDENT ID || Enter

RETRIEVAL TIME || Minutes

OUTCOME || Select

🔍 Execution tip: Follow the incident from report to retrieval, preservation, disclosure, action, and final closure.

8. Playback, export, evidence integrity, and disclosure

43 Confirm authorized users can locate and play footage by camera, date, and time.

CRITICAL

RETRIEVAL TEST

SAMPLE CAMERA || Select

SAMPLE TIME || Enter

RETRIEVAL TIME || Minutes

🔍 Execution tip: Use a defined sample and record the time taken to find the correct footage without external assistance.

44 Test footage export in an approved format with the required viewer or playback instructions.

CRITICAL

EXPORT TEST

Export passed

Partial

Failed

FORMAT || Enter

🔍 Execution tip: Confirm the exported file opens on an approved separate device and preserves the intended image quality.

45 Verify exported footage contains the correct camera, date, time, duration, and incident reference.

CRITICAL

EVIDENCE VERIFICATION

☐ Correct camera

☐ Correct time

☐ Correct duration

☐ Incident reference

🔍 Execution tip: Use a second-person check for material incidents to reduce the risk of exporting the wrong file or time range.

46 Confirm original footage is preserved and cannot be overwritten before an investigation or legal hold is complete.

CRITICAL

PRESERVATION CONTROL

PRESERVED BY || Select

HOLD UNTIL || Date

REFERENCE || Enter

🔍 Execution tip: Record the preservation method, owner, start date, review date, and release approval.

47 Verify exports, copies, handovers, and disclosures are logged with chain-of-custody details.

CRITICAL

CHAIN-OF-CUSTODY LOG

Date / time	Person	Action	Signature

🔍 Execution tip: Record who created, received, copied, transported, viewed, and returned or destroyed the evidence.

48 Confirm footage disclosure to police, insurers, customers, employees, or third parties follows approval rules.

CRITICAL

APPROVAL WORKFLOW

RECIPIENT || Select

APPROVED BY || Select

Record disclosure

Attach proof

🔍 Execution tip: Do not release footage informally. Link every disclosure to authorization, purpose, recipient, and retained record.

9. Power, cabling, physical protection, and maintenance

49 Confirm CCTV recorders, servers, switches, and critical cameras have approved power and backup protection.

CRITICAL

POWER PROTECTION REVIEW

UPS UNITS | Count

RUNTIME | Minutes

FAULTS | Count

🔍 Execution tip: Verify UPS coverage, surge protection, battery condition, runtime, and safe shutdown where supported.

50 Test the UPS, generator interface, or backup power according to the approved maintenance method.

CRITICAL

BACKUP POWER TEST

Pass

Partial

Fail

OBSERVED
RUNTIME | Minutes

🔍 Execution tip: Use a controlled test and confirm recording continuity, alerts, recovery, and no loss of configuration.

51 Inspect camera, recorder, switch, and monitor cabling for damage, exposure, loose connections, or tampering.

CABLE INSPECTION + PHOTO

Good

Repair needed

Tamper risk

Add photo

🔍 Execution tip: Prioritize accessible, outdoor, loading, ceiling, and back-of-house cable routes.

52 Verify recorder rooms, cabinets, and network equipment are locked, ventilated, clean, and access-controlled.

CRITICAL

ENVIRONMENT STATUS

Locked

Ventilated

Clean and
dry

Access
controlled

🔍 Execution tip: Heat, dust, moisture, pests, clutter, and unrestricted access can cause failure or evidence loss.

53 Review preventive maintenance, cleaning, inspection, and firmware schedules for completion.

MAINTENANCE SCHEDULE

TASKS DUE | Count

OVERDUE | Count

NEXT SERVICE | Date

🔍 Execution tip: Compare planned dates with completed records and escalate overdue tasks affecting critical cameras or recording.

54 Confirm every CCTV fault has a ticket, priority, owner, temporary control, target date, and closure evidence.

CRITICAL

FAULT ACTION WORKFLOW

FAULT ID | Enter

OWNER | Select

Assign action

Retest proof

🔍 Execution tip: Do not close faults based only on engineer attendance. Require a functional retest and evidence of restored recording.

10. Findings, corrective actions, review, and sign-off

55 Calculate overall CCTV compliance, camera availability, recording availability, and retention performance.

CALCULATED SCORECARD

COMPLIANCE || %

CAMERA AVAILABILITY || %

RECORDING AVAILABILITY || %

🔗 Execution tip: Report system health separately from audit compliance so management can distinguish control gaps from device faults.

56 Escalate privacy breaches, critical blind spots, total recorder failure, evidence loss, and unauthorized access immediately.

CRITICAL

CRITICAL ESCALATION

No critical issue

Critical issue open

Escalate now

🔗 Execution tip: Define who must be contacted and the maximum response time for each critical CCTV failure.

57 Confirm each material finding has containment, a named owner, priority, due date, and evidence requirement.

CRITICAL

CORRECTIVE ACTION REGISTER

Finding	Owner	Due date	Evidence

🔗 Execution tip: Use shorter deadlines for critical coverage, recording, access, privacy, and evidence-integrity failures.

58 Verify completed repairs and configuration changes were retested under normal operating conditions.

CRITICAL

RETEST + CLOSURE PROOF

Retest passed

Retest failed

Closure proof

VERIFIED BY | Select

🔗 Execution tip: Confirm live view, recording, playback, alerts, time, retention, and evidence export after the fix.

59 Schedule fault follow-up, retention verification, access review, and the next CCTV audit.

FOLLOW-UP SCHEDULE

FAULT REVIEW | Date

ACCESS REVIEW | Date

NEXT AUDIT | Date

🔗 Execution tip: Use earlier follow-up for repeat faults, temporary controls, privacy gaps, or critical cameras awaiting replacement.

60 Complete store manager and security or IT reviewer approval with timestamp.

CRITICAL

DUAL SIGNATURE + TIMESTAMP

STORE MANAGER | Sign

SECURITY / IT REVIEWER | Sign

SUBMITTED | Timestamp

🔗 Execution tip: Require the manager to acknowledge local findings and the reviewer to verify system evidence, actions, and escalation.

RUN THIS AUDIT IN TAQTICS

Turn every CCTV fault into accountable action

Schedule audits by store, enforce geo-fencing and time windows, collect approved evidence, test cameras and recording, escalate critical failures, and compare CCTV performance across locations.

Geo-fenced audits

Approved evidence

System tests

Fault actions

CCTV dashboards

Try the CCTV audit in Taqtics