RETAIL LOSS PREVENTION CHECKLIST TEMPLATE

Loss Prevention Audit Checklist

Use this template to review physical security, employee controls, POS and cash, receiving, inventory shrink, CCTV, incidents, corrective actions, and management sign-off across retail locations.

STORE / LOCATION	AUDIT TYPE	DATE AND WINDOW	AUDITOR

1. Audit setup and loss risk context

1 Confirm the correct store, audit type, date, and approved audit window. — CRITICAL — DROPDOWN + DATE + TIME

AUDIT TYPE | Routine / targeted | DATE | Select | WINDOW | Start to end

Execution tip: Activate geo-fencing and a defined audit window. Use the correct audit version so scores remain comparable across stores and periods.

2 Record current footfall, promotional activity, staffing level, and any unusual trading condition. — SELECTION + COUNT

FOOTFALL | Low / normal / high | STAFF | Count | PROMOTION | Yes / no

Execution tip: Context affects loss exposure. Record peak periods, sales events, product launches, or staffing gaps that may change normal control conditions.

3 Confirm the store manager, loss prevention contact, and security personnel on duty. — PEOPLE PICKER

STORE MANAGER | Select | LP CONTACT | Select | SECURITY | Select

Execution tip: Use named users rather than free text. This creates clear ownership when critical findings or incidents require immediate escalation.

4 Review previous audit findings, open actions, and recent loss incidents before starting the inspection. — CRITICAL — LINKED RECORDS

OPEN ACTIONS | Count | RECENT INCIDENTS | Count | LAST AUDIT | Score

Execution tip: Surface overdue actions and repeat failures at the start. Repeated gaps should receive a higher priority than isolated observations.

5 Assign the store a current loss risk level based on location, season, product mix, and recent events. — CRITICAL — RISK RATING

Low | Medium | High | Critical

Execution tip: Define risk criteria in advance. High-value stock, organized retail crime activity, seasonal peaks, and recurring shrink should influence the rating.

6 Capture arrival geo-location, timestamp, and an approved exterior reference photo. — CRITICAL — GEO + TIME + LIVE PHOTO

GEO | Verified | ARRIVAL | Timestamp | Add live photo

Execution tip: Require live capture rather than gallery upload where policy allows. This verifies that the audit occurred at the assigned store and time.

2. Exterior, entrances, exits, and physical security

7 Check exterior lighting, visibility, signage, and perimeter conditions around the store. SCORED CHECK + PHOTO

Compliant | Partial | Non-compliant | Add photo

Execution tip: Inspect dark zones, damaged lighting, hidden approaches, and signage that affects surveillance or safe employee access.

8 Verify customer entrances and emergency exits are secure, unobstructed, and monitored. CRITICAL | SCORED CHECK + COMMENT

Compliant | Partial | Non-compliant | Create action

Execution tip: Emergency exits must remain usable without becoming uncontrolled access points. Any failed lock, alarm, or obstruction should create a high-priority action.

9 Inspect doors, locks, shutters, gates, windows, and glazing for damage or tampering. CRITICAL | MULTI-SELECT + PHOTO

Locks | Shutters | Glass | Gates | Add photo

Execution tip: Capture exact location and damage type. Require closure evidence after repair and escalate any opening that cannot be secured.

10 Confirm delivery, service, and staff entrances are controlled and are not left propped open. CRITICAL | SCORED CHECK + TIMESTAMP

Compliant | Partial | Non-compliant | CHECKED | Time

Execution tip: Check during active delivery periods as well as normal trading. A door that is compliant only when no delivery is occurring can hide a recurring control failure.

11 Review parking, loading, waste, and other external high-risk areas for concealment or unauthorized access. AREA ASSESSMENT

AREA | Select | RISK | Low / medium / high | Add photo

Execution tip: Include camera coverage, lighting, access routes, abandoned packaging, and locations where stock can be passed outside.

12 Confirm alarm keypads, access devices, and security codes are protected from public view. CRITICAL | SCORED CHECK + COMMENT

Protected | Partially exposed | Exposed | Create action

Execution tip: Do not record actual codes in the audit. Record the exposure risk, affected device, and required corrective control.

3. Opening, closing, key, and access controls

13 **Verify store opening and closing procedures are completed by authorized employees.** CRITICAL | USER VERIFICATION + TIMESTAMP

OPENED BY | User | CLOSED BY | User | TIME | Timestamp

Execution tip: Match users and timestamps to the approved roster. Flag access outside scheduled hours or procedures completed by unauthorized employees.

14 **Confirm dual-person verification is used for cash, alarm, key, or high-risk access steps where required.** CRITICAL | MULTI-USER CONFIRMATION

PRIMARY USER | Select | VERIFIER | Select | STEP | Select

Execution tip: Use separate authenticated users. The same person should not be able to complete and verify a control intended to require two people.

15 **Review master key, access card, and restricted key issue and return records.** CRITICAL | DYNAMIC KEY LOG

KEY / CARD | ID | ISSUED TO | User | RETURNED | Time

Execution tip: Record unique key or card IDs, custody changes, missing items, and overdue returns. Missing master access should trigger immediate escalation.

16 **Compare alarm activation and deactivation records with authorized users and expected times.** CRITICAL | SYSTEM LOG COMPARISON

ALARM EVENT | Time | USER | Authorized | VARIANCE | Minutes

Execution tip: Integrate or attach alarm logs where possible. Investigate unexplained early entry, late exit, repeated failed codes, or shared credentials.

17 **Check stockrooms, offices, cash rooms, server rooms, and restricted doors remain locked when not in active use.** CRITICAL | ZONE CHECKLIST

☐ Stockroom ☐ Office ☐ Cash room ☐ Server room

Execution tip: Make photo evidence mandatory for failed restricted-area controls. Assign each gap to the store manager or facilities owner with a short closure window.

18 **Confirm the final security sweep and end-of-day sign-off are completed before the last employee leaves.** CRITICAL | CHECKLIST + SIGNATURE

SWEEP | Complete | LAST EXIT | Timestamp | MANAGER | Sign

Execution tip: Include toilets, fitting rooms, stockrooms, offices, external doors, cash areas, and any zone that could conceal a person or unsecured stock.

4. Employee access, conduct, and internal theft controls

19 Verify employee entrances and restricted work areas are controlled by authorized access. CRITICAL ACCESS CHECK + PHOTO

Controlled | Partial | Uncontrolled | Add photo

Execution tip: Review tailgating, shared cards, blocked readers, propped doors, and temporary staff access. Record the affected shift and access point.

20 Check bags, personal belongings, lockers, and mobile devices are managed according to company policy. POLICY CHECKLIST

☐ Bags stored ☐ Lockers used ☐ Device rule EXCEPTION | Comment

Execution tip: Apply the policy consistently and respectfully. Record exceptions without collecting unnecessary personal information.

21 Review employee purchases, discounts, holds, returns, and exchanges for authorization and documentation. CRITICAL TRANSACTION SAMPLE GRID

SAMPLE SIZE | Count EXCEPTIONS | Count APPROVAL | Verified

Execution tip: Sample transactions across employees, shifts, and supervisors. Check approval, receipt, item movement, and any unusual timing or discount pattern.

22 Confirm employees use individual POS logins and do not share till credentials. CRITICAL USER ACCESS REVIEW

USERS SAMPLED | Count SHARED ACCESS | Yes / no Create action

Execution tip: Compare active sessions to the roster. Shared credentials weaken accountability and should be corrected immediately.

23 Check controls preventing unauthorized consumption, use, gifting, or removal of stock and supplies. CRITICAL SCORED CHECK + EVIDENCE

Effective | Partial | Ineffective EVIDENCE | Reference

Execution tip: Include samples, testers, damaged items, staff meals, packaging, consumables, and merchandise reserved without authorization.

24 Record suspicious conduct, policy exceptions, or conflicts of interest requiring review. CRITICAL CONFIDENTIAL INCIDENT NOTE

CATEGORY | Select SEVERITY | Select ESCALATE TO | LP / HR

Execution tip: Limit access to sensitive findings. Record facts, dates, transaction references, and observable behaviour without making unsupported accusations.

5. POS, cash, refund, discount, and transaction controls

25 Verify the opening till float is counted, recorded, and acknowledged by authorized employees.

CRITICAL | CASH COUNT + DUAL SIGN-OFF

EXPECTED | Amount | ACTUAL | Amount | VARIANCE | Amount | VERIFIER | User

Execution tip: Use numeric validation and require a reason for any variance. Do not allow submission until the opening difference is resolved or escalated.

26 Compare physical cash to the POS or safe balance and record any variance.

CRITICAL | NUMERIC VALIDATION

SYSTEM BALANCE | Amount | CASH COUNTED | Amount | VARIANCE | Calculated

Execution tip: Set the accepted tolerance by policy. Variances outside tolerance should create an immediate corrective action and notify finance or loss prevention.

27 Sample refunds, voids, cancellations, and price overrides for approval and supporting evidence.

CRITICAL | TRANSACTION SAMPLE GRID

TRANSACTION | ID | TYPE | Select | APPROVAL | Verified | EVIDENCE | Receipt / comment

Execution tip: Prioritize transactions completed near closing, by supervisors, without customers present, or repeatedly by the same user.

28 Check manual discounts, coupons, promotions, and price changes follow approved rules.

CRITICAL | SCORED CHECK + SAMPLE COUNT

SAMPLES | Count | EXCEPTIONS | Count | Compliant | Non-compliant

Execution tip: Compare the applied discount to the approved offer and authorization level. Require comments for overrides and expired promotions.

29 Review no-sale drawer openings, paid-outs, cash drops, and cash movements.

CRITICAL | EXCEPTION LOG REVIEW

NO-SALE OPENS | Count | CASH DROPS | Count | UNEXPLAINED | Count

Execution tip: Trend activity by user, time, and till. Repeated unexplained drawer access or delayed cash drops should be escalated.

30 Verify gift cards, store credits, loyalty points, and other cash-equivalent transactions are controlled.

CRITICAL | TRANSACTION CONTROL CHECK

☐ Activation ☐ Redemption ☐ Balance change ☐ Approval

Execution tip: Check unusual activations, reversals, manual balance adjustments, and transactions linked to employee or related accounts.

6. Receiving, stockroom, transfers, and inventory shrink controls

31 Match incoming deliveries to purchase orders or advance shipment records before acceptance.

CRITICAL | DOCUMENT MATCH + COUNT

PO / ASN | Reference | EXPECTED UNITS | Count | RECEIVED UNITS | Count

Execution tip: Count before signing acceptance. Record seal condition, delivery time, driver details, and any variance at the point of receipt.

32 Record shortages, overages, damage, and tampering with supporting evidence.

CRITICAL | VARIANCE GRID + LIVE PHOTO

SKU | ID | VARIANCE | Quantity | REASON | Select | Add photo

Execution tip: Capture packaging, seal, and product condition before stock is moved. Assign follow-up to receiving, vendor, or distribution teams.

33 Confirm receiving zones, cages, stockrooms, and high-value storage have restricted access.

CRITICAL | ZONE ACCESS CHECK

☐ Receiving ☐ Stockroom ☐ Cage ☐ High-value area

Execution tip: Review access lists and actual behaviour. Temporary and vendor access should be time-bound, supervised, and recorded.

34 Verify high-value, fast-moving, or theft-prone stock is stored under enhanced controls.

CRITICAL | CATEGORY CONTROL CHECK

CATEGORY | Select | CONTROL | Select | QUANTITY | Count | Add photo

Execution tip: Define enhanced controls by category, such as locked storage, serial tracking, daily counts, restricted access, or dual verification.

35 Review transfers, returns to vendor, write-offs, disposals, and stock adjustments for traceability.

CRITICAL | MOVEMENT SAMPLE GRID

MOVEMENT | Type | REFERENCE | ID | APPROVAL | Verified | DESTINATION | Recorded

Execution tip: Follow the item from system entry to physical destination. Require reason codes, approvals, evidence, and separation of duties.

36 Compare cycle count results to system stock and investigate material variances.

CRITICAL | COUNT + VARIANCE + ACTION

SKU / CATEGORY | Select | SYSTEM | Count | PHYSICAL | Count | Investigate

Execution tip: Set variance thresholds by value and risk. Repeat variances should trigger root-cause review rather than repeated stock adjustment alone.

7. Sales floor, high-value stock, fitting rooms, and theft deterrence

37 Verify high-value products are displayed and secured according to the approved control plan. CRITICAL | PLAN CHECK + PHOTO

CATEGORY | Select | FIXTURE | Select | Compliant | Add photo

Execution tip: Check locks, tethers, cabinets, display quantity limits, dummy units, and staff-controlled access for each high-risk category.

38 Check EAS, RFID, or other security tags are applied correctly and remain active until purchase. CRITICAL | TAG SAMPLE COUNT

ITEMS SAMPLED | Count | MISSING TAGS | Count | INACTIVE TAGS | Count

Execution tip: Sample different products and price bands. Missing or incorrectly placed tags should be corrected before the audit is closed.

39 Assess blind spots, concealed zones, shelf layouts, and fixture placement that could increase theft risk. RISK MAP + PHOTO

ZONE | Select | RISK | Low / medium / high | Add photo

Execution tip: Include camera visibility, staff sightlines, tall fixtures, promotional stacks, corners, and customer routes to exits.

40 Verify fitting room entry, item counts, occupancy monitoring, and recovery checks follow policy. CRITICAL | COUNT + TIMESTAMP

ROOMS CHECKED | Count | COUNT CONTROL | Verified | LAST RECOVERY | Time

Execution tip: Check abandoned tags, empty packaging, hidden items, and unresolved count differences. Escalate repeated findings by room or shift.

41 Confirm customer service coverage is sufficient in high-risk zones and during peak periods. COVERAGE ASSESSMENT

ZONE | Select | STAFF ASSIGNED | Count | COVERAGE GAP | Minutes

Execution tip: Use staffing schedules and observed coverage. Long unattended periods in high-risk zones should create a staffing or deployment action.

42 Log empty packaging, tampered products, concealed merchandise, or other suspected theft indicators. CRITICAL | FINDING GRID + EVIDENCE

LOCATION | Select | ITEM / SKU | Reference | INDICATOR | Select | Add photo

Execution tip: Preserve evidence and record the exact location, time, product, and condition. Do not confront customers based only on an audit finding.

8. CCTV, alarms, EAS, and security system readiness

43 **Verify cameras are operational, recording, correctly timed, and free from obstruction.**

CRITICAL | SYSTEM CHECK + TIMESTAMP

CAMERAS TESTED	OFFLINE	CLOCK CORRECT
Count	Count	Yes / no

Execution tip: Test representative views, not only the monitor display. Record blind, blocked, blurred, or incorrectly aimed cameras by ID.

44 **Confirm CCTV retention, export, and user access controls meet company requirements.**

CRITICAL | SYSTEM CONFIGURATION REVIEW

RETENTION	EXPORT TEST	AUTHORIZED USERS
Days	Pass / fail	Count

Execution tip: Do not expose sensitive footage in the checklist. Record configuration status, access exceptions, and the owner responsible for correction.

45 **Test EAS pedestals or theft alarms and verify the expected response procedure.**

CRITICAL | LIVE TEST + RESPONSE TIME

TEST RESULT	RESPONSE	RESPONDER
Pass / fail	Seconds	User

Execution tip: Perform an approved test without disrupting customers. Record alarm audibility, employee response, reset, and any false alarm issue.

46 **Verify intrusion, panic, duress, and other security alarm status or scheduled test records.**

CRITICAL | ALARM STATUS CHECKLIST

- ☐ Intrusion
- ☐ Panic
- ☐ Duress
- ☐ Monitoring link

Execution tip: Follow approved test procedures. Failed life-safety or duress systems require immediate escalation and temporary risk controls.

47 **Check radios, phones, panic devices, and emergency communication tools are available and charged.**

EQUIPMENT COUNT + STATUS

DEVICE TYPE	AVAILABLE	WORKING
Select	Count	Count

Execution tip: Confirm devices are assigned to the correct roles and can reach store management, security, and emergency contacts.

48 **Confirm incident forms, evidence storage, emergency contacts, and response instructions are available.**

READINESS CHECKLIST

- ☐ Incident forms
- ☐ Evidence storage
- ☐ Contacts
- ☐ Instructions

Execution tip: Keep current versions accessible to authorized staff. Outdated contact lists or uncontrolled evidence storage can delay response and weaken investigations.

9. Incident handling, evidence, safety, and compliance

49 **Verify incidents are reported promptly with factual details, timestamps, and involved roles.**

CRITICAL | INCIDENT RECORD REVIEW

INCIDENT ID | Reference | REPORTED AFTER | Minutes | REQUIRED FIELDS | Complete

Execution tip: Use factual observations and system records. Avoid unsupported conclusions, emotional language, or unnecessary personal information.

50 **Check video, photos, receipts, statements, and other evidence are retained and access-controlled.**

CRITICAL | EVIDENCE CHAIN LOG

EVIDENCE TYPE | Select | STORED AT | Reference | ACCESS OWNER | User

Execution tip: Maintain chain of custody, retention dates, and restricted access. Do not attach sensitive evidence where the checklist audience is too broad.

51 **Confirm suspected theft response follows the approved safe, non-confrontational procedure.**

CRITICAL | SCENARIO CHECK + COMMENT

Procedure followed | Partial | Not followed | COMMENT | Required

Execution tip: Employee and customer safety takes priority. Audit observation, notification, monitoring, and escalation steps without encouraging unsafe intervention.

52 **Verify escalation to security, police, insurer, legal, or regional management follows defined criteria.**

CRITICAL | ESCALATION MATRIX CHECK

TRIGGER | Select | ESCALATED TO | Select | TIME | Timestamp

Execution tip: Define thresholds by incident type and value. Critical incidents should automatically notify the correct people and track acknowledgment.

53 **Review known-offender, exclusion, or trespass information for currency and lawful use.**

CRITICAL | RESTRICTED RECORD REVIEW

RECORD STATUS | Current / outdated | ACCESS | Authorized | REVIEW DATE | Date

Execution tip: Restrict access and follow local law and company policy. Do not include sensitive identity details in widely visible audit comments.

54 **Check privacy notices, CCTV signage, data access, and information handling follow policy.**

CRITICAL | COMPLIANCE CHECK

☐ CCTV notice | ☐ Privacy notice | ☐ Access control | ☐ Retention

Execution tip: Review the visible notice and actual practice. Escalate missing signage, excessive access, or retention outside approved limits.

55 **Confirm incident-related corrective actions have owners, priorities, due dates, and closure evidence.**

CRITICAL | ACTION TRACKER

OPEN ACTIONS | Count | OVERDUE | Count | CRITICAL | Count | Review actions

Execution tip: Escalate overdue critical actions. Closure should require evidence that the control was restored, not only a comment saying the action is complete.

10. Overall risk, corrective action, and management sign-off

56 Rate overall loss prevention control effectiveness across people, process, inventory, cash, and security systems.

CRITICAL | WEIGHTED RATING

PEOPLE | 1 to 5 | PROCESS | 1 to 5 | INVENTORY | 1 to 5 | SECURITY | 1 to 5

Execution tip: Keep category ratings separate before calculating the overall score. Critical failures should cap or override the final result.

57 Record the three highest loss risks identified and their likely business impact.

CRITICAL | PRIORITY RISK GRID

RISK | Describe | LIKELIHOOD | Select | IMPACT | Value / safety / compliance

Execution tip: Prioritize by likelihood, financial exposure, customer or employee safety, repeat occurrence, and ability to exploit the gap.

58 Create a corrective action plan with owner, priority, due date, evidence, and escalation path.

CRITICAL | CORRECTIVE ACTION WORKFLOW

OWNER | Select | PRIORITY | Select | DUE | Date / time | Closure proof

Execution tip: Assign actions to roles with authority to close them. Use shorter deadlines and automatic escalation for controls that expose cash, stock, people, or data.

59 Confirm all immediate critical risks are contained before the audit is closed.

CRITICAL | CRITICAL CLOSURE CHECK

Contained | Temporary control | Open risk | Escalate

Execution tip: Do not close the audit with an uncontrolled critical risk. Record the temporary control, accountable owner, and next review time when permanent repair is pending.

60 Complete store manager and regional or loss prevention reviewer approval with timestamp.

CRITICAL | DUAL SIGNATURE + TIMESTAMP

STORE MANAGER | Sign | LP REVIEWER | Sign | SUBMITTED | Timestamp

Execution tip: Require the manager to acknowledge findings and the reviewer to verify evidence, scoring, action ownership, and escalation before final submission.

RUN THIS AUDIT IN TAQTICS

Turn every loss prevention finding into accountable action

Schedule audits by store, enforce geo-fencing and time windows, collect live evidence, create critical actions, escalate overdue risks, and compare control performance across locations.

Try the loss prevention audit in Taqtics

Geo-fenced audits | Live evidence | Critical actions | Escalations | Risk dashboards