hicomply

The Ultimate Audit Readiness Checklist

Stop Scrambling. Stay Ready. Walk Into Every Audit With Confidence.

Stop Scrambling. Stay Ready. Walk Into Every Audit With Confidence.

Audit readiness isn't something you achieve in the final weeks before an auditor arrives. It's a state you maintain. The organisations that consistently produce clean audit results aren't the ones who prepare hardest at the last minute — they're the ones who treat readiness as an operational discipline year-round. This checklist covers every area auditors examine — from documentation and internal controls to risk management and process compliance — so you can confirm your programme is genuinely ready, not just assembled under pressure.

Step 1

Documentation and Records

- [ ] **Financial statements and closing balances** – Must be current, reconciled, and accessible without requiring manual effort to locate or compile.
- [ ] **Bank statements and VAT returns** – Should be up to date and held in a centralised, secure repository — not distributed across inboxes or shared drives.
- [ ] **Significant transaction documentation** – Supporting documentation and clear audit trails must exist for all significant transactions and related party transactions.
- [ ] **Accounting policies** – Must be documented, consistently applied, and reflect actual practice — not an aspirational version written at implementation and never revisited.

What Good Looks Like

Every document an auditor might request can be produced in minutes, not days. If locating current financial records requires a search across systems, inboxes, or individuals, that's a documentation gap — not a documentation programme.

15% completed

Step 2

Internal Controls

- [ ] **Named control owners** – Every control must have a named individual responsible for it — not a team or job title. Accountability without a name is accountability that's easy to avoid.
- [ ] **Controls reviewed within 12 months** – Each control must have been formally reviewed and updated within the last year, with documented evidence of that review.
- [ ] **Evidence covers the full audit period** – Control operation must be evidenced across the entire audit window — not just recent activity assembled before the audit began.
- [ ] **Segregation of duties in place** – Financial processes must have appropriate separation of duties, and system access controls must reflect current, authorised requirements only.

What Good Looks Like

A well-controlled organisation can demonstrate not just that controls exist, but that they have been operating consistently throughout the audit period. If your evidence only covers the last few weeks, auditors will notice — and it will show in the report.

30% completed

Step 3

Risk Management

- [ ] **Risk register reviewed within 90 days** – Management must have formally reviewed and approved the register within the last 90 days — not updated once at certification and left untouched.
- [ ] **New risks captured as they arise** – Emerging risks from operational changes, new regulatory requirements, or evolving threats must be recorded as they occur, not accumulated pre-audit.
- [ ] **Treatment plans tracked to completion** – Risk mitigating actions must be actively tracked, with documented evidence that treatments have been implemented and tested.
- [ ] **Management sign-off documented** – Formal approval of the current risk register must be on record and available for auditor review without additional preparation.

What Good Looks Like

Auditors are not looking for a static document produced for audit purposes. They want evidence of ongoing risk management — that your organisation has been identifying, assessing, and treating risks as a continuous discipline, not a pre-audit exercise.

45% completed

Step 4

Process and Compliance

- [ ] **Process notes reflect current practice** – Documentation must describe how work actually happens today — not how it was designed to happen when procedures were first written.
- [ ] **Compliance obligations actively tracked** – Regulatory requirements must be evidenced continuously, with no reliance on individual memory or informal processes.
- [ ] **Previous findings formally closed** – Findings from past audit cycles must have documented evidence of remediation — not noted and filed away.
- [ ] **Framework obligations mapped to controls** – Requirements for relevant frameworks (ISO 27001, SOC 2, statutory audit) must be mapped to current controls with supporting evidence in place.

What Good Looks Like

The most avoidable audit findings arise when documentation describes aspiration rather than practice. If written procedures have drifted from what the team actually does, auditors will find it. Regular reviews that confirm documentation reflects current operations close that gap before it becomes a finding.

60% completed

Step 5

Readiness and Communication

- [ ] **Designated auditor point of contact** – A single named individual must be responsible for managing the audit relationship and routing queries to the right people.
- [ ] **Team roles clearly understood** – Internal team members must know what controls they own, what evidence they're responsible for, and what to do when something changes.
- [ ] **Post-audit debrief process in place** – A structured process must exist to capture learnings from each audit cycle and feed improvements into the next.
- [ ] **Compliance training evidenced** – Employees with compliance responsibilities must have completed relevant training, with records available on request.

What Good Looks Like

Audit friction is rarely about the controls themselves — it's about communication, routing, and readiness. A single, well-briefed point of contact and a team that understands its responsibilities removes the organisational drag that slows audits down and generates avoidable findings.

75% completed

Step 6

Continuous Compliance Programme

- [ ] **Evidence captured continuously, not assembled retrospectively before the audit.**
- [ ] **Key controls monitored regularly, with pass/fail visibility and drift alerts.**
- [ ] **Audit-ready status reports producible in minutes, not compiled manually on request.**
- [ ] **Structured internal audits operating on a regular cadence, with documented outcomes.**
- [ ] **Evidence covers the full observation window, not just the weeks before the audit.**
- [ ] **Past audit findings confirmed closed, with documented evidence of remediation.**
- [ ] **Compliance posture visible at any point, not only when an audit is approaching.**
- [ ] **Risk register, policies, controls evidence, and audit workflows held in one place.**
- [ ] **Review cycles enforced by process, not reliant on individuals remembering.**
- [ ] **Evidence mapped once and available across all applicable audit requirements.**
- [ ] **Post-audit reviews identify what worked, what didn't, and what changes next time.**

What Good Looks Like

👍 Always audit-ready isn't a sprint you run before each audit — it's a state you maintain. Organisations that achieve it aren't working harder. They're doing the same work at a different point in time, with systems that make continuous compliance the path of least resistance.

100% completed

Walk Into Every Audit Already Prepared.

By working through this **checklist**, you're not just preparing for the next audit — you're building a compliance programme designed to stay ready year-round.

Ready to make audit readiness a baseline, not a crisis?

Hicomply centralises your **controls**, **evidence**, **risk register**, and **internal audit workflows** in one platform — so your programme is continuously maintained, not periodically assembled. When an auditor arrives, you're pulling from a structured, timestamped record that covers the full audit period. No scramble. No gaps. Just a programme that was ready before the date was confirmed.