ZenGRC

ZenGRC Simply Powerful GRC

CHECKLIST · AUDIT READINESS

Get Audit-Ready in 90 Days

A week-by-week, phase-by-phase checklist for security and compliance teams preparing for SOC 2, ISO 27001, HIPAA, PCI, NIST, and beyond.

Format
5-Phase Checklist

Duration
90 Days

Published
2026 · ZenGRC

1 Discovery
Days 1–14

2 Evidence Collection
Days 15–42

3 Gap Remediation
Days 43–63

4 Pre-Audit Review
Days 64–80

5 Audit Week
Days 81–90

ZenGRC Simply Powerful GRC

ZenGRC

PHASE 1

Discovery

Days 1–14 · Know where you stand

- [ ] **Identify all frameworks in scope**
  List every framework your organization must address: SOC 2, ISO 27001, HIPAA, HITRUST, PCI, NIST, CMMC.

- [ ] **Map current control coverage**
  Document controls currently in place. Identify gaps between your current state and framework requirements.

- [ ] **Inventory evidence sources**
  List every system generating evidence: cloud providers, ticketing systems, HR platforms, and identity tools.

- [ ] **Assign control owners**
  Every control needs a named owner responsible for evidence collection and auditor responses.

- [ ] **Review last audit findings**
  Pull prior findings and observations. Confirm each one has been fully remediated before moving forward.

PHASE 2

Evidence Collection

Days 15–42 · Gather and organize

- [ ] **Set up automated evidence collection**
  Connect your GRC platform to cloud environments, Jira, ServiceNow, and identity tools. Schedule recurring pulls.

- [ ] **Collect manual evidence artifacts**
  Screenshots, policies, training records, and meeting minutes — store everything centrally in your GRC platform.

- [ ] **Map evidence to controls**
  Every control needs at least one evidence artifact. Cross-framework evidence should be mapped everywhere it applies.

- [ ] **Validate evidence currency**
  Check dates on all artifacts. Auditors reject stale evidence — replace anything older than the audit period.

- [ ] **Run evidence gap report**
  Identify controls with no supporting evidence. Prioritize by risk level and framework criticality.

PHASE 3

Gap Remediation

Days 43–63 · Fix what is missing

- [ ] **Remediate high-risk gaps first**
  Sort gaps by risk impact and auditor scrutiny likelihood. Address findings before observations.
- [ ] **Update or create missing policies**
  If a control exists but lacks a supporting policy, write it. Auditors require documentation for every control.
- [ ] **Implement missing technical controls**
  MFA, encryption, logging, access reviews — this phase is your window to close technical gaps before audit.
- [ ] **Document compensating controls**
  If a control cannot be implemented, formally document the compensating alternative and its rationale.

PHASE 4

Pre-Audit Review

Days 64–80 · Rehearse before showtime

- [ ] **Run internal readiness assessment**
  Walk through every control as the auditor would. You should be able to locate any evidence artifact in under 60 seconds.

- [ ] **Brief control owners**
  Everyone who will interact with auditors must know exactly what they own and where their evidence lives.

- [ ] **Test evidence exports and reports**
  Generate the reports auditors will request. Confirm they are complete, accurate, and properly formatted.

- [ ] **Prepare walkthrough package**
  Map each control to its evidence, owner, and testing method. This becomes your master audit guide.

PHASE 5

Audit Week

Days 81–90 · Execute with confidence

- [ ] **Set up auditor access**
  Provide read-only access to your GRC platform so auditors can pull evidence directly — minimizing back-and-forth.

- [ ] **Designate a single point of contact**
  One person manages all auditor requests and routes them to the appropriate control owner. Avoid communication chaos.

- [ ] **Track requests in real-time**
  Log every auditor request, its current status, and resolution. Nothing falls through the cracks.

- [ ] **Address findings immediately**
  If an auditor surfaces a finding during fieldwork, begin remediation before the final report is issued.

ZenGRC

ZenGRC Simply Powerful GRC

3 weeks → 3 days

ZenGRC Automates the Heavy Lifting

ZenGRC automates evidence collection, maps controls across frameworks, and gives your auditor direct read-only access. Your team manages compliance. The platform handles the evidence.

Request a Demo →

zengrc.com/demo