ITEO

AUDIT PREP CHECKLIST

Make audit readiness part of your leadership rhythm — not a last-minute scramble.

presented by

AGILE TECH ADVISORS

DIRECTING STRATEGY. OPTIMIZING ECOSYSTEMS.

ITEO Audit Prep Checklist

Make audit readiness part of your leadership rhythm — not a last-minute scramble.

This checklist covers the documentation, processes, and leadership sign-offs auditors look for — plus the behavioral checks that prove controls live in practice, not just on paper. Score each item by evidence quality and note its severity, then re-run it on a standing cadence so readiness never depends on a scramble.

ORGANIZATION	AUDIT / REVIEW TYPE	REVIEW DATE

ACCOUNTABLE LEADER

How to score each item

0 = Not documented.
1 = Documented, but not tested.
2 = Tested, but owner unclear.
3 = Owner-confirmed and reviewed on cadence.

Severity: HIGH MED LOW
HIGH = board, regulatory, customer, or continuity exposure.
MED = important but contained; localized or recoverable impact.
LOW = minor; little exposure if it slips.

Data Governance	EVIDENCE STATE (0-3)	SEVERITY
Data ownership is assigned, with a named owner for each critical data domain.		HIGH
Access controls and permissions are documented and reviewed on a schedule.		HIGH
Retention, classification, and disposal policies exist and are followed in practice.		MED
Data handling for regulated records meets the applicable standard for your sector. Insurance, legal, and healthcare records each carry their own requirements.		HIGH

Vendor Contracts	EVIDENCE STATE (0-3)	SEVERITY
Every vendor has a current contract on file with a named business owner.		MED
Vendor security and compliance attestations are verified — not just collected. Checklists from vendors foster false confidence; verify rather than trust.		HIGH
Vendor risk exposure has been mapped (see the Vendor Mapping Template).		MED
Exit and continuity plans exist for critical vendors.		HIGH

Intake & Process Protocols	EVIDENCE STATE (0-3)	SEVERITY
Intake processes for new requests, systems, and vendors are documented.		MED
Every active project has a business sponsor accountable for results.		MED
A clear process exists to identify and retire shadow IT.		HIGH
Change and approval workflows are recorded with decision points and owners.		LOW

Leadership Sign-offs & Documentation	EVIDENCE STATE (0-3)	SEVERITY
Required leadership approvals are documented and accessible.		MED
Policy reviews are scheduled — and actually executed, not just calendared. A common failure: reviews scheduled but never performed.		HIGH
Each critical control has a named owner and a stated business outcome.		HIGH

Leadership Sign-offs & Documentation	EVIDENCE STATE (0-3)	SEVERITY
Cross-functional sign-offs are documented, not assumed.		LOW
Governance / steering meetings are held on schedule, with logged decisions.		MED
Risk owners remain in their assigned roles (no orphaned controls).		HIGH
Overdue reviews, missing owners, and stale policies are tracked openly. A simple red-flag register surfaces reviews that have quietly lapsed.		HIGH
At least one recovery or incident simulation has been run recently.		LOW

From Checklist to Leadership Action

From Checklist to Leadership Action

Escalation rule — what goes straight to the leadership agenda

Some gaps cannot wait for the next review cycle. Any of the following must be placed on the leadership agenda at the next meeting:

- ! Any control without a named owner.
- ! Any vendor without a documented exit plan.
- ! Any review overdue by more than 30 days.

Audit readiness is a leadership function. Escalation is how it stays one.

Your scramble risk score

A quick, deliberately rough signal of how fragile your readiness is right now. You do not need precision — you need to see the number move toward zero over time. Add up:

Items scored 0 or 1 (not documented / not tested) +

Controls missing an owner +

Reviews overdue by 30+ days +

= Scramble risk score

SCRAMBLE RISK SCORE

Higher means more of your readiness depends on heroics. Track it each cycle and drive it down.

READINESS SIGN-OFF

Reviewed by		Date	
Next review date			
Open items / follow-ups			
Accountable owner for open items			

Compliance Reporting Matrix

Map where compliance intersects governance, vendors, and operations — and who reports what, when.

Before you fill it in — four questions for regulated firms

If you operate in financial services, insurance, or another regulated sector, make sure you can answer these before an auditor asks. Each maps to rows you should have in the matrix below:

- ☐ Can you produce a current list of critical systems and their owners?
- ☐ Can you show who owns access review for customer, account, lending, investment, or claims data?
- ☐ Can you identify which vendors touch regulated data?
- ☐ Can you show the last review date for each critical vendor?

The matrix — one row per control or requirement

Control / Requirement	Owner	Intersects (Gov / Vendor /Ops)	Report To	Frequency	Status
EXAMPLE Vendor access review	J. Okafor (Risk)	Vendor + Operations	Risk Committee	Quarterly	AMBER

Status: use Green (current), Amber (attention needed), or Red (overdue / no owner) so the table reads at a glance.

What your result means

If more than three controls lack clear owners or current evidence, your audit readiness depends on heroics, not governance. That is a leadership problem, not a paperwork one — and itis fixable. Assign the owners, set the cadence, and watch your scramble risk score fall.