Finance Audit Policy and Scope

Purpose

This policy defines how Finance Internal Audit plans, executes, and reports audits over finance processes, ensuring compliance, control effectiveness, and risk reduction. It applies to all finance teams, systems, and critical third?party providers.

Objectives

- Confirm accuracy and integrity of financial records and reporting.
- Validate compliance with internal policies and external regulations.
- Evaluate design and operating effectiveness of key controls.
- Identify opportunities to improve efficiency and reduce risk.

Governance

- Audit Committee approves the annual audit plan and receives all final reports.
- Finance Internal Audit reports administratively to the CFO and functionally to the Audit Committee.
- Independence is maintained by prohibiting auditors from designing or operating controls they audit.

Audit Universe and Scope

- Core Finance: AP, AR, GL close, fixed assets, treasury, tax, payroll interfaces.
- Supporting Systems: ERP configuration, access controls, change management.
- Third Parties: critical finance BPOs, payment processors, and key vendors.

In/Out of Scope Examples

In Scope	Out of Scope
Invoice approval workflow, payment runs	Sales forecasting assumptions
Month?end close and reconciliation	Product pricing decisions
User access provisioning and reviews	Marketing spend optimization

Risk Rating Method

Risk Score = Likelihood (1-5) x Impact (1-5). Coverage % = (Audited entities / total entities) x 100.

Likelihood	Definition
1	Rare: not expected in 5 years
3	Possible: may occur in 2-3 years
5	Almost Certain: likely within 12 months

Impact	Definition

1	Low: < $50k or minimal regulatory impact
3	Moderate: $50k-$250k or reportable issue
5	High: > $250k or significant regulatory exposure

Annual Planning Inputs

- Risk assessment results and prior audit issues.
- Financial statement materiality and critical accounts.
- System changes, mergers, or new vendors.
- Regulatory or policy updates affecting finance processes.

Roles and Responsibilities

Role	Key Responsibilities
Audit Committee	Approve plan, review high-risk findings, monitor remediation
CFO	Ensure resources, remove blockers, sponsor remediation
Audit Manager	Plan audits, review workpapers, issue reports
Process Owners	Provide evidence, respond to findings, remediate

Evidence Standards

- Evidence must be sufficient, reliable, relevant, and traceable.
- Sampling follows documented methodology and is reproducible.
- All conclusions are supported by workpapers and control test results.

Confidentiality and Data Handling

Audit materials may include sensitive payroll, vendor, and banking data. Access is restricted and data is encrypted at rest. External sharing requires Audit Committee approval.

Document Control

All audit artifacts are stored in the audit repository for 7 years. Access is restricted to Audit and Compliance staff.

Policy Exceptions

Exceptions to this policy require documented justification and Audit Committee approval before execution.

Audit Frequency Guidelines

Process Risk Tier	Typical Frequency	Examples
Tier 1 (High)	Annually	Treasury, Revenue Recognition
Tier 2 (Medium)	Every 2 years	AP, Fixed Assets
Tier 3 (Low)	Every 3 years	Travel & Expense

Key Performance Indicators

- Plan Coverage % = Audited entities / total entities.

- Finding Closure % = Closed findings / total findings.

- Average Remediation Age = Sum of days open / number of findings.

Training Requirements

Audit staff complete annual training on fraud awareness, data privacy, and updated accounting standards.

Version History

Version	Date	Description
1.0	2025-01-10	Initial policy release
1.1	2026-02-01	Updated scope for new treasury platform