University of Alabama System®

THE UNIVERSITY OF ALABAMA
THE UNIVERSITY OF ALABAMA AT BIRMINGHAM
THE UNIVERSITY OF ALABAMA IN HUNTSVILLE
THE UAB HEALTH SYSTEM

Internal Control Checklist

Office of Internal Audit

Revised May 2026

Purpose and Use of This Checklist

This checklist is a tool to support management's implementation and evaluation of internal controls as described in *Understanding Internal Controls (Revised – 2026)*. It is not intended to be exhaustive and should be applied using a risk-based approach.

"Yes/No/Not Applicable" responses should trigger discussion and consideration of whether compensating or automated controls exist. Departments should focus more attention on high-risk areas, significant financial activity, sensitive data (including PHI), regulated activities, and automated or AI-enabled processes.

Yes / No / N/A

Control Environment (Applies to All Areas)

- Management communicates and demonstrates expectations regarding integrity, ethics, and compliance.
- Roles, responsibilities, and accountability are clearly defined and documented.
- Employees have the knowledge, training, and resources needed to perform their duties.
- Required compliance, privacy, cybersecurity, and safety training is completed timely.
- Conflicts of interest and outside activities are disclosed and managed in accordance with policy.
- Exceptions to policy are infrequent, approved, documented, and monitored.
- Procedures exist for reporting suspected misconduct, compliance concerns, or control failures.
- Disaster response and continuity plans address loss of systems, vendors, and key personnel.

Management Oversight

- Monthly or periodic financial and operational reports are reviewed for reasonableness and trends.
- Significant variances or anomalies are investigated, resolved, and documented.
- Account reconciliations and key control activities are completed and reviewed timely.
- Oversight activities are documented (e.g., sign-offs, dashboards, review notes).
- Access reviews for critical systems are performed periodically.

Assets (Physical, Financial, and Digital)

Authorization and Approval

- Asset purchases are approved by appropriate management.
- System access is formally approved using role-based criteria.
- Unique user credentials and approved authentication methods are used (no shared credentials).

Documentation and Monitoring

- Assets are recorded timely and accurately in inventory or financial systems.
- Physical inventories or validation procedures are performed periodically.
- Discrepancies are investigated and resolved.
- Suspected theft, loss, or misuse is reported promptly.

Safeguarding

- High-risk or portable assets are secured when not in use.
- Cloud-hosted assets and data are protected through configuration, access controls, and monitoring.

Cash, Receipts, and Revenue (Including Clinical and Student Receivables)

Authorization and Approval

- Collection points, banking arrangements, and receivable processes are formally approved.
- Automated billing, charge capture, or coding tools are approved and documented.

Documentation and Monitoring

- Receipts are generated through approved systems (electronic or point-of-sale).
- Deposits are made timely and intact.
- Overages, shortages, cancellations, and adjustments are documented and reviewed.
- Accounts receivable aging and follow-up procedures are performed.

Reconciliation and Segregation of Duties

- Receipts, deposits, and receivables are reconciled to financial records.

- Individuals handling cash or receipts do not perform reconciliations.
- Compensating controls exist where full segregation is not feasible.

Disbursements and Expenditures

Authorization and Approval

- Purchases, contracts, and disbursements are approved by appropriate personnel prior to commitment.
- Approval workflows rely on system-based controls and unique credentials.

Documentation and Monitoring

- Business purpose and allowability are documented.
- Automated matching, duplicate payment detection, or exception reporting is enabled where available.
- Procurement card activity is reviewed timely.

Reconciliation and Safeguarding

- Expenditures are reconciled to supporting documentation.
- Access to purchasing and payment systems is restricted and reviewed periodically.

Financial Reporting

- Financial reports are prepared using reliable, authorized data sources.
- Reports are reviewed for accuracy, completeness, and reasonableness.
- Variances and reconciling items are investigated and resolved.
- System report logic, queries, or templates are reviewed periodically.

Human Resources and Payroll

- New hires, compensation changes, and terminations are approved appropriately.
- Access to systems is provisioned and removed timely based on role.
- Payroll and salary distributions are reconciled periodically.
- Time reporting and leave approvals follow policy.
- Confidential personnel information is protected.
- Performance Evaluations are completed annually.

Information Technology and Cybersecurity

Access and Security

- System access is approved, role-based, and reviewed periodically.
- Multi-factor authentication is enabled where appropriate.
- Security logs are enabled and reviewed for anomalies.
- Security patches and updates are applied timely.

Data Protection

- Sensitive and regulated data is classified and protected.
- Data stored in cloud platforms complies with institutional security standards.
- Backups are performed and tested periodically.

Research and Sponsored Programs

- Sponsored awards are reviewed and accepted by authorized offices.
- Costs charged are allowable, allocable, reasonable, and timely.
- Cost sharing is properly budgeted and monitored.
- Effort reporting is accurate and supported.
- Sponsor budgets are reconciled to actual activity.
- Regulatory and export control requirements are understood and followed.
- Required financial and technical reports are completed.

Automation and Artificial Intelligence

- Automated or AI-enabled tools are used in financial, clinical, research, or monitoring processes.
- The purpose, data inputs, and outputs of these tools are documented.
- Human oversight exists for material decisions or outputs.
- Outputs are reviewed for accuracy, bias, and reasonableness.
- Models or rules are updated and validated periodically.
- Sensitive data is not used in unauthorized AI platforms.
- Access to AI tools and underlying data is restricted.

Continuity of Operations

- Business continuity plans address system outages, cyber incidents, and vendor failures.
- Recovery priorities and acceptable downtime are defined.
- Plans are tested periodically and updated as systems or vendors change.
- Plans are communicated to executive leadership, internal employees and external stakeholders.

Overall Assessment

- Key risks have been identified and addressed through appropriate controls.
- Compensating or automated controls exist where traditional controls are not feasible.
- Action plans are documented for identified control gaps.
