University of Alabama System®

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

Understanding Internal Controls

Office of Internal Audit

Revised May 2026

Objectives of This Manual

This manual provides a modernized framework for establishing, documenting, maintaining, and evaluating internal controls within higher education institutions, including academic medical centers and healthcare operations. It reflects current regulatory expectations, emerging risks, digital and cloud-based operations, data-driven processes, and the responsible use of automation and artificial intelligence (AI).

The objectives are to:

- Clarify management's responsibility for designing and maintaining effective, risk-based internal controls.
- Ensure faculty and staff understand their role in executing and monitoring controls.
- Promote efficiency by leveraging technology, automation, and data analytics where appropriate.
- Address emerging risks related to cybersecurity, third-party vendors, cloud platforms, and AI-enabled processes.

This manual is not a substitute for existing policies and procedures. It should be used in conjunction with existing university policies, regulatory requirements, and professional standards.

Scope

This guidance applies to all institutional operations, including academic, administrative, research, and healthcare activities. Control examples are illustrative, not exhaustive. Control processes should evolve as risks, technologies, regulations, and operational models change.

Management is responsible for determining the appropriate level of control using a risk-based approach. When control weaknesses are identified, management must:

- Implement additional or compensating controls *(an alternative measure implemented by an organization when a primary, intended control is too costly, impractical, or impossible to apply)*; or
- Formally accept the risk after evaluating cost, impact, and likelihood, with approval by senior leadership and notification to Internal Audit for disclosure to the Audit Committee for significant risks.

Introduction to Risk Management

Risk management and internal control are interdependent. Risks arise from strategic, operational, financial, compliance, technological, and reputational factors.

Risk management should include:

- Identification of risks, including cybersecurity, privacy, AI-related, and third-party risks;
- Assessment of likelihood and impact;
- Determination of risk response (avoid, mitigate, transfer, or accept);
- Assignment of a responsible risk owner.

Risk assessments should be refreshed periodically and when significant changes occur, such as leadership and significant personnel change, system implementations, regulatory changes, vendor transitions, or adoption of automated or AI-enabled tools.

What Are Internal Controls?

Internal controls are processes and activities designed and implemented to provide reasonable assurance regarding:

- Achievement of institutional objectives;
- Reliability and integrity of financial and operational information;
- Effectiveness and efficiency of operations;
- Safeguarding of assets, including data and digital resources;
- Compliance with laws, regulations, and contractual obligations.

Internal controls may be:

- **Preventive** – designed to prevent errors or misuse;
- **Detective** – designed to identify issues after they occur;
- **Directive** – designed to guide or encourage desired behavior.

Common internal control activities include the following:

- Authorization and Approval
- Continuity of Operations and Disaster Recovery
- Documentation
- Management Oversight
- Monitoring
- Policies, Standards, and Procedures
- Reconciliation
- Safeguarding Assets

- Segregation of Duties

Assets include physical property, financial resources, data (including student, patient, and research data), intellectual property, digital systems, and automated or AI-enabled tools.

Management sets the “tone at the top” and remains accountable for controls regardless of automation or delegation.

Key Controls

Key controls are those that management relies upon most heavily to achieve critical objectives and mitigate significant risks. These controls may be manual, automated, or a combination of both and are often supported by technology and data analytics.

Management Override of Internal Controls

While management has authority to make decisions, no individual is exempt from internal control requirements. Overrides increase fraud and compliance risk and must be rare, justified, documented, and subject to independent review.

A strong ethical culture, transparent reporting channels, and accountability mitigate the risk of improper override.

Authorization and Approval

Authorization ensures transactions occur in accordance with institutional directives. Approval signifies appropriate review for accuracy, legitimacy, compliance, and business purpose.

- Approvals may occur through electronic workflows and system-based controls.
- Authentication must rely on unique user credentials and, where appropriate, multi-factor authentication.
- Automated approvals must include defined thresholds, audit logs, and exception reporting.

No individual may approve a transaction that directly benefits themselves or where a conflict of interest exists.

Continuity of Operations and Disaster Recovery

Continuity planning ensures essential functions continue during disruptions, including:

- Natural disasters;
- Cyber incidents (e.g., ransomware, data breaches);
- Cloud or third-party system outages;
- Loss of key personnel.

Business continuity and disaster recovery plans should be documented, tested periodically, and updated for changes in systems, vendors, personnel or operations.

Documentation

Documentation provides evidence that controls were executed and supports accountability and transparency.

- Electronic records and system-generated audit trails are acceptable and preferred where reliable and secure.
- Documentation should be complete, timely, retrievable, and retained in accordance with records retention requirements.
- Redundant manual documentation should be avoided when system controls provide sufficient evidence.

Management Oversight

Management oversight includes reviewing financial, operational, and compliance information to identify anomalies, trends, or control deficiencies.

Oversight activities may be supported by dashboards, automated reports, and analytics. Significant issues must be investigated, resolved, and documented.

Monitoring

Monitoring is an ongoing evaluation of control effectiveness.

Monitoring may include:

- Continuous or automated control monitoring;
- Data analytics and exception reporting;
- Periodic independent reviews;
- User access and activity reviews.

Controls should be updated when monitoring identifies deficiencies or changes in risk.

Policies, Standards, and Procedures

Policies and standards define expectations; procedures explain how activities are performed. They should be reviewed regularly and updated to reflect operational, technological, and regulatory changes.

Reconciliations

Reconciliations compare independent data sources to ensure accuracy and completeness. Reconciliations may be automated or manual but must be reviewed and approved by someone independent of transaction processing.

Safeguarding Assets

Safeguards must protect physical, financial, and digital assets.

This includes:

- Restricted access to facilities and financials
- Asset tagging
- Periodic physical inventories
- Secure disposal methods
- Daily cash counts
- Timely deposits
- Role-based system access;
- Timely removal of access upon role changes;
- Encryption of sensitive data;
- Secure cloud configurations;
- Protection of AI models, training data, and outputs.

Segregation of Duties

Segregation of duties reduces risk by separating key functions (authorization, custody, recordkeeping, reconciliation).

When staffing limitations exist, management should implement compensating controls such as automated controls, enhanced monitoring, and independent review.

Use of Automation and Artificial Intelligence

Automation and AI may be used to enhance efficiency, monitoring, forecasting, billing, coding, and decision support. Management remains accountable for outcomes produced by these tools.

Controls over AI-enabled processes should include:

- Defined purpose and scope;
- Human oversight and review of material outputs;
- Periodic validation and performance monitoring;
- Data quality, privacy, and bias risk management;
- Restricted access and security safeguards.