UNIVERSITY OF ILLINOIS SYSTEM

Section 9 - Audits, Internal Control, and Business System Security

9.1 Internal Control Responsibilities

Policy Statement

All employees are responsible for safeguarding system resources and assets to ensure that they are used only for authorized purposes. Unit heads are responsible for implementing systems of internal control and proper segregation of duties to avoid mismanagement, fraud, theft, or personal use of system resources and assets. All employees are responsible for reporting fraudulent activities or misconduct.

All internal control procedures are subject to the review of the Office of University Audits and the Office of the Chief Financial Officer, as well as external auditors such as those commissioned by the Illinois Auditor General and other state and federal agencies.

Reason for the Policy

Internal controls are intended to prevent errors or irregularities, identify problems, and ensure that monitoring and corrective action is taken.

Applicability of the Policy

Employees and units are responsible to comply with laws, rules, regulations, policies and procedures, and other internal control practices and structures related to the performance of their duties and operations.

Procedure

Internal control is a term used to describe a variety of procedures that prevent or detect unintentional misstatements (errors) or intentional misstatements (irregularities). There are four general types of internal controls:

- **Directive**: Procedures to communicate what the rules are, or what should happen. For example, posted safety procedures or policies and procedures at the system, university, and unit levels are directive controls.
- **Preventive**: Procedures to keep errors or irregularities from happening. For example, segregation of duties, and designation of approval authority and spending limits are preventive measures.
- **Detective**: Procedures to identify errors or irregularities as they happen or shortly after they happen. For example, detailed account reconciliations and budget variance reports are detective controls.
- **Corrective**: Procedures to correct any errors that are identified. For example, when an error is made, employees should follow whatever procedures have been put into place to correct the error, such as reporting the problem to a supervisor. Training to strengthen staff knowledge in areas where weaknesses are identified is another example of a corrective internal control.

Consult Internal Control Tools from the Office of University Audits for additional information and training.

All employees are responsible for knowing the policies, procedures, and processes related to their position. Employees should be properly trained to correctly process transactions related to assigned duties and responsibilities. Employees should consult Job Aids and Training Materials for resources related to various business systems and processes.

Unit heads are responsible for establishing an operational environment that supports proper internal controls and segregation of duties as outlined in, 9.1.1 Unit Head Responsibilities for Internal Controls.

Related Policies and Procedures

1.6.2 Reporting Fraud or Misconduct, Whistleblower Protection, and Investigations

Additional Resources

Fiscal Control and Internal Auditing Act (FCIAA)
FCIAA
Internal Control Tools
Office of University Audits

Section 9 - Audits, Internal Control, and Business System Security

9.1.1 Unit Head Responsibilities for Internal Controls

Policy Statement

Unit heads must develop and implement internal control systems to provide reasonable assurance that:

- Information is reliable, accurate, and timely.
- Policies, plans, procedures, laws, regulations, and contracts are followed.
- Assets (including people) are safeguarded.
- Resources are used in an economical/efficient manner.
- Established objectives and goals are met.

Reason for the Policy

Internal controls are intended to prevent errors or irregularities, identify problems, and ensure that corrective action is taken.

Applicability of the Policy

Employees designated as the head of an established system unit.

Procedure

Unit heads should identify and analyze risks that could impact the achievement of system, university, and unit objectives to ensure that appropriate internal control policies and procedures are in place. Acquaint yourself with the general guidelines of the Fiscal Control and Internal Auditing Act (FCIAA).

Develop and implement an internal control system that conforms to these standards:

- Responsibilities are divided among different employees to ensure segregation of duties throughout the business process, especially those tasks related to authorization, record keeping, and asset custody. Proper segregation of duties prevents identified inappropriate business system role combinations that create high levels of risk.
- Authorization and record-keeping procedures provide reasonable accounting control over assets, liabilities, revenues, expenses, and other changes in the balance of funds.
- Office practices and routines comply with approved authorization and record-keeping procedures, including, proper storage, access control, and disposal of private and confidential data.
- Employees have the knowledge and skills needed to execute their assigned responsibilities.

Review your internal control system on a regular basis to determine whether:

- System and university-specific policies are being interpreted properly and are being followed.
- Procedures that are cumbersome or inadequate because of changes in operating conditions have been updated.
- The cost of protection outweighs potential losses, or a method would cause gross inefficiency. In this case, a given control may not be feasible and other alternatives may be more advisable.
- Corrective measures are taken promptly when an internal control system fails.
- The annual Fiscal Control and Internal Auditing Act (FCIAA) Questionnaire has been completed.

Unit heads may also request that an internal audit be performed. An audit provides an independent appraisal of the effectiveness and efficiency of your unit's administration. An internal audit can help you attain the missions and goals of your unit, inform you of best practices in fiscal and administrative management of your unit, and provide you with suggestions to streamline your operations, reduce costs, or increase revenues. Your unit may find it helpful to request an audit when it:

- Has installed new business or financial software.

- Needs to evaluate its internal controls.
- Needs to confirm it is complying with regulations.
- Suspects fraudulent activity has occurred.

If you have questions about your internal control procedures or need information about available resources, contact the Office of University Audits or consult their Internal Control Tools.

Related Policies and Procedures

1.6.2 Reporting Fraud or Misconduct, Whistleblower Protection, and Investigations

Additional Resources

Fiscal Control and Internal Auditing Act (FCIAA)
FCIAA
Internal Control Tools
Office of University Audits

Section 9 - Audits, Internal Control, and Business System Security

9.2 Annual FCIAA Questionnaire

Policy Statement
The president certifies to the Illinois Auditor General that the University of Illinois System complies with FCIAA requirements.

Reason for the Policy
The system is subject to and complies with the state of Illinois Fiscal Control and Internal Auditing Act (FCIAA) which requires public universities and other agencies to have fiscal and administrative controls in place to ensure that:

- Resources are utilized efficiently, effectively, and in compliance with applicable law.
- Obligations and costs are in compliance with applicable law.
- Funds, property, and other assets and resources are safeguarded against waste, loss, unauthorized use, and misappropriation.
- Revenues, expenditures, and transfers of assets, resources or funds applicable to operations are properly recorded and accounted for to permit the preparation of accounts and reliable financial and statistical reports and to maintain accountability over the State's resources.
- Funds held outside the State Treasury are managed, used, and obtained in strict accordance with the terms of their enabling authorities and that no unauthorized funds exist.

Applicability of the Policy
All employees identified as having a role in the annual FCIAA process.

Procedure
FCIAA Group Managers designate individuals to represent each unit. The individual designated to represent the unit (Submitter) receives access to the form, answers the questions on the form, and submits the form to his or her unit head (Approver) for review and approval. The unit head certifies the information by approving and submitting the form before the given deadline.

Units will be notified as to the timing of the annual FCIAA process by their respective university or University of Illinois System Offices coordinator.

Additional Resources
University of Illinois System - FCIAA
(30 ILCS 10/) Fiscal Control and Internal Auditing Act (FCIAA)

Section 9 - Audits, Internal Control, and Business System Security

9.3 Report Activity from Audits, Reviews, Consulting Engagements, and Attestation Services Provided by External Parties

Policy Statement

Units may hire external business and consulting professionals to provide, audit, review, consulting, attestation, and related services. Any resulting draft or final work product received from the external provider must be submitted to system offices staff annually.

Reason for the Policy

Units of the University of Illinois System may need external financial and business services, such as audit, review, consulting and attestation services. External providers frequently possess specialized skills, knowledge, credentials and independence that may not be readily available among System faculty and staff. Resulting draft or final reports received from these engagements could reveal risks to the overall University of Illinois System, beyond the individual units that seek these services.

Applicability of the Policy

Draft or final work product received from external business and consulting professionals with issues related to:

- Financial information
- Business processes and potential improved efficiencies
- Fiscal, administrative, and internal controls
- Compliance with laws and regulatory requirements

Examples of audits, reviews, and consulting recommendations which **do not need** to be submitted include issues related to:

- Sponsored projects and grant funding agencies. These reports should continue to be provided to your university's Grants and Contracts, Post Award Office for review.
- Academic programs and accreditation with only incidental references to financial information
- Building design or potential construction projects or site inspections of existing structures
- Commercialization of intellectual property

Procedure

To submit all draft and final audit, review, consulting, and attestation service engagement reports received from external providers:

1. Identify any draft or final audit, review, consulting, and attestation service reports received from external providers during the twelve-month period ending on June 30th.

2. With the exception of reports or recommendations made pursuant to the attorney-client privilege as indicated below, submit all draft and final reports prepared by these external providers to ConsultRepRev@uillinois.edu by August 15 of each year. Units are encouraged to submit these reports throughout the fiscal year if they are available sooner.

   If your unit has such reports or recommendations that were performed or received pursuant to the attorney-client privilege, please contact the Office of University Counsel for guidance as to whether or not such reports or recommendations are subject to this policy; they are not necessarily exempt from this requirement.

3. Prepare to answer any questions related to the report(s) that may come from the review process, which evaluates the potential risk and other considerations related to the System's financial statement reporting process.

4. Disclose adverse results from these engagements and any related reports during the annual Fiscal Control and Annual Auditing Act (FCIAA) certification process.

Questions can be sent to ConsultRepRev@uillinois.edu.

Section 9 - Audits, Internal Control, and Business System Security

9.4 Business Financial Information

Policy Statement

The University of Illinois System owns all information gathered, stored, or maintained for business purposes, unless otherwise stated in a contractual agreement. This ownership includes all system information regardless of location or media. Such information is to be used only for conducting system business.

People who act as stewards or caretakers for the business financial information of the system have a responsibility to ensure that business is transacted legally, protect the assets of the system, and avoid conflicts of interest.

System units have unlimited, read-only access to most business financial information, but must follow the standard access approval process that includes Unit Security Contacts and Administrative Information Technology Services (AITS). Unit heads are responsible for the security of system data used by their unit. Unit heads must ensure that that Unit Security Contacts are notified in a timely manner when employees transfer to another unit or no longer work for the University of Illinois System.

Individuals must report known or suspected security violations to the Associate Vice President for Administrative Information Technology Services (AITS) or delegate.

Reason for the Policy

The system has a fiduciary responsibility regarding business financial information (including Social Security Numbers). The system will respond to security violations by:

- Limiting the individual's access to some or all university systems,
- Initiating legal action, including, but not limited to, criminal prosecution under appropriate state and federal laws,
- Requiring the violator to provide restitution for any improper use of service, and,
- Enforcing disciplinary sanctions in accordance with the relevant system policy.

Applicability of the Policy

Business financial information covered by this policy includes but is not limited to information held in systems where financial, payroll, employment, and student transactions can be started, routed, approved, and/or completed.

Procedure

Employees, contractors, and students are expected to exercise responsible, ethical behavior when using system computers, information, networks, or resources.

Individual responsibilities include preserving the confidentiality and security of data to which the user has been granted access and ensuring that data are used only for and in the conduct of system business. These responsibilities also include the proper storage, access control, and disposal of private and confidential data presented to the user in any form.

Unit heads are responsible for establishing proper data controls, such as;

- Implementing consistent data security policies and standards,
- Maintaining proper segregation of duties by ensuring that system access and associated permissions are divided among different employees,
- Developing a disaster recovery plan that includes access controls and contingency plans for continuous operation in case of emergencies such as power outages,
- Developing and maintain an internal security plan to assure data integrity and authentication,
- Ensuring that each system utilized by your unit is used ethically and for its intended purpose, and,

- Notifying your Unit Security Contact (USC) when employees leave the system or are transferred to another unit.

Related Policies and Procedures
Ending University of Illinois Systems Access Upon Employee Separation Termination
University of Illinois System: Social Security Number Policy

Additional Resources
Find Your USC
Get Enterprise Data
For data security policies and standards, consult IT Policies.
For additional information regarding the rules for use of financial information, search for keywords such as "software" or "security" in:
University Policy and Rules for Civil Service Staff
University of Illinois Statutes
Academic Staff Handbooks
Urbana
Chicago
Springfield
Code on Campus Affairs
Urbana
Springfield - Consult the Academic Staff Handbook