Introduction

There are two primary schools of thought in developing an audit approach:

- One viewpoint is to assume that everyone is looking for ways to “beat the system”; therefore, the auditors devise audit steps that focus on finding evidence of wrongdoing.

- The other approach is to assume that most people take pride in their work and want to do the right thing—they just need to know what is expected of them and have the information and tools available to allow them to successfully carry out their responsibilities. In this case, the auditor’s approach is to examine areas of high risk and focus on ways these risks can be most effectively and efficiently mitigated.

We are pleased to say that the latter is the vision, philosophy, and progressive approach we have adopted in the Department of Internal Auditing at Georgia Institute of Technology.

As we have canvassed the campus conducting audits and collaborated with colleagues throughout higher education, we have compiled perspectives and observations of “best practices” in handling many of the areas of risk that most units (departments, schools, etc.) encounter. This is not a policies and procedures manual – there are already many valuable policies and procedures which outline business rules. Our goal with this document, instead, was to compile our observations and recommendations on best practices in managing business risks and creating effective and efficient systems of internal control.

In establishing solid risk mitigation procedures and strong systems of internal control, faculty and staff are then free to advance their units’ missions towards achieving their strategic goals.

This will be a living document and will be updated frequently so we encourage visits to our web site to check for updates and revisions. We welcome questions and feedback regarding the information contained herein, particularly comments regarding how this may be more useful.

We express our appreciation for the support from the Office of the President, the Executive Staff, and the many subject matter experts around campus who have provided input and feedback on this document. This collaborative approach with senior management demonstrates the Institute’s commitment to ensuring its administrative processes are on par with the high standards of excellence Georgia Tech is known for in its academic and research initiatives.

Department of Internal Auditing

November 2014
# INTERNAL CONTROL GUIDE

## TABLE OF CONTENTS

### INTERNAL CONTROL GUIDANCE: FISCAL

- I. Accuracy of Financial Records .............................................................. 3
- II. Sponsored Programs ........................................................................... 5
- III. Capital Assets..................................................................................... 8
- IV. Foundation Funds ............................................................................... 11
- V. Travel .................................................................................................... 14
- VI. Cash and Receivables ........................................................................ 16
- VII. Procurement ...................................................................................... 19
- VIII. Telecommunications ........................................................................ 21
- IX. Insurance and Claims Management ................................................. 23

### INTERNAL CONTROL GUIDANCE: HUMAN RESOURCES

- X. Leave Reporting .................................................................................. 25
- XI. Off-Campus Assignments .................................................................. 26
- XII. Employment Eligibility Verification .............................................. 27
- XIII. Sexual Harassment .......................................................................... 28
- XIV. Consultants vs. Employees .............................................................. 30
- XV. Compliance with Equal Employment Opportunity Laws ............ 31
- XVI. Annual Performance Evaluations .................................................. 32

### INTERNAL CONTROL GUIDE: LEGAL AND REGULATORY

- XVII. Contracts ....................................................................................... 33
- XVIII. Gifts ................................................................................................. 35
- XIX. Open Records Act ........................................................................ 36

### INTERNAL CONTROL GUIDANCE: HEALTH & SAFETY

- XX. Safety of Workplace ......................................................................... 37
- XXI. Environmental Protection ................................................................. 39

### INTERNAL CONTROL GUIDANCE: INFORMATION SYSTEMS

- XXII. Strategy and Vision ........................................................................ 41
- XXIII. Operations / Administration .......................................................... 44
- XXIV. Physical & Environmental Security Controls ................................ 48
- XXVI. Data Stewardship Controls ............................................................ 51
- XXVII. Training ......................................................................................... 53
- XXVIII. Documentation ........................................................................... 55
- XXIX. Equipment Maintenance ............................................................... 57
- XXX. Business Continuity Planning ......................................................... 58
- XXXI. Software Licensing ........................................................................ 61
- XXXII. Web Site Operation / Development ............................................ 63

### INTERNAL CONTROL GUIDANCE: PUBLIC RELATIONS

- XXXIII. Public Relations Management .................................................. 64
- XXXIV. Association with External Organizations ................................... 65

### INTERNAL CONTROL GUIDANCE: STUDENTS

- XXXV. International Students ................................................................. 66
- XXXVI. Students/Sexual Harassment ....................................................... 68
INTERNAL CONTROL GUIDANCE: FISCAL

I. Accuracy of Financial Records

**Description of Risk:** If errors are made in official Institute financial records, and go undetected, the Institute could be exposed to legal risk and adverse publicity.

**Criteria:** Basic requirements for recording and reporting financial activities have been established in the Board of Regents’ Business Procedures Manual (BPM), Section 1.0: Accounting Principles and Definitions. Based on this and other pertinent instructions, the Institute has developed policies and procedures designed to record its financial activities into project ledgers. Although not specifically stated in Institute policy, it is the campus unit that is responsible for establishing these ledger projects and seeing that their entire unit’s accounting records are recorded there. Good business practices suggest that campus units ensure that their Institute reports and ledgers are reasonably stated and free of error that could potentially cause legal liability and negative publicity at the Institute.

**Auditor’s Overview:** Campus units must be aware of Institute project ledgers and where their budgets, revenues, expenditures and other accounting data are recorded. Many employees, both in and outside the unit, will be recording information to these projects. Nevertheless, it is the unit’s responsibility to periodically review these records. The unit should verify that differences and discrepancies have been identified, reported, and corrected, so that Institute records accurately show the financial condition of the unit.

**Best Practices:**
- 1. Designate an individual with the responsibility of identifying unit accounts
- 2. Develop and document internal policies and procedures
- 3. Ensure segregation of duties exist
- 4. Reconcile unit accounts
- 5. Supervisory oversight

**Process**
**RESPONSIBILITY, DELEGATION, and COMMUNICATION**
The unit head has the ultimate responsibility for ensuring the accuracy of all unit account balances. *Delegating the oversight for this activity does not relieve the unit head of the responsibility for the accuracy and reliability of the unit’s financial records.*

The first step is for the individual delegated the oversight for this activity is to have a reasonable understanding of how Institute, sponsored, State, and other applicable policies and procedures affect the unit’s operation. It is this person who is responsible for preparing internal policies and procedures that satisfy all the criteria required by these entities. As a part of developing internal policies and procedures, this individual should ensure a complete listing of project numbers for the unit is identified and validated. This person will assign, and ensure appropriate training of, personnel to accomplish the unit’s objectives. This person will make the necessary adjustments and management decisions to temporarily change or alter policy and procedures, such as might
be needed when hiring new, untrained employees. Finally, it is this person who will generally enforce policy and procedure adherence among all involved employees.

The level of complexity and number of projects often dictates how many employees are assigned responsibility for assuring the accuracy of the unit’s financial records. In larger units, this responsibility may well be separated into sponsored projects, foundation projects, and State/other projects. Further, there may well be duplicate responsibilities over multiple units. For example, principal investigators have general responsibility for the integrity of their sponsored projects, but units will typically have a separate business employee monitoring all sponsored project accounting. Further, both the Institute and Georgia Tech Research Corporation perform their own monitoring of sponsoring activities, designed to complement and reinforce the units’ efforts. In this environment, it is essential that the unit documents how it will perform this function.

GOOD INTERNAL POLICIES AND PROCEDURES
Policies and procedures to reasonably ensure the reliability and accuracy of a unit’s financial records must be an integral part of overall unit financial activity policies and procedures. The level of detail and complexity will vary based on the number of employees involved in recording project activity, the number of projects, the sources and amount of funding, and external assistance or influences directly affecting unit activities. These policies should provide references to Institute policies as a minimum. These procedures should inform personnel what they are responsible for, what other employees are responsible for, the general timing of events, how errors and corrections will be addressed, and when they will be expected to have completed their assigned duties.

SEPARATION OF DUTIES
Ideally, unit personnel charged with verifying the reliability of its accounting records should not have the ability to post transactions to those accounts. Other, compensating controls must be in place if this condition is present. For example, in the case of sponsored projects above, since the principal investigator has access (and responsibility) for directing the financial activities posted to his/her project, then another employee, with no ability to initiate any project activity, should be reviewing the project’s activity on a regular basis.

Related Issues:
1. **Foundation Accounts**: This section addresses Institute projects. Many units also maintain accounting records that do not go through, or are not covered by, Institute rules. The primary example is Georgia Tech Foundation accounts. While Georgia Tech usually establishes a corresponding/related Institute account to be used for expending Foundation monies, this is not always the case. Even if this Institute account is established, some expenditures may be paid directly by the Foundation, and not be recorded in the Institute’s account. In these and all other cases where the unit has the responsibility for ensuring the accuracy and reliability of its non-Institute accounting records, we strongly advise that the unit adopt the same, or similar, standards as presented above.

2. **Record Retention**: Most original source documents to support the accounting information in the unit’s Institute project records are still the responsibility of OHR, Budgets, Payroll, and other Business Office units. Campus units are more frequently being called-upon to
retain these original records. Units should include information in their internal policies that informs unit staff members of the applicable rules and regulations for their unit.

II. Sponsored Programs

**Description of Risk:** Improper administration of sponsored contracts could cause disallowance of costs, refusal of sponsors to award future contracts, and negative publicity for Institute.

**Criteria:** OMB Circular A-21 and the Institute’s Grants and Contracts Policy and Procedures, at http://www.policylibrary.gatech.edu/business-finance/grants-contracts-accounting, require that academic units be responsible for the reasonable and accurate reporting of their sponsored expenditures. [Note: Federal Acquisition Regulation (FAR) 31.2 and Georgia Tech Research Institute’s (GTRI) Policies and Procedures provide similar guidance for GTRI expenditures. Although this section addresses Institute sponsored activities, the same principles apply to GTRI activities.]

**Auditor’s Overview:** This section addresses how the unit should be involved in the oversight of sponsored accounts. Actions discussed here are in addition to general steps taken to verify the reasonableness and integrity of financial records, as discussed in “Accuracy of Financial Records.”

**Best Practices:**
1. Understand the level of sponsored activity in the unit
2. Designate an individual responsible for coordinating all sponsored activities in the unit
3. Provide training to individuals on proper administrative procedures
4. Develop and document internal policies and procedures on administration of sponsored activities

**Process**

**UNIT EVALUATION**
The Institute asks all academic unit heads to encourage and support, to the fullest extent possible, efforts by the faculty and staff to attract and perform sponsored research activities. Part of this support is administrative assistance in complying with the many rules, regulations, and standards applicable to sponsored activities. In this environment, all unit heads should periodically, but at least annually, evaluate their sponsored activities in relation to their overall activities. One purpose of this evaluation is to determine if personnel and resources are reasonably allocated to sponsored activities. A support staff of one or two employees may have been adequate, using old administrative techniques or processes, but a doubling of sponsored dollars or projects may require more support help and/or new processes/techniques. Conversely, reduction in sponsored activities means that support staff efforts may need to be reallocated, and that efforts to boost sponsored activity should be initiated.
The unit head must be involved with his/her personnel who perform sponsored research from the point of hiring, before any sponsored activity starts. This advance knowledge is needed so that the unit head can anticipate, and plan for, both the long-range and the near-term needs of the unit. For the near-term, this information is needed to reasonably plan for needed employee training, coordination of physical space, unit budgeting, and for Faculty evaluations.

RESPONSIBILITY AND DELEGATION
In most units with sponsored activity, the unit head selects one person to exercise the care and attention that will be needed to administer the sponsored activities of the unit. This person is given BOTH the responsibility AND the authority to coordinate the unit’s sponsored activities. Delegating the oversight for this activity does not relieve the unit head of the responsibility for the accuracy and reliability of the unit’s financial records. The complexities of Institute sponsored accounting have made experience, formal training, and cross-training prerequisites for this position and for those who may work for this person. In most campus units, this person will:

- Supervise the unit’s business office employee(s) who monitor(s) project accounting
- Coordinate activities between Office of Sponsored Programs, the principal investigator, and Grants and Contracts Accounting; this employee will also work with their counterparts in other campus units for proper interdisciplinary accountability
- Generally protect the Institute’s interests in the proper conduct of his/her unit’s sponsored activities

The first step is for the responsible person to become familiar not only with Institute sponsored policies and procedures cited above, but also on the related areas of budgeting, accounting, procurement, facilities management, & PeopleSoft data entry and reports. This person must then be aware of the unit’s scope of sponsored activities to be administered. With this background, the person can then document how the unit will handle its sponsored activities. Other basic steps should include:

- Require appropriate activity to be processed through the unit’s assigned business office employee. This step is not necessarily to “approve” any single transaction, activity, or report, but is the only way the unit can ensure that PIs are performing their activities in a reasonable and prudent manner.
- Maintain a master project control record, to track the activity from proposal through final deliverable. Important dates and milestones should be monitored, and actions taken as needed to ensure compliance with policies, procedures, laws, and contract terms.
- The unit’s business office should have a copy of the proposal (if applicable) and signed contract or sponsored agreement before initiating a request for a project number. Generally, no expense should be incurred before the project number is assigned or an authorized pre-award number is assigned. In addition, this information is needed so that the business office employee responsible for monitoring the unit’s sponsored activities can reasonably perform this function.
- Finally, the unit should receive, access, and/or run Institute supplied reports and information, made available to assist them in the proper administration of their sponsored activities. Besides Institute project ledgers and PeopleSoft Salary Planning and Distribution (SPD) reports, there are Grants and Contacts Accounting PEB reports, Workload Assignment forms, undesignated reports, undeliverable and late deliverable
reports, and many others. Units should incorporate these reports in an overall plan of sponsored activity controls.

COMMUNICATE WITH EVERYONE
While everyone in the unit has to understand their duties and responsibilities in the handling of the unit’s sponsored activities, principal investigators are ultimately responsible for their own sponsored activities. Savvy campus units strive not only to educate and assist their PI’s, but to tailor the level of assistance to the specific needs of each PI.

Everyone in the unit should be notified of the previously documented internal policies and procedures on how the unit will administer its sponsored activities.

Related Issues:
1. Record Retention: Most original source documents to support the accounting information in the unit’s Institute sponsored project records are still the responsibility of OHR, Budgets, Payroll, Grants and Contracts Accounting, and other Business Office units. But campus units are being called-upon more and more to retain these original records. Units should include in their internal policies appropriate document retention for Institute project records.
2. A-21/Plan Confirmation System: Participation in sponsored activities puts the Institute under many additional compliance rules and regulations, over and above those imposed by the state and the Board of Regents. One such entity is the federal Office of Management & Budget, which issued its Circular A-21 to provide Educational entities with the rules they are to use for sponsored activities. The Institute, for its part, incorporated these rules into its Plan-Confirmation System (PCS). A-21/PCS policies and procedures are in place to offer assurance to our sponsors that the expenditures the Institute is asking them to reimburse are reasonable and timely. Since salaries and wages constitute the bulk of Institute charges, that is where most of the processing and procedural controls are. Some of the major areas requiring unit attention under the PCS include the following.

- Undesignated Costs: For any number of reasons, a unit may not always have a sponsored account to which encumbrances and expenditures can be posted. In these cases, units are to charge a special undesignated account, until such time as the regular sponsored account can be established. For personnel costs, this typically means the Institute starts the fiscal year with several million dollars in these costs. Since no sponsor has been designated to invoice, the Institute must fund these costs until the sponsored account is established. Units must monitor and reduce all of their undesignated costs in a reasonable manner during the fiscal year. Institute policy requires no such costs be on the books at the close of the fiscal year.

- Cost Transfers: When expenditures are incorrectly charged, units are expected to identify and correct the error. All cost transfers are to be processed in a timely manner and properly documented. A cost transfer made within 60 days after the posting date of the transaction requiring a transfer will be considered timely. Cost transfers to externally-funded sponsored funds beyond 120 days of the original expense posting will not be allowed under normal circumstances.

- Annual Statement of Reasonableness (ASR) forms: A-21/PCS rules require that all Institute employees (or an acceptable substitute) covered by the PCS should sign an annual statement, certifying that their salary and wages distribution reasonably reflects
their work effort. Electronic Workload Assignment forms distributed monthly to covered employees provide the means for employees to review and notify appropriate unit personnel of needed changes during the fiscal year.

III. Capital Assets

**Description of Risk:** Failure to properly account for capital assets could result in the loss of equipment, adverse publicity, potential loss of overhead recovery, and/or a misstatement of the value of capital assets on Institute records.

**Criteria:** The State of Georgia requires the Institute to be accountable for all equipment under its control. The Institute's policy requires the maintenance of a capital asset perpetual inventory to achieve correct financial reporting for the Institution, to provide the basis for suitable insurance coverage, and to assist departments in accountability for their equipment. ([http://www.policylibrary.gatech.edu/business-finance/equipment-management](http://www.policylibrary.gatech.edu/business-finance/equipment-management))

**Auditor’s Overview:** The purpose of reviewing this area is to ensure that campus units are engaging in true perpetual inventory practices. The perpetual inventory practice ensures the continual tracking of additions, deletions, and movements of equipment on a regular basis. Also, physical inventory counts must be conducted at least annually and their results used to adjust the inventory record.

**Best Practices:**
1. Empower one person with the responsibility and authority to oversee this process
2. Communicate the importance of this issue to the entire unit, enlisting their full cooperation in this matter
3. Develop and document internal capital asset procedures
4. Ensure that equipment entries are properly coded
5. Ensure that equipment is tagged in an accurate and timely fashion
6. In moving the asset from one location to another, information regarding the move is properly recorded and timely reported
7. In performing a physical inventory, information regarding the physical inventory is properly recorded and timely reported as a means of adjusting inventory records
8. Remember, capital asset control is much easier, faster, and more accurate if you view it as an ongoing process rather than allowing it to accumulate

**Process**

**RESPONSIBILITY AND DELEGATION**
The first basic step is that the Unit Head has to decide on one person that can be trusted to exercise the care and attention that will be needed to accomplish a reliable inventory control over the long run. This person then has to be given BOTH the responsibility AND the authority to see that the job gets done, from acquisition and tagging to disposal.

The person assigned capital assets responsibility should:
• Familiarize himself/herself with the policies and procedures contained on Georgia Tech’s web page, as well as the information contained on the Procurement Services web page.
• Formalize an approach for implementing these procedures. Write down specific steps that staff should follow to ensure accurate and timely handling and recording of asset transactions.
• Ensure that all purchase requisitions are properly completed. Accurate information up front may save headaches later.
• Ensure that assets are properly controlled up front.
• When the asset arrives, be sure that the packing slip information matches the purchase request information; and check the actual asset to make sure it matches both of these. Refer to the Capital Assets Accounting Department (CAAD) website for proper methods of tagging new equipment. http://www.business.gatech.edu/cont_web/caad.html

COMMUNICATION
Everyone in the unit has to understand that accurate and timely inventory practices continue constantly, not just once per year, and that these practices are everyone’s responsibility. The Unit Head communicates this by email, memo, meeting topics, and/or one-on-one conversations. Be sure to notify all personnel about internally developed policies and procedures.

ENSURE ACCURACY OF INFORMATION
Always check and double-check your project codes and other information that will be input to establish the new equipment on the Institute asset records. Procurement information is appropriately coded to ensure that “equipment” is added to the capital assets records. For example, if the equipment is inadvertently coded to the account code “Software,” the asset will NOT show up on the CAAD inventory. It becomes a time-consuming process to add it to the inventory after the fact.

EQUIPMENT TRANSFER
Remember, to transfer equipment within the Georgia Tech campus you must update the location in PeopleSoft. This information flow helps keep annual inventory records accurate.

OFF-CAMPUS EQUIPMENT TRACKING
It is normal for some faculty and staff members to conduct some of their work from their homes or offices away from the Tech campus. When it becomes necessary to take some of the Institute’s equipment off-campus to use in this work, keep in mind the following points:
• Be sure to complete and sign the Equipment Loan Agreement form
• Retain a copy at your school or department for audit and insurance recovery purposes
• Contact Risk Management (4-3483) to obtain information on how to insure the property off site
• Remember, if a piece of equipment is at home and there is no loan agreement on file, the equipment is not insured under Georgia Tech’s policy; any loss may be borne by the unit or the individual using the equipment
INVENTORY SYSTEM
State law requires that all schools within the University System of Georgia keep a perpetual inventory of their capital assets. As part of this inventory system, Georgia Tech conducts annual physical inventories. Here are some tips to make things go more smoothly:

- Access and read Institute Policies and CAAD websites
- Establish a contact person in CAAD
- Obtain a user ID and/or access to the system
- Run an inventory report for your department
- After conducting the physical inventory, investigate the variances, if any.
  - Is an item simply missing? Ask another individual to check for the item. A fresh pair of eyes may pick up things that someone else missed. If it cannot be located after two consecutive inventories, contact CAAD in order to determine what steps to take.
  - Does the item appear to have been stolen? Report this to the Chair or Department Head and also to Georgia Tech Police Department 404-894-2500.
- In researching and resolving variances, the first step of course is to double check your original counts; it may be useful to have someone who did not count the item originally perform the second count.
- Report results to CAAD so that Institute records can be adjusted

SURPLUS EQUIPMENT
When it comes time to retire Georgia Tech equipment, remember to go to [http://www.admin-fin.gatech.edu/business/equipment/070090.html](http://www.admin-fin.gatech.edu/business/equipment/070090.html), for instructions on how to notify the business office of surplus equipment.

**Related Issues:**
**Equipment not owned by the Institute**
Institute units may be in possession of equipment not owned by the Institute and not on the Institute’s CAAD property records. Generally, the equipment in question will have been purchased under an 8433xx account code, and should be marked with the owner’s equipment tag. Owners of such Institute used equipment would include the Georgia Tech Research Corporation and Sodexho (dining services). Proper equipment controls between the equipment users and the owners should be in place, and Risk Management should be made aware of these conditions.

Special rules apply when a federal sponsor holds title to equipment used by the Institute. This equipment is administered by GTRI under rules found on their website.

**Equipment relocation out of country**
A Carnet is an official pass or permit used when shipping equipment temporarily to another country. You should consider it the "passport" for equipment you are shipping, because it is a document that must accompany the equipment during export and import through customs. The advantages of obtaining a carnet are to eliminate assessment of taxes or duties, and to simplify the customs procedures - especially reentry of the equipment into the United States. Carnets are issued for a one-year period. Note: Most countries will not extend the time period of the Carnet.
All information and forms regarding obtaining a Carnet can be found at the United States Council for International Business web page: [http://www.uscib.org/](http://www.uscib.org/). Scroll down and click on ATA Carnet Export Service. (Our thanks to Mechanical Engineering for this wording from their internal web handbook.)

Managing software

The controls on commercial software become more important not only because of the aggregate costs of software packages, but more importantly because managers must mitigate the high liability associated with failure to control licenses on commercial software. Hence, like capital assets, inventory and management of software is an area requiring close management scrutiny. Some best practices can be found at [http://oit.gatech.edu/service/softwarehardware/softwarehardware](http://oit.gatech.edu/service/softwarehardware/softwarehardware).

IV. Foundation Funds

**Description of Risk:** The primary risk is using Foundation funds for purposes not intended by the donor, or that violate Institute or Foundation policies. Serious violations at the unit level can result in reduced unit funding and personnel actions, possibly leading to criminal and civil penalties. Beyond the unit, serious violations can damage the reputation of both the Institute and the Georgia Tech Foundation, and impair our joint, future fund-raising efforts.

**Criteria:** Georgia Tech policies and procedures require that all units encourage gift/grantee donors to make their gifts payable to the Georgia Tech Foundation, Inc. (GTF or the Foundation). All private gifts must be approved by the Vice President for Development to ensure that the gift being solicited is consistent with the needs of the campus unit, and the conditions of the gift are within the scope of activities that may be properly supported by the Institute. Further, all funds held by the GTF must be expended in accordance with the restrictions or intent of the donor and with Georgia Tech policies and procedures. GTF funds intended to benefit a function of Georgia Tech (instruction, research, service, and supporting functions) are to be recorded on Institute financial records. All transactions financed by GTF funds are to be made through the Institute in accordance with generally accepted business practices and procedures, except where there are specific prohibitions on the use of the funds by the Institute, or when prior approval of individual transactions has been received from the Office of the President. This and other Institute policies can be viewed at [http://www.policylibrary.gatech.edu/business-finance/foundation-funds](http://www.policylibrary.gatech.edu/business-finance/foundation-funds)

**Auditor’s Overview:** The availability of external funds to finance unit activities is a welcomed benefit, but there are rules and conditions that come with these funds. Campus units should exercise reasonable and prudent care in the acceptance, allocation, and use of private, non-sponsored Foundation funds.

**Best Practices:**

1. Work with an Institute development officer on ways to maximize gifts to the unit
2. Evaluate this area on an annual basis and decide what level of effort should be expended on this activity
3. Document the assignment of responsibility and authority to administer the unit’s Foundation activities
4. All requests for disbursement, whether the processing will be through the Institute’s GTF matching account or by direct GTF payment, should be reviewed by the unit’s business office
5. Foundation account activity, and activity in any matching Institute accounts, should be reconciled to internal supporting documents
6. Units should make every effort to productively use available funds that will revert to general Foundation control at year-end if unspent (lapsing)

Process

DEVELOPMENT OFFICER
All academic units have a development officer responsible for soliciting gifts for the Institute. In some cases, that person works solely for, and is paid by, the unit. In other instances, however, the development officer works for several units. Nonacademic units do not have development officers to actively solicit gifts, but the Institute does employ development officers to solicit gifts for the general benefit of the Institute.

Depending on your unit’s situation, a working relationship with a development officer may provide the opportunity to increase the Foundation funds available to your unit. This may occur simply by informing the development officer of your needs, or by relaying relevant ideas or tips on possible donors. At a minimum, a development officer can offer insights to unit administrators and faculty on how they may recognize opportunities for soliciting grants and gifts when performing their regular Institute duties. For specific information and further guidance, contact the Vice President of Development.

UNIT EFFORT
Unit heads have several responsibilities in this area, including: deciding the level of effort needed for this function; informing faculty and staff of possibilities and benefits of having Foundation funds available; budgeting and appropriate use of funds; and putting in place proper administrative controls.

Annually, the unit head should plan for the level of unit effort that will be devoted to soliciting grants and gifts. For academic units, the unit head may assume significant development responsibility, incorporating not only his/her time, but also that of unit administrators and faculty. (Note: Many schools enlist the aid of emeritus professors and successful alumni into this planning.)

As a part of the annual budgeting process, unit heads should make sure that anticipated Foundation funding is included. This process should document the unit head’s approval for accumulating otherwise available Foundation funds for planned, future purposes.
DELEGATION AND AUTHORITY

Ideally, one person should be assigned the responsibility and authority to coordinate the functions of these individuals. The unit should be mindful that appropriate separation of duties should be practiced in the handling of these accounts.

There are two minimum accounting responsibilities units should perform in administering their Foundation accounts.

- Procedures should be established so that all expenditures are processed through a unit’s business office employee. Some units split this responsibility between two employees, depending on whether the disbursement will be processed through the Institute’s matching account or paid directly by the Foundation. The reason for this step is to ensure that the disbursements are reviewed for compliance with the donor’s intent and applicable policy restrictions.
- Monthly Foundation account reports should be reviewed for reasonableness and accuracy. It is highly recommended that the accounts be reconciled to their matching Institute account, if appropriate. If the same employee who processes disbursements is made responsible for this reconciliation, then reasonable compensating internal controls should be established to counter this processing weakness.
- Project Expense Budget Reports (PEBs) are made available through Grants and Contracts. These reports reflect Georgia Tech and GTF expenditures and should be examined regularly.

MANAGING FUNDS

Grants may come with deadlines for using the funds. Much of the funding provided by the Foundation’s governing board for general Institute use must be expended in the current year. These are but two examples of available funding that may be lost if the unit does not properly administer its Foundation accounts. While these amounts are generally immaterial, both individually and in total for the unit, we have noted one case where a unit “lost track” of an account and nearly forfeited more than $300,000 in available grant funding. Good business practices, and a reasoned stewardship over these funds, call for units to include this aspect in administering their Foundation funds. As a result, we recommend that units develop a reasonable tracking system that provides feedback to the unit head and describes the remaining fund balances and deadlines for usage.

Related Issues:

Employee Gifts
Georgia Tech employees may not be permitted to accept gifts for personal use from third parties who conduct business with either Georgia Tech or the Board of Regents. (See our section on gifts for more on this topic.) The Governor’s memo regarding this issue can be viewed on the Department of Internal Auditing website at www.audit.gatech.edu.

Contract vs. Grant/Gift
Contracts are administered by the Office of Sponsored Programs (OSP), and by the Grants and Contracts Accounting Department. The Foundation handles grants and gifts. Campus units can determine the difference between these by reading the policy in
Scholarships
Sometimes, donors will designate their gifts as scholarships available only to students that a particular college or school decides are qualified. In these cases, although the Office of Scholarships and Financial Aid will make the actual disbursement from the account, the unit will be the one to designate who will receive the scholarship. Generally, the unit head will assign this responsibility to a faculty member. The unit employee assigned with general Foundation administrative responsibility will need to work with this faculty member to ensure that the Foundation account is properly administered through the Office of Scholarships and Financial Aid.

V. Travel

Description of Risk: The risk is that travelers may request and be reimbursed for travel costs that exceed allowable limits or for personal expenses, rather than those items essential to carrying out the business of the Institute. Reimbursements of this type are a violation of state law. If such violations were to occur, it could result in financial loss for the Institute and could generate negative publicity.

Criteria: The Institute’s travel policies and procedures are contained in the Institute Policy Library at [http://www.policylibrary.gatech.edu/business-finance/travel](http://www.policylibrary.gatech.edu/business-finance/travel). The policies and procedures set forth in the travel statements apply to reimbursements from state funds and sponsored funds, unless the sponsored agreement states otherwise. Some of the basic requirements are that:

- Authorization to travel must be obtained prior to travel.
- Travelers are entitled to reimbursement for reasonable, necessary, and allowable expenses incurred. Additional expenses incurred for personal preferences or conveniences are the responsibility of the employee.
- Travel Expense Statements, with supporting original receipts, must be submitted as a basis of reimbursement for travel costs incurred. Everyone should familiarize him/herself with the travel policies and procedures to avoid miscommunications regarding funds available in advance for travel.

Auditor’s Overview: The purpose of reviewing this area is to ensure that campus units have an organized approach for authorizing travel correctly and reimbursing only those expenses that are allowable according to Institute policy and state law.
Best Practices:
1. The unit head authorizes all travel for the employees of the unit in advance of the travel via on-line Travel Authorization and Expense Reimbursement (T&E) system in TechWorks or delegates, in writing, the authority to authorize travel to someone in the unit.
2. The unit head’s immediate superior or that superior’s designated representative is responsible for authorizing travel made by the unit head.
3. The unit head communicates the importance of this issue to the entire unit, enlisting their full cooperation in this matter.
4. Each unit is responsible for assigning a T&E Administrator to manage the set-up of supervisors, preparers, delegates and financial approvers for their unit.
5. All documentation is reviewed thoroughly for errors and compliance with Institute policies prior to being forwarded to Accounts Payable for reimbursement.
6. Expense reports and related receipts should be submitted to Accounts Payable via T&E system within 45 calendar days of the last day of travel.

Process
TRAVEL APPROVAL
Ensure that everyone in the unit understands that all travel must be approved by the unit head or other designated individual prior to the travel. The unit head should set the example by having his/her travel approved by the next level of management.

DELEGATION AND AUTHORITY
The unit head must select one or more persons who can be trusted to exercise the care and attention necessary to accomplish a reliable system for tracking and controlling travel documentation. This person is then given BOTH the responsibility AND the authority to see that the job gets done, from Travel Authority Requests (TAR) to expense reimbursements. It is important that this delegation be in writing; written authorization provides reasonable assurance to the individual and to outside entities of the authority extended.

- Double check to ensure that all Travel Expense Statements are properly completed.
  “Properly completed” means that the TES is mechanically accurate (everything adds up), supported by original documentation, and contains no personal or unallowable expenses.
- Compare the TES to the TAR. Is the purpose stated for the trip the same on both documents? Are the travel dates in agreement on both documents?

COMMUNICATION
Everyone in the unit has to understand that responsible travel practices ensure compliance with policies and regulations, promote the most economical use of state and sponsored funds, and reinforce public confidence in faculty and staff as responsible professionals. This communication may be accomplished via email, memo, meeting topics, and/or one-on-one conversations.

DISSEMINATE POLICIES AND PROCEDURES
The first basic step is for the responsible person to familiarize him/herself with the policies and procedures contained on Georgia Tech’s web page. These policies and procedures can be found at the Georgia Tech Policy Library which is located at:
VI. Cash and Receivables

**Description of Risk:** Cash is the most liquid of assets, susceptible to loss if not properly controlled. Improper or unauthorized invoicing by individuals can result in loss of receipts if not prohibited. Units may not realize that open invoices at year-end must be recorded on the Institute's financial records.

**Criteria:** The Georgia Tech Policy Library, Section Business and Finance, covers the rules and regulations over cash receipts and accounts receivables. These are web accessible at [http://www.policylibrary.gatech.edu/business-finance/cash-receipts-and-accounts-receivable](http://www.policylibrary.gatech.edu/business-finance/cash-receipts-and-accounts-receivable)

**Auditor’s Overview:** The Bursar’s Office is the primary unit for collecting and depositing all Institute cash, checks, credit cards, and wire transfers. Auxiliary Services and Business Office units may collect and deposit funds with the Bursar as a part of their normal operations, but there are few reasons for academic units to handle cash. Units that do collect cash should ensure timely deposits, secure funds, and segregation of duties over the cash handling process. Most units should refer persons wanting to pay funds to the Bursar or other, applicable units. Likewise, cash and checks sent through the mail should be forwarded to the Bursar for deposit.

Although any unit may have a petty cash account, these accounts are usually made available to provide change for cash collection activities. Further, petty cash accounts are generally needed by academic units only if the unit is located off-campus, or has an off-campus office, which requires funds for small purchases. In rare cases, and only with approval of Accounting Services, should any unit establish or use an external checking account.

If a campus unit has a specific need to prepare and issue its own invoices to a third party, it must have the specific approval of Accounting Services or Grants and Contracts Accounting, respectively. This approval can only be provided upon acceptance by the unit to perform this activity using standards approved by these Accounting Services or Grants and Contracts Accounting.

**Best Practices:**
1. A review should be conducted annually to determine the nature and extent of the unit’s cash handling activities.
2. Empower one person with the responsibility and authority to administer the unit’s cash collecting activities.
3. Prepare and document internal control processes and procedures over this function.
4. Ensure that separation of duties is embedded in the internal cash handling activities.
5. Ensure that all funds collected are secured under lock and key until deposited.
6. Deposit receivables in a timely manner.
7. Units are advised to let Accounting Services handle the invoicing function.
8. Institute revenue ledger account(s) should be regularly reconciled.

Process

ANNUAL REVIEW
Annually, all units should determine how cash is coming into the unit and why. All units may receive cash, even if delivered by mail in error. An annual review should identify all sources of funds so that management can determine if current processes and procedures to control these funds are reasonable and necessary. This is also the time to remind personnel of their responsibilities for cash handling.

DELEGATION AND AUTHORITY
If the unit is involved in cash handling processes, one person in the unit should be assigned oversight responsibility for this activity. That person will be responsible for ensuring that internal unit processes for cash handling are in compliance with Institute and internal policies and procedures, support staff is properly trained, cash is properly safeguarded until deposited, and that internal detail records are regularly reconciled to appropriate revenue ledger account(s). The oversight individual should ensure that separation of duties is imbedded in this process.

This means that a person, who actually handles cash and checks, or issues invoices, should not have the ability to enter data into the corresponding Institute accounts, or have any reconciling duties. Strong compensating controls need to be in place if this cannot be done.

DISSEMINATE POLICIES AND PROCEDURES
The unit should develop and document internal policies and procedures on cash handling, even if just to operate a (small purchase) petty cash account. These are needed to provide appropriate personnel with the unit-specific details for the more general Institute policies and procedures. These may address such issues as:

• Why the unit collects cash or issues invoices
• Assignment of specific responsibilities and timeframes for task completion
• Cash register operation and daily register tally
• Receipt, deposit, & invoice forms to use
• Approval process for significant steps
• Deposit preparation steps
• Georgia Tech Police procedures for making a deposit with the Bursar’s Office, and/or a procedure for armored car pick-up
• What to do if a shortage or theft is discovered
• How cash is safeguarded until deposit, and who has the safe combination and/or strong box key(s)
• Processes for maintaining detail internal records
• Who sets-up and reconciles ledger accounts
• Required year-end actions

CASH HANDLING PROCEDURES
Accountability in cash collection processes is paramount. It is a disservice to employees when a unit’s poor processes make them suspect for theft or shortages by others.
Each department/unit is responsible for the funds it receives for the Institute. Cash receipts must be officially recorded by approved validating equipment or in official pre-numbered receipt books. All checks in payment of amounts due the Institute must be made payable to "Georgia Institute of Technology." Department heads should make certain that proper safekeeping facilities are available and that proper safeguards are taken to protect Institute funds until they are appropriately deposited with the Bursar's Office or as otherwise designated. This may be accomplished by such means as, a fireproof safe, a locked desk drawer, or other locked device. The monetary cost should be a consideration when choosing the actual locking device. Further, more than one member of the unit should have access to the device in the event that the primary person responsible is absent. Funds accepted by the unit, which exceed $100, should be deposited with the Bursar by the next business day. Following these policies reduces the risk of loss and ensures accurate Institute financial records. If you have specific questions regarding cash handling procedures, contact the Director.

INVOICING PROCEDURES
Grants and Contracts Accounting is responsible for invoicing sponsored activities, the Bursar is responsible for invoicing students, and Accounting Services is responsible for invoicing third parties for non-sponsored activities. If a campus unit has a specific need to prepare and issue its own invoices to a third party, it must have the specific approval of Accounting Services or Grants and Contracts Accounting, respectively. This approval can only be provided upon acceptance by the unit to perform this activity using standards approved by these business units. All units doing their own invoicing are required to coordinate with Accounting Services at year-end on their outstanding invoices, for proper accrual and/or possible write-off action.

RECONCILIATION
Institute revenue ledger account(s) should be regularly reviewed to ensure that deposited amounts were correctly posted. Although rare, errors can occur and deposits may be recorded to the wrong revenue account. This should be part of the regular monthly reconciliation process between the ledger account total and internal records.

Related Issues:
Holding Cash/Non-payroll Checks
The Institute’s policies and procedures address how Institute cash should be handled. However, it may not always be apparent what to do with checks that are not made out to the Institute, or that are made out to the Institute but sent to your unit in error. The general rule in these cases is to send the cash/checks to the Bursar’s Office for proper identification and disposition. The mailing envelope and any other documentation should be attached, to aid in this process. The unit should exercise the same care and protection as afforded Institute funds in safeguarding these items until receipt by the Bursar.

Third Parties
For any number of reasons, third parties may be on campus or using Institute physical facilities. Generally, the Institute has no responsibilities in safeguarding or protecting any funds these third
parties collect or have on the premises. Units, however, should include this as a risk discussion topic when discussing overall risk conditions with the Office of Insurance and Claim Management.

Club Funds
There may be times when Institute personnel collect and/or store cash and checks on campus, as a part of their external association duties. Generally, the Institute has no responsibilities in safeguarding or protecting an outside organization’s funds. However, if the Institute sponsors the external group, provides them with free office space or other benefits, or even encourages the association or person in this relationship, there may be an implied responsibility to ensure the organization is handling cash in a reasonable and prudent manner. The unit head has a responsibility to make sure the individual is made aware of Institute resources available to assist in this endeavor.

VII. Procurement

Area of Risk: Procurement

Description of Risk: If campus units do not follow good purchasing practices, they may violate state laws, rules, or regulations, and expend funds in an uneconomical manner.

Criteria: Procurement and Business Services, under the direction of the Associate Vice President for Financial Services, is responsible for the procurement of all materials, supplies, equipment and services required by all departments and units of the Georgia Institute of Technology. This responsibility includes, but is not limited to, the following:

- Establishing all purchase contracts, except rentals, purchase of real property, or facility contracts (architects, construction, etc.) entered into on behalf of the Institute for all supplies, materials, equipment, and services. These include, but are not restricted to, equipment, supplies, printing, surveys and consultant services.
- Assuring that all purchases made are properly authorized and result in proper quality goods or services being delivered to the designated location, at the right time, in the right quantity, and at the best possible cost.
- Maintaining and operating a Central Receiving Department which has the responsibility of receiving, checking, and redelivery of supplies, equipment, and materials ordered for the campus that are not shipped directly from the vendor to the department requisitioning the order. This unit also controls the return of merchandise for reasons as necessary.

Guidance for the performance of these functions and responsibilities is provided from several sources. The primary authorities are:

- The Department of Administrative Services, the Agency empowered by the Purchasing Act, State of Georgia Annotated Code 50-5.
- State of Georgia Agency Purchasing Manual
- State of Georgia Vendor Manual
• Georgia Institute of Technology Policy Library, Business and Finance, Purchasing and Account Payable can be found at http://www.policylibrary.gatech.edu/business-finance/purchasing-and-accounts-payable
• Institute Policies and Procedures regarding PCards can be found at http://www.policylibrary.gatech.edu/business-finance/procurement-cards-pcard
• Institute Policies and Procedures regarding Petty Cash can be found at http://www.policylibrary.gatech.edu/business-finance/petty-cash

Auditor’s Overview:  The importance of this subject is to ensure that campus units understand and follow the appropriate procurement procedures. There are several types of procurement that may be accomplished by campus units. These include (1) Procurement card (PCard), (2) Departmental Purchase Order (DPO), (3) Petty Cash, and (4) those via contract through procurement services. The procurement source utilized is based upon the dollar amount of purchase and/or type of purchase.

Best Practices:
1. Gain a working knowledge of procurement policies and procedures
2. Attend procurement training
3. Develop internal policies and procedures on procurement and disseminate.
4. Empower PCard Coordinators with the responsibility and authority to oversee this process
5. Empower one person as the unit’s central authority for handling invoices and DPO’s
6. Empower one person as the unit’s petty cash fund custodian
7. Ensure that petty cash is adequately secured
8. Petty cash should be subject to proper supervisory oversight
9. Retain all appropriate supporting documentation to validate the authenticity of the transaction and to make it available for audit and/or review if requested

Process
DELEGATE AND COMMUNICATE
Unit head should designate an individual within the unit as the unit’s Departmental Procurement Coordinator, responsible for the overall process; a PCard Coordinator, a Petty Cash Custodian, and communicate this decision to the entire unit. Delegation of this authority does not relieve the unit head of ultimate responsibility for this activity. He or she should develop managerial assurance that the unit is in compliance with internal and Institute policies and procedures regarding these areas. This may be accomplished by instituting a feedback mechanism so that regular reports are directed to the unit head on a periodic basis. The unit should examine the purpose of the petty cash fund annually. The examination should answer such questions as: Why do we have petty cash? Could we accomplish the same thing using the PCard system? Are the funds properly secured? Is the dollar amount of the fund too high or too low? Who is handling the fund? Should this responsibility be rotated?

All procurement activity should be reconciled to the accounts payable information for the unit.
While the Institute requires PCard Coordinators to attend formal training, training for all PCard holders is important. Online training can be found at: http://www.trainsweb.gatech.edu

VIII. Telecommunications

**Description of Risk:** If transactions are not reviewed for reasonableness and accuracy, inappropriate charges, errors, omissions, or abuses could go undetected.


**Auditor’s Overview:** The importance of this subject is to ensure that campus units are implementing procedures to effectively use communication services and equipment at the lowest possible cost, and that there are internal controls to ensure that Institute resources are properly protected from abuse.

**Best Practices:**
1. Empower one person with the responsibility and authority to oversee this process
2. Management communicates the importance of this issue to the entire unit, enlisting their full cooperation and compliance in this matter
3. Develop internal policies and procedures on telecommunications and disseminate these to the entire unit to promote compliance in this area
4. Protect telephones accessible to the public from improper long distance calls
5. Review and verify long distance and cellular phone bills in a timely manner
6. Retain GTA bills and any other supporting documentation in accordance with the Institute retention guidelines
7. Hold unit personnel accountable for telecommunications equipment (i.e. telephone sets and other devices); conduct an annual inventory on telecommunications equipment
8. Ensure your unit's telecommunications closet is adequately secured to reduce the potential for fraudulent activity
9. In moving telecommunications equipment from one location to another, ensure information regarding the move is properly recorded

**Process:**
**EMPOWER THE PEOPLE RESPONSIBLE**
The first basic step is for the Dean, Chair, or Director to decide on one person that can be entrusted to exercise the care and attention that will be needed to accomplish adequate oversight over telecommunications. The person has to be given BOTH the responsibility AND the authority to oversee the entire process.
COMMUNICATE WITH EVERYONE
Development of an awareness campaign begins with management’s communication and dissemination of internal policies and procedures on telecommunications. Management establishes the tone from the top that will affect how the entire unit handles telecommunications in the day-to-day operations of the unit. This will also determine how challenging your job will be in executing your responsibilities. Be proactive, review Institute and the unit’s internal policies and procedures. If the need arises, consider refreshing user responsibilities regarding telecommunications at faculty and staff meetings.

EXECUTION OF POLICIES AND PROCEDURES
The following are suggestions on implementing other best practices:

- **Restrict public telephones** from long distance service by completing and submitting a work order form: [http://www.remedy.gatech.edu/telephone/](http://www.remedy.gatech.edu/telephone/) to OIT Telecommunications Department.
- Encourage faculty and staff to **secure workspaces** to ensure inappropriate calls are not made from unattended telephones. Additionally, the same may be said for being aware of who is entering and leaving your workspaces during business hours.
- Ensure **vacant workspaces** with telecommunications equipment are **properly secured** regardless if the telephone equipment has or has not been disconnected from phone service.
- **Maintain documentation** of all telecommunication lines, sets, and other equipment, individual assigned and its location. This documentation may be stored in any format you deem allows for the best means to manage the information (i.e. excel spreadsheet). At least annually, conduct an inventory to verify telecommunications assets are where you think they should be.

ENSURE ACCURACY OF INFORMATION
Ensure Accounts Payable is aware of your units’ designee for review of the GTA monthly phone bills for timely receipt. Develop a process to **review phone bills** and for contacting individuals for questionable charges. This contact may be face-to-face, by phone call, or by email. You must determine what provides the most efficient method of obtaining resolution of questionable charges by individuals within your unit.

Further, it is important for the unit to maintain adequate records of questionable charges and cost associated with the call(s) to assist in reimbursement process. The Institute has extended the responsibility for maintaining this documentation to the individual units. Internal policies and procedures should reflect operational procedures relative to how the reimbursement will be handled by the unit. The unit should ensure the Long Distance Call Reimbursement Form ([http://www.policylibrary.gatech.edu/book/export/html/1072](http://www.policylibrary.gatech.edu/book/export/html/1072)) is used to document the reimbursement prior to depositing these funds with the Bursar’s Office.

Additionally, **get to know OIT Telecommunication Services**; this area is the appropriate contact for inquiries regarding your telephone bill. OIT Telecommunication Services may be contacted by (404) 894-7173, Option 3. For additional information regarding OIT Telecommunication Services reference their web site at:
IX. Insurance and Claims Management

**Description of Risk:** Institute assets may be put at risk should the unit incur liability above the Institute’s self-insured limits.

**Criteria:** Insurance and Claims Management Policies are written for the faculty, staff, and students of Georgia Tech. These policies may be accessed via the Policy Library at [http://www.policylibrary.gatech.edu/campus-use-facilities/insurance-and-claims-management](http://www.policylibrary.gatech.edu/campus-use-facilities/insurance-and-claims-management). They are intended to assist those who may have questions concerning risk, liability, insurance coverage and workers compensation. Final approval of all claims rests with the Georgia Department of Administrative Services. In addition, all suits and legal actions become the responsibility of the Board of Regents and the Department of Law.

Insurance and Claims Management is responsible for protecting the assets and resources of the Georgia Institute of Technology. This involves the identification and evaluation of potential exposure to loss. It includes the reduction of the loss potential and the selection of the most appropriate technique for treating the loss exposure.

**Auditor’s Overview:** The importance of this subject is to ensure that campus units are taking adequate measures to protect the physical and financial assets of the unit by ensuring that appropriate insurance needs are met, and associated risks are identified.

**Best Practices:**
1. Empower one person with the responsibility and authority to oversee this process
2. Communicate the importance of loss prevention and control to the entire unit, enlisting their full cooperation and compliance in this matter
3. Identify areas of risk for the unit and develop a plan to control these areas of risk
4. Develop internal policies and procedures on risk management and disseminate to the entire unit to promote compliance in this area
5. Determine proper insurance coverage exists for normal and extra-curricular activities sponsored by the unit
6. Develop a process for issuance and control of door keys and access cards
7. Report all incidents that present a risk to the Institute

**Process:**
Delegation and Authority
Empower one person with the responsibility and authority to oversee this process. The first basic step is for the Dean, Chair, or Director to decide on one person that can be entrusted to exercise the care and attention needed to accomplish adequate oversight over risk management. The person has to be given BOTH the responsibility AND the authority to oversee the entire process.
Communication
Communicate the importance of loss prevention and control to the entire unit, enlisting their full cooperation and compliance in this matter. This may be accomplished by development of an awareness campaign. It begins with management’s communication about risk management and dissemination of internal policies and procedures. Management establishes the tone from the top that will affect how the entire unit handles risk management in the day-to-day operations.

Identify and Control Risks
Identifying perils and risk exposures is probably the most important step in the risk management process. If a poor job of exposure identification is done and risk exposures are not recognized, the entire risk management program will suffer. Therefore, it is extremely important that a thorough job of exposure identification is accomplished. The process of identifying risk exposures is a continuous one. Organizations are dynamic, and the composition of the organization's employees, programs, resources, and environment are in a state of constant change. Because of these dynamics, the organization is constantly subjected to changing exposures. Consequently, a single effort to identify risk exposures simply provides a "snapshot" of the exposures at one point in time. Subsequent risk exposures may not be included in the snapshot. **Periodic updates of risk exposure identification must be conducted.**

Several methods could be used to identify risk exposures, such as:

- Checklists, surveys, and questionnaires
- Reports
- Flowcharts
- Professional expertise
- On-site inspections

Unit Sponsored Activities
Determine whether proper insurance coverage exists for normal and extra-curricular activities sponsored by the unit. The unit should define what “normal” and “extra-curricular” activities. Insurance and Claims Management Services may require a certificate of insurance, and/or signed release and waiver of liability when formalized activities, groups, concerts, shows, performances, athletic events, and presentations require the use of campus facilities. This applies especially to outside parties.

Any Institute group, department, or individual contemplating any activity described above, or involved in activities promoted by others must call Insurance and Claim Management Services at 404-894-3483, or write Risk Management Services mail code 0259 as soon as it is reasonably convenient. An events questionnaire must be completed to determine all risk factors and needs. Finally, take a step back and examine these processes even if your current methods have remained the same for some period of time.

Access to Unit
Develop a process for issuance and control of door keys and access cards. Ensure the inventory of unissued door keys and access cards is secured. Documentation should exist for all door keys.
and access cards issued to faculty, staff, and students. For access cards, periodically obtain a list of the individuals who have access cards and review their access privileges.

 INTERNAL CONTROL GUIDANCE: HUMAN RESOURCES

X. Leave Reporting

Area of Risk: Leave Reporting

Description of Risk: Improper compensation could result from inaccurate vacation sick leave record keeping, which may be immaterial individually, but material for the Institute as a whole.

Criteria: The Institute’s Policy Library, Employment, entitled Time Away From Work contains descriptions and policies regarding types of leave available to employees at http://policies.gatech.edu/employment/time-away-work

Auditor’s Overview: The purpose of reviewing this area is to ensure that campus units have in place a system that ensures accuracy of vacation and sick leave by all applicable employees.

Best Practices:
1. Communicate the Institute’s leave reporting practices to the unit employees; training resources are available at http://www.ohr.gatech.edu/timeout/training
2. Designate an individual (and alternates) within the unit the responsibility for overseeing the leave reporting process
3. Verify and/or ensure accuracy of the unit employees’ reporting relationships; if modifications are needed, contact hr.ask@ohr.gatech.edu
4. Ensure supervisors acknowledge/approve monthly time reported by unit employees
5. Notify individuals who have not reported their monthly leave balances
6. Time Reporting policy and necessary forms for hourly paid employees are available at: http://www.policylibrary.gatech.edu/employment/time-reporting

Process:
SET THE TONE AT THE TOP
We recommend the unit head ensure faculty and staff understand their responsibilities regarding monthly leave reporting. This may be accomplished by composing, approving, and distributing written policies and procedures internal to the unit.

REPORTING
OHR launched a new leave management system, TimeOut. The system provides monthly-paid faculty and staff an online system to request and report vacation, sick, paid military leave,
consulting and court leaves. Employees are required to submit their monthly time report even if they did not take any time off. Supervisors can electronically approve and view employees’ leave report, correct leave reports and verify leave. Employees can access TimeOut through Techworks http://www.ohr.gatech.edu/timeout

Related Issue:
Termination/Retirement: Remember when an employee resigns or retires, payments for accrued vacation leave or credit for sick leave are to be based on the official Institute leave balance as supported by TimeOut.

XI. Off-Campus Assignments

Area of Risk: Off-Campus Assignments

Description of Risk: Failure to comply with Board of Regents, and Institute Policies and Procedures regarding off-campus assignments could subject the Institute to risk of loss by compensating employees for activities that are not conducted in the best interest of the Institute, and could result in negative publicity.

Criteria: The Board of Regents (BOR) Academic and Student Affairs Handbook, Section 4.9.2, discusses “Educational and Professional Leave”:

http://www.usg.edu/academic_affairs_handbook/section4/handbook/C695

Institute policy on “Professional Absence and Leave Policies” contains detailed policy for faculty:

http://www.policylexury.gatech.edu/faculty-handbook/3.1.4-professional-absence-and-leave-policies

Auditor’s Overview: The purpose of reviewing this area is to ensure that campus units have in place a system that ensures that off-campus assignments are reported, documented, approved in advance, and monitored.

Best Practices:
1. The Unit Head communicates, in written policies and procedures, the internal process for acceptable documentation and approval of absences from the campus for professional and other activities.
2. All faculty and staff members should be aware of Board of Regents and Institute policies and procedures regarding off-campus assignments. Periodic reminders during faculty and staff meetings will serve to reinforce Board of Regents policies and procedures.
**Process:**
DEVELOP AND EXECUTE INTERNAL PROCESS FOR PROFESSIONAL LEAVES OF ABSENCES
Responsible unit staff should familiarize themselves with Board of Regents and the Institute’s policies and procedures pertaining to professional leaves of absences. The unit should communicate to employees, on a periodic basis, the Institute’s policy pertaining to professional leaves of absences. This may be accomplished through reminders at faculty/staff meetings, correspondence with employees, or unit internal procedure manuals. A designated person in the unit should establish a procedure to ensure the receipt of all requests for professional leaves of absences. The designated person should ensure that the unit obtains required approvals of professional leaves of absences and that such approvals are documented within the unit.

**XII. Employment Eligibility Verification**

**Area of Risk:** Employment Eligibility Verification

**Description of Risk:** Failure to complete and maintain required documentation for employees of the Institute could subject the Institute to fines and penalties imposed by the U.S. Immigration and Naturalization Service, a hold put on hiring of non-resident aliens, as well as adverse publicity. These documents are subject to review during U.S. Department of Labor, Office of Federal Contract Compliance Programs audits.

**Criteria:** The Immigration Reform and Control Act of 1986 require employers to verify the identity and employment eligibility of anyone hired after November 1986. It is unlawful to knowingly hire, or to continue to employ, any individual not authorized to work in the U.S. Form I-9, Employment Eligibility Verification, was developed for verifying that persons are eligible to work in the United States. Institute requirements call for a new employee to complete Form I-9 on the first day of employment and present required forms within the first three days of employment. Also, policy requires the tracking of expiration of employment authorization documents held by non-resident aliens. Institute hiring departments are responsible for advising new employees of the time frame and documentation required to complete or update Form I-9s.

**Auditor’s Overview:** The purpose of reviewing this area is to ensure that campus units advise new employees of the need to contact Human Resources to complete Form I-9, Employment Eligibility Verification, before they work in the unit.

**Best Practices:**
1. The Unit Head empowers one person with the responsibility and authority to advise new employees regarding the completion and updating of Form I-9, entitled Employment Eligibility Verification.
2. The appointed administrator advises new employees that they are to report to Human Resources to complete required paperwork, including Form I-9, before they are permitted to work in the unit.

3. The appointed administrator establishes the appropriate contact with the Office of Human Resources in order to be informed on the tracking of expiration of employment authorization documents held by non-resident aliens in the unit. The unit administrator advises applicable personnel of the need to update Form I-9s.

**Process:**
**EMPOWER THE PEOPLE RESPONSIBLE**
The Unit Head appoints a person within the unit to ensure compliance with the Immigration Reform and Control Act of 1986, which requires employers to verify the identity and employment eligibility of new employees.

**EXECUTION OF POLICIES AND PROCEDURES**
The appointed administrator should put in place a process to ensure compliance with the Immigration Reform and Control Act. Some tasks an administrator might do to implement a compliance process are:

- Familiarize him/herself with the “New Hire Documents” on OHR website: [http://www.ohr.gatech.edu/NewHireDocuments](http://www.ohr.gatech.edu/NewHireDocuments)
- Formalize approach for assuring compliance with Form I-9 procedures
- Communicate procedures to staff, as applicable
- Communicate Form I-9 requirement to staff in pre-employment correspondence and when they initially report to the unit
- Establish lines of communications with the Office of Human Resources in order to track and notify non-USA citizens of the expiration of work authorization documents and the need to update Form I-9s

XIII. **Sexual Harassment**

**Area of Risk:** Sexual Harassment

**Description of Risk:** Sexual harassment can (1) alienate employees, (2) create a hostile work environment, (3) result in lawsuits, fines, and penalties for violations; and (4) cause adverse publicity.

**Criteria:** It is the policy of this Institute that no member of its community, including administrators, faculty, staff, or students, should be subjected to sexual harassment by another. This policy and procedure is intended to create an atmosphere in which individuals who believe that they are the victims of harassment are assured that their complaints will be dealt with fairly and effectively. Toward this end, the Georgia Institute of Technology supports the principle that sexual harassment represents a failure in ethical behavior, and that sexual exploitation of professional relationships will not be condoned.
Sexual harassment is defined as unwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature when: (1) submission to such conduct is made, either explicitly or implicitly, a term or condition of an individual's employment or academic standing; or (2) submission to or rejection of such conduct is used as the basis for employment or academic decisions affecting the individual; or (3) such conduct has the effect of unreasonably interfering with an individual's work or academic performance or creates an intimidating, hostile working, or academic, environment. Both men and women may be either the initiators or victims of sexual harassment. Complaints are to be directed to the Employee Relations unit for faculty and staff members and to the Dean of Students for students. Institute officials may require an investigation. The Associate Vice President for Human Resources or the Vice President for Student Affairs will review the results of the investigation and take or recommend appropriate disciplinary and/or other action. Individuals subject to disciplinary action may exercise their appeal rights pursuant to the procedures set forth in the Faculty Handbook, the Classified Employee Handbook, or the Student Conduct Code as appropriate.

Auditor’s Overview: The purpose of reviewing this area is to ensure that campus units have in place a system that communicates with staff and students the importance of an environment free of sexual harassment and a means of dealing with situations in which a person believes they have been subjected to sexual harassment.

Best Practices:
1. The Unit Head communicates the importance of the prevention of sexual harassment in the unit on a periodic basis
2. An individual, or individuals within the unit, are designated as contact points for employees to be referred to the appropriate level for counsel in instances where they believe they have been sexually harassed
3. All faculty and staff should be trained on preventing sexual harassment. http://trains.gatech.edu/

Process:
SET THE TONE AT THE TOP
Ensure that everyone in the unit understands that the Institute’s policy is that no member of its community should be subjected to sexual harassment by another and if an employee or student believes they have been subjected to such harassment there is a means to deal with the matter fairly and effectively.

DEVELOP AND EXECUTE SEXUAL HARASSMENT PREVENTION PROCEDURES
- Responsible unit staff should familiarize themselves with the Institute’s sexual harassment policy and procedures. The Institute’s policy can be found in the following:
  - Policy Library, Student Affairs, Other Academic Student Policies at: http://www.policylibrary.gatech.edu/student-sexual-harassment-misconduct-policy
• The unit should communicate to all employees, on a periodic basis, the Institute’s policy on sexual harassment. This may be accomplished through reminders at faculty/staff meetings, correspondence with employees, or through unit internal procedure manuals.
• Unit should encourage employees to attend training on sexual harassment offered by the Institute.
• Deal effectively and fairly with any complaints of sexual harassment in accordance with Institute policy.
• No member of the community may, under any circumstances use Georgia Tech’s computers or network to create a hostile work environment.

XIV. Consultants vs. Employees

Area of Risk: Consultants vs. Employees

Description of Risk: Improper classification of independent contractors/employees could result in the Institute being out of compliance with Internal Revenue Service (IRS) regulations, thereby increasing the liability of tax penalties and fines, as well as negative publicity.

Criteria: Georgia Tech’s Policy Library, Consultants (Individuals and Firms) [http://www.policylibrary.gatech.edu/business-finance/consultants-individuals-and-firms](http://www.policylibrary.gatech.edu/business-finance/consultants-individuals-and-firms) provides guidelines for determining job classification of independent contractors versus employees. When the Institute is required to make payments to individuals, a determination must be made to ensure that payment clearly meets the IRS definition of independent contractor. Any individual who performs services for the Institute is presumed to be an employee unless the relationship satisfies the IRS standards for Independent Contractor. The campus unit must examine the issue of whether an individual is an employee or independent contractor because of the familiarity of the relationship. If the answer is “yes” to any of the following questions, the individual must be treated as an employee.

• Does the individual provide essentially the same service as an employee of the Institute?
• Is the individual a current employee (or within the previous 12 months) of Georgia Tech providing the same or similar services?
• Is it expected that the Institute will hire this individual as an employee immediately following the termination of his/her services as a consultant?
• Does the Institute control how the individual will perform or accomplish the service?
• Will the individual supervise or control Institute employees in accomplishing the service?

If any of the above questions are answered as “yes,” or if there is any doubt regarding the issue, the campus unit should consult with the Office of Human Resources. If there is uncertainty about any of the questions, the Office of Legal Affairs is to be contacted for assistance. If all answers are “no” to the questions above, the individual may be paid as an Independent Contractor.
Auditor’s Overview: The purpose of our audit in this area is to ensure that campus units, when contemplating payments to an independent contractor, make a determination to ensure that such payments clearly meet the IRS definition of independent contractor.

Best Practices:
1. Management should designate an individual to monitor instances where payments are contemplated to an individual as an Independent Contractor, to ensure that a determination is made in each instance that such payments are in accordance with IRS guidelines.
2. When contemplating payments to an Independent Contractor, any question in the Institute policy is answered as ‘yes,” Human Resources is contacted regarding hiring the person as an employee.

Process:
- The Unit Head should designate a person responsible for assisting with the monitoring of instances where the unit contemplates payments to an independent contractor.
- The Unit Head should empower the designated person to deal with Human Resources or Legal Affairs on questions regarding contemplated payments to Independent Contractors.
- The designated person should bring to the Unit Head’s attention any instance where in applying the five Institute questions regarding Independent Contractors, a “yes” answer is obtained. The Unit Head should be advised to hire an individual as an employee if any of the applied questions result in a ‘no” answer.

XV. Compliance with Equal Employment Opportunity Laws

Area of Risk: Compliance with Equal Employment Opportunity Act

Description of Risk: The Institute could be subjected to legal actions if the Equal Employment Opportunity Laws are not complied with, resulting in both monetary and adverse publicity impacts.

Criteria: Georgia Tech is committed to affirmative implementation of equal employment opportunity in conjunction with an Equal Opportunity Program that is in keeping with this policy. The Institute will continue to recruit, hire, train, and promote into all job levels the best-qualified persons without regard to race, color, religion, sex, or national origin. Similarly, all other personnel matters such as compensation, benefits, transfers, layoffs, Institute sponsored training, education, tuition assistance, social and recreational programs will continue to be administered in accordance with the Institute's policy. Each administrative officer of the Institute at every supervisory level is responsible for avoiding prohibited bias in the workplace with respect to race, color, religion, sex, national origin, disability, or veteran status. This criterion is in the Institute Policy Library, Section Equal Opportunity Complaint: http://www.policylibrary.gatech.edu/employment/equal-opportunity-complaint-policy
**Auditor’s Overview:** The purpose of our audit in this area is to ensure that campus units have in place a process that assures compliance with the Equal Employment Opportunity Laws.

**Best Practices:**
1. Management has communicated the importance of Equal Employment Opportunity to the entire unit, enlisting their full cooperation.
2. The unit’s hiring and other personnel procedures are administered without regard to race, color, religion, sex, or national origin.
3. Training for managers and supervisors on preventing discrimination.
4. Training for manager and supervisors on conflict resolution.
5. Periodic climate assessments that include EEO issues; for assistance with these assessments, contact the Office of Diversity Programs at [http://www.ohr.gatech.edu/diversity](http://www.ohr.gatech.edu/diversity).
6. Consistency in application of work rules, processes and disciplinary actions.

**Process:**
- The Unit Head should designate a person responsible for assuring compliance with the Equal Employment Act in all unit personnel actions.
- The Unit Head should develop written policies and procedures that detail the requirements of Equal Employment Opportunity and develop a written plan for the development of unit personnel.
- The Unit Head should communicate the Equal Employment Opportunity Act procedures to all employees and emphasize the importance of the Equal Employment Opportunity Act, enlisting their full cooperation.
- The Unit Head should serve as the final checkpoint, assuring that all personnel actions are administered fairly, without regard to race, color, religion, sex, or national origin.

**XVI. Annual Performance Evaluations**

**Area of Risk:** Annual Performance Evaluations

**Description of Risk:** If the unit fails to properly prepare annual performance evaluations for all employees, the employee may not clearly understand what is expected of him or her. The unit may not have a basis for personnel decisions.

**Criteria:** Institute policy is reflected in Employment section, Performance Management Policy: [http://www.policylibrary.gatech.edu/employment/performance-management-policy](http://www.policylibrary.gatech.edu/employment/performance-management-policy)

The objective of the appraisal system is to:
- Provide employees with a sense of their work accomplishments relative to expectations and predefined performance indicators.
- Support employee development through discussion of assigned opportunities and training.
- Emphasize the Institute's commitment to continuous improvement and learning.
- Avoid surprises; keep lines of communication open.
Board of Regents’ policy requires that all faculty members receive an annual, written review by their unit head. In addition, the faculty member is to discuss the review with the unit head and sign a statement to the effect that the faculty member has received the written review. The faculty member has the opportunity to respond, in writing, to the evaluation, and to receive a written response from the supervisor to the comments of the faculty member. Both the faculty member’s comments and the response will then become part of the record.

**Auditor’s Overview:** The purpose of our audit in this area is to ensure that campus units have in place a process that ensures the accomplishment of employee performance evaluations in accordance with Institute policy.

**Best Practices:**
1. Ensure that everyone responsible for employee reviews has had appropriate training; more information on training can be found at: [http://www.ohr.gatech.edu/performance](http://www.ohr.gatech.edu/performance)
2. Management has developed and communicated to employees the policies and procedures that detail the requirements of Annual Performance Evaluations
3. Establish specific performance goals and objectives annually
4. Establish an annual employee development plan
5. Provide regular communications and feedback on performance

**Process:**
- The Unit Head should designate a person responsible for assisting with the monitoring of the Annual Performance Evaluation process and the accumulation of the required documentation in order to meet the Institute’s schedule
- The Unit Head should develop policies and procedures that detail the requirements of the Annual Performance Evaluation process
- The Unit Head should communicate the Annual Performance Evaluation procedures to all employees, enlisting their full cooperation
- The Unit Head should serve as the final checkpoint for all performance evaluations, assuring that all evaluations are administered fairly, without regard to race, color, religion, sex, or national origin

**INTERNAL CONTROL GUIDE: LEGAL AND REGULATORY**

**XVII. Contracts**

**Description of Risk:** The Institute may incur unintended financial obligation, legal liability, or negative public opinion if unauthorized employees act as agents of the Institute in contracting with third parties. Also, employees are personally liable because they unknowingly contract in the name of the Institute.

**Criteria:** According to the Institute’s “Contracts” policy, [Contract Policy Link](http://www.ohr.gatech.edu/performance), very few people within the Georgia Tech community are authorized to sign contracts on behalf of the University.
Those authorized to sign contracts include the President; the Vice President for Finance & Administration; the Vice President for Research; Purchasing Agents; and certain staff of the Office of Contract Administration.

The authority to sign a purchase order does NOT give a member of the Georgia Tech community the authority to sign a contract. No member of the faculty or staff may sign a contract without specific written authorization from the President to do so. State law provides that persons entering into contracts without complying with all applicable state laws and regulations become personally liable for any amounts due under those contracts.

Auditor’s Overview: The purpose of reviewing this area is to promote awareness of the issue of restrictions on signing contracts on behalf of Georgia Tech. A contract signed by an unauthorized person, while possibly binding on Georgia Tech, may also create a legal and/or financial obligation for that person. In addition, the Institute may suffer legal entanglements or less than optimal public relations.

Best Practices:
1. Maintain any written authorization from the President to contract that you may have on file in your location
2. Ensure that all faculty and staff are made aware of the restrictions regarding contracting on behalf of the Institute
3. Reinforce this message through periodic discussion of the topic at faculty and staff meetings
4. Seek advice from authoritative sources anytime you are uncertain about a potential contracting situation

Process:
COMMUNICATE WITH EVERYONE
It is a good practice to communicate this issue periodically during faculty and staff meetings. If this is not practical, the issue could be communicated via email, hard copy memo, or postings on bulletin boards, whatever means works most efficiently for your mode of operation.

COMMUNICATE WITH PROCUREMENT SERVICES OR OTHER AUTHORITATIVE SOURCES YOU FEEL ARE NEEDED
If you have any doubt about your authority to make a contractual commitment, contact Procurement Services or another authoritative body. There is strength in numbers and these organizations are meant to be a resource to you so that you do not have to be without advice when dealing with contractual situations.

Related Issues:
The term “contract” may include a letter, document, memo of understanding, email, or other communication that gives the impression to a third party that the Institute is obligating itself in any manner. This activity may or may not involve compensation. It may also include employees bypassing Institute purchasing functions in ordering equipment or supplies for their unit.
XVIII. Gifts

**Description of Risk:** The risk is that accepting gifts could give the appearance of improper preference or treatment in the conduct of normal business activities. If any laws were broken, the individuals involved could be criminally liable and this occurrence could bring significant adverse publicity for the Institute.

**Criteria:** Georgia Board of Regents’ Personnel Manual, Section 8.2.13, Gratuities contains the following: An employee of the University System or any other person on his/her behalf, is prohibited from knowingly accepting, directly or indirectly, a gift from any vendor or lobbyist as those terms are defined in Georgia statutes (O.C.G.A. 21-5-70(6) and 45-1-6(a)(5)b).

The Governor of Georgia issued an Executive Order dated January 13, 2003 that, in essence, precluded state employees from accepting gifts exceeding a value of $25.

**Auditor’s Overview:** The purpose of reviewing this area is to promote awareness of the issue of restrictions on accepting personal gifts. A personal gift accepted by a Georgia Tech employee may create the appearance of improper favoritism towards the gifting party. In addition, the Institute may suffer legal repercussions and/or less than optimal public relations.

**Best Practices:**
1. Ensure that all faculty and staff are made aware of the restrictions regarding accepting personal gifts from potential vendors to the Institute, as sited in the Governor’s memo and the Board of Regents policy.
2. Reinforce this message through periodic discussion of the topic at faculty and staff meetings.

**Process:**
**COMMUNICATE WITH EVERYONE**
It is a good practice to communicate this issue periodically during faculty and staff meetings. If this is not practical, the issue could be communicated via email, hard copy memo, included in the faculty/staff handbook, posted to the web page, or posted on physical bulletin boards; whatever means works most efficiently for your mode of operation.

**COMMUNICATE WITH LEGAL AFFAIRS OR OTHER AUTHORITATIVE SOURCES OF INFORMATION**
If you face any situation in which you are uncertain as to the nature of events or how to proceed, contact Legal Affairs or any other source you feel would be appropriate.

**BE A RESPONSIBLE GEORGIA TECH EMPLOYEE**
All Georgia Tech employees should be familiar with the rules regarding the acceptance of gifts. Adhering to these rules is the responsible professional legal course of action.

**Related Issues:**
The Office of the Vice President for Development handles the receiving of gifts to the Institute. These Institute employees are trained and experienced in appropriate policies and procedures.
concerning the transfer of assets to Georgia Tech. Gifts to individual Georgia Tech employees from vendors, potential vendors, or others, who may benefit from a decision by the gift recipient, may create the appearance of impropriety and should be handled with care. In a situation where giving and receiving of gifts is culturally the norm, seek the advice of the Office of the Vice President for Development as to how to approach the situation.

XIX. Open Records Act

**Description of Risk:** A violation of ORA requirements could result in fines and penalties for the Institute and the record custodian, including criminal liability, as well as adverse publicity for the Institute.

**Criteria:** As a public institution, Georgia Tech is subject to the Open Record Act, O.C.G.A. 50-18-70 et seq. The law requires that Georgia Tech make available for public inspection public documents within three business days of receiving a request. The Institute’s policy regarding ORA is available at [http://www.policylibrary.gatech.edu/open-records-act-policy](http://www.policylibrary.gatech.edu/open-records-act-policy)

Employees receiving ORA requests are instructed to contact their supervisor and Office of Legal Affairs without delay, for assistance in a correct response. Further information is available through Office of Legal Affairs web site [http://www.legalaffairs.gatech.edu](http://www.legalaffairs.gatech.edu) under the subject “topics”. Open records request details should not be released without the approval of the Office of Legal Affairs.

**Auditor’s Overview:** The purpose of reviewing this area is to promote awareness on the issue of the importance of compliance with the Open Records Act. Proper and timely responses to ORA requests ensure legal compliance and responsible stewardship of public information.

**Best Practices:**
1. Ensure that the school or business unit has an explicit plan for responding to ORA requests
2. Ensure that all faculty and staff are informed and periodically reminded of the rules and regulations regarding timely and accurate responses to ORA requests

**Process:**
COMMUNICATE WITH EVERYONE
It is a good practice to communicate this issue at any orientation your unit may have, and periodically during faculty and staff meetings. If this is not practical, the issue could be communicated via email, hard copy memo, included in the faculty/staff handbook, posted on the web page or on physical bulletin boards, whatever means works most efficiently for your mode of operation.

KNOW PROPER ORDER OF RESPONSE
These are:
- Notify your immediate supervisor that you have received an ORA request
- Notify the Office of Legal Affairs that you have received an ORA request
- Begin collecting the materials that have been requested
- Ensure that you have authorization for release from your supervisor or the Office of Legal Affairs prior to releasing the material

INTERNAL CONTROL GUIDANCE: HEALTH & SAFETY

XX. Safety of Workplace

**Area of Risk:** Safety of Workplace

**Description of Risk:** Occupational injury, illness, or death, as well as significant property damage can result from improper training or failure of the Institute to provide a safe working environment. A violation of the State of Georgia’s “Public Employee Hazardous Chemical Protection and Right to Know Act of 1988” could result in future liabilities and adverse publicity for the Institute.

**Criteria:** It is the policy of Georgia Institute of Technology for each unit to develop a safety program per the Institute Safety Policy memorandum issued by the Office of the President dated February 1, 1995. Each department is responsible for working with the Environmental Science, Health and Safety Office, in assessing safety needs and developing a safety program unique to their organization. The Institute’s policy in this area is available at [http://www.policylibrary.gatech.edu/campus-use-facilities/environmental-health-and-safety](http://www.policylibrary.gatech.edu/campus-use-facilities/environmental-health-and-safety)

Furthermore, it is the policy of the Institute that an ongoing Right to Know Program for hazardous chemicals shall be instituted and maintained in order to comply with the State of Georgia’s “Public Employee Hazardous Chemical Protection and Right to Know Act of 1988”. The “Right to Know” training courses are available on the Institute’s Training website at [http://trains.gatech.edu/](http://trains.gatech.edu/)

Campus units should ensure that employees receive all required training and comply with the various rules and regulations pertaining to each of these areas.

**Auditor’s Overview:** The purpose of reviewing this area is to promote awareness on the importance of safety in the workplace and compliance with the State of Georgia’s “Public Employee Hazardous Chemical Protection and Right to Know Act of 1988”.

**Best Practices:**
1. Designate an individual within the unit with the responsibility for ensuring compliance with unit, Institute and state policies
2. Ensure that your unit has an explicit plan for training employees
3. Ensure that your unit has a written training program
4. Ensure that all faculty, staff, and students are informed and periodically reminded of workplace safety

Process:
RESPONSIBILITY AND DELEGATION
The first basic step is for at least one person, usually a supervisor or manager, to have a reasonable understanding of how Institute and state policy affect the unit’s operation. It is this person who is responsible for preparing internal policies and procedures that satisfy all the criteria required by these entities. This person should develop a training program to ensure appropriate training of unit personnel (e.g., faculty, staff, and student workers). Finally, it is this person who will generally enforce policy and procedure adherence among all employees.

Documentation and Compliance, It’s The Law
A written training program should be developed and updated as necessary to maintain currency to ensure consistency in the communication of information provided to employees. The unit may contact the Institutes Environmental Health and Safety Compliance Officer at (404) 894-4635, for identifying safety needs, assistance in developing a safety program, and guidance on safety of workplace compliance. The Environmental Health and Safety Department has developed a general laboratory safety manual (http://www.ehs.gatech.edu/chemical/AAA_Lab Safety Manual April 29 2013.pdf) to provide guidance in the area of laboratory safety.

Regarding the Georgia Right to Know law, all hazardous chemicals used by the unit should be identified and material safety data sheets (MSDS) maintained on each hazardous chemical. The unit must ensure they meet the minimum information standards set forth in the law regarding MSDS. The specific details on acceptable methods for MSDS may be at found at http://www.usg.edu/facilities/rtk-ghs/P40. A central location for maintaining the MSDS within the unit should be identified and a process developed to ensure requests for information are readily available to employees.

Communication
Employees should receive job specific training. The training should include these minimum information standards per the Georgia Right to Know Act:

1. The requirements of Georgia Right To Know section 45-22-8
2. What a material safety data sheet is and the contents of the material safety data sheet for any hazardous chemical to which he is exposed, or equivalent information, either in written form or through training programs
3. Any operations in his work area where hazardous chemical are present
4. The location and availability of training programs
5. His right to receive information regarding hazardous chemicals to which he may be exposed
6. His right for his physician to receive information regarding hazardous chemicals to which the employee may be exposed
7. His right against discharge or other discrimination due to the employee’s exercise of the rights provided by this chapter

A process for identifying and certifying all employees have received training should be developed and records maintained within the unit.

A best practice is to communicate this information at employee orientations your unit may have, periodically during faculty and staff meetings, and in the internal faculty/staff handbook. Various communication methods such as email, hard copy memo, posted on the unit’s web page or on physical bulletin boards, may provide alternative methods for effectively refreshing the topic to employees based on your mode of operation. An online basic awareness Right to Know Training Module provided by the University System of Georgia is a resource tool that may be incorporated into your unit’s initial and/or refresher training. It can be found at:

http://www.usg.edu/facilities/resources/training/

Further, providing general principles of recognition of hazards and injuries, procedures for reporting hazardous conditions and methods and procedures for early reporting of injuries may further inform employees of concepts to reduce risk of workplace hazards and injuries. The University System of Georgia maintains an Environmental Health and Safety Video library, which provides numerous training materials on various subjects free of charge. The videotapes may be requested by members of the University system and would be a great addition to your units Safety in the Workplace Training Program.

XXI. Environmental Protection

**Area of Risk:** Environmental Protection

**Description of Risk:** Georgia Tech is obligated to protect the general and Institute environments by properly managing and disposing of hazardous chemical wastes, and by implementing appropriate construction procedures to prevent visible and asbestos emissions. Furthermore, the Institute could be subject to fines from regulatory enforcement action and negative publicity that could adversely affect research activity and student populations.

**Criteria:** It is the policy of Georgia Tech that hazardous waste be managed and disposed of appropriately in accordance with federal Hazardous Waste Management regulations (40 CFR 260-272) and rules of Georgia’s Department of Environmental Resources and Environmental Protection Division. Furthermore, construction projects must be accomplished in a manner that prevents visible emissions (National Emission Standards for Hazardous Air Pollutants or NESHAP, 40 CFR 70) including compliance with NESHAP and Georgia (1986 Georgia Asbestos Safety Act, Chapter 391) asbestos rules. The Institute policy for managing and disposing hazardous waste can be found at: http://www.ehs.gatech.edu/hazardous/
**Auditor’s Overview:** The purpose of reviewing this area is to determine: (1) Whether the unit has established reasonable policies and procedures for ensuring environmental protection safety and compliance; (2) Whether the unit has ensured that all employees have received required training in the area of environmental protection and hazardous materials; and (3) Whether the unit has in place a monitoring process through which to ensure that all employees comply with rules and regulations regarding environmental protection and hazardous materials.

**Best Practices:**
1. Designate an individual within the unit with the responsibility for ensuring compliance with hazardous waste polices
2. Develop internal policies and procedures
3. Ensure that your unit has an explicit plan for training employees

**Process:**
**RESPONSIBILITY AND DELEGATION**
The first basic step is for at least one person, usually a supervisor or manager, to have a reasonable understanding of how Institute, state and federal policy affect the unit’s operation. The Environmental Health and Safety Department (EHS) have developed a general laboratory safety manual at [http://www.ehs.gatech.edu/chemical/AAA Lab Safety Manual April 29 2013.pdf](http://www.ehs.gatech.edu/chemical/AAA Lab Safety Manual April 29 2013.pdf), which contains the hazardous waste policy, hazardous materials storage and disposal policy, and the policy and procedures for bio-hazardous waste. It is this person who is responsible for preparing internal policies and procedures that satisfy all the criteria required by these entities.

This person should develop a training program to ensure appropriate training of unit personnel (e.g., faculty, staff, and student workers). Finally, it is this person who will generally enforce policy and procedure adherence among all employees. This can be accomplished by establishing an internal monitoring program of facilities where hazardous materials are used to determine adherence with policy. Management should establish the frequency of conducting monitoring. A simple checklist containing policy criteria can be used to record compliance or noncompliance. The results should be communicated to management and other appropriate individuals for resolution of noncompliance issues. The unit should maintain the document and responses.

For direct questions regarding hazardous waste, contact the Hazardous Waste Officer at (404) 894-4635.

**DOCUMENTATION CLARITY**
First and foremost approved internal policies and procedures should be well documented and provided to faculty, staff and students. A more cost effective and efficient means of distributing policies and procedures may be via the unit’s internal web site. However, the unit should make the necessary provisions for individuals who may not have access to the internal web site.

The unit should develop a written training program that provides faculty, staff and students chemical-specific training to ensure consistency in the communication of pertinent information. The training should be updated as necessary to maintain currency. The unit may seek guidance
from the EHS manual at http://www.ehs.gatech.edu/, which contains the hazardous waste policy, hazardous materials storage and disposal policy, and the policy and procedures for bio hazardous waste. Additionally, the unit may contact the Institutes’ Environmental Health and Safety Compliance Officer or the Hazardous Materials Officer at (404) 894-4635 for assistance and guidance.

A process for certifying that appropriate individuals have received required training should be developed and records maintained within the unit. This may be accomplished by identifying individuals who work with hazardous materials by area, and require participants to sign a training attendance sheet or certification statement. A certification statement may include acknowledgement and understanding of policies and procedures, as well as agreement to adhere to accepted workplace practices established by the unit.

COMMUNICATION

Employees should receive job-specific training regarding specific chemicals he will come into contact with prior to commencing work. Along with development of the unit’s training program, a training plan should be developed to ensure that all faculty, staff, and students are informed and periodically reminded of environmental protection. The initial training and frequency of refresher training should be in compliance with policy.

INTERNAL CONTROL GUIDANCE: INFORMATION SYSTEMS

XXII. Strategy and Vision

Description of risk: Because of the increased reliance on information systems to support academic, research and administrative processes, it is important for management within each unit to have a keen awareness of how those information systems resources will be utilized and managed. If unit management does not have a clear view of the required resources to support its mission critical processes, there is a risk that organizational objectives may be hindered. If there is not a connection between the strategic vision for the unit and the available systems and resources to support that plan, there is a risk that organizational objectives may not be met. This could lead to inefficient and ineffective use of resources and possible compromise of Institute data. Without adequate strategy and vision the following may occur:

- Loss of monetary resources
- Loss of proprietary data
- Loss of productivity
- Hardware damage
- Software corruption of proprietary systems
- Compromises of systems
- Expenditure of resources on equipment inadequate to support the business goals of the unit
Criteria: Managing an information system in the campus environment is the most demanding role an administrator can have. Management practice surrounding an information system can affect virtually all aspects of campus business. Unit success is largely dependent on an organization that can take advantage of rapid changes in their field and in technology that support the education process. Management facilitates the executive tasks of strategic planning, budgeting, and assessing the adequacy of information systems to meet Institute needs. Astute units have a plan of progression tied to a timetable, how they intend to get there, and a clear understanding of how this will enhance the learning experience. Specific strategy for management of information systems is left to each campus unit head. There are several guides that can assist in managing the information systems of a unit.

- GAO/AIMD-10.1.13 Assessing Risk and Returns: A guide for evaluating federal Agencies’ IT investment Decision Making
- GAO/AIMD-10.1.23 Information Technology Investment Management
- GAO/AIMD-94-115 Executive Guide to Improving Mission Performance through Strategic Information Management and Technology
- The IT Infrastructure Library (ITIL): A cohesive set of best practices for IT service management. It is comprised of a series of ITIL Books and is intended to assist organizations in developing a quality IT framework.

The previously listed documents provide models for affordable and efficient guides to management of information systems.

Auditor’s Overview: In this time of scarce resources, both human and monetary, strategic planning is essential. We are looking to see that management has a plan, in line with its resources, to maintain and focus the campus unit in line with the strategic plan of the Institute.

Best Practices:
As an overall process:
1. Recognize information resources as an essential organizational asset that must be protected.
   - Information resources should be deployed to enhance the unit’s strategy, objectives, or business needs. Information systems are the catalyst for the transfer of all information and should be recognized as a critical component to achieving business success.

2. Develop a practical information systems strategy and assessment model that links the information systems resource needs to your business plan.
   - Ensure that there is a clear budget for IT investment and that it is tied to the unit and Institute goals.

3. Hold program or business managers accountable for insuring that information systems projects, designs, implementations, and expenditures support a specific business need or strategic goal.
• Have a multi-year plan that addresses technology replacement, upkeep, and management.

4. Manage risk on a continuing basis.
   • Tools for doing this are provided by the Department of Internal Auditing ([http://www.audit.gatech.edu/resources](http://www.audit.gatech.edu/resources)) and the Office of Information Technology ([http://oit.gatech.edu/service/information-security/security-assessments](http://oit.gatech.edu/service/information-security/security-assessments))

5. Designate a central group or authority within the unit to develop information systems priorities and to carry out and implement those key priorities.

6. Provide the central group ready and independent access to senior executives or management within the campus unit.

7. Dedicate funding and staff resources in each year's budget as well as the budget planning process to support technical (Information Systems) needs.

8. Ensure departmental policies on information systems are related to business needs and business risks, in addition to supporting the strategic goals of the unit.

9. Distinguish between policies and guidelines, ensuring that personnel understand the purpose of the information systems resources, the appropriate use of these resources, and how they support the business needs of the unit.
   • Ensure training of users is adequate and is updated regularly.

10. Monitor information system resources and their return-on-investment to determine how well they have supported the strategic goals, business needs, and the mission of the local unit.
    • The Office of Information Technology should be able to assist in this process if necessary.

11. Use these results to direct future efforts and to hold the managers accountable.

12. Use these results to support the unit budgeting process.
    • Prepare for situations such as unexpected monies becoming available and decisions being made to buy based on the unit’s long-term plan vs. impulse buying.

**Process:**
**EMPOWER THE PEOPLE RESPONSIBLE:**
Strategic planning encompasses several areas of accountability: information systems, budget, technical, business, and vision. While management should designate a responsible party for each area of the strategic plan, management remains responsible for the overall strategic plan.
COMMUNICATE WITH EVERYONE IN THE UNIT:
In order to maintain a relevant strategic plan, feedback/input from technical members, users and business managers is a necessity. Management is encouraged to use direct face-to-face methods of communications such as staff meetings, brown bags, and targeted training programs. Management also has at its disposal several supporting methods for communications such as email, the internet, and electronic messaging.

USE A SYSTEMATIC APPROACH:
One approach to creating a successful plan is to take each of the goals outlined in the strategic plan of Georgia Tech and evaluate local unit approaches to supporting it with information technology.

Related Issues:
Georgia Tech Strategic Plan

XXIII. Operations / Administration

Description of Risk: If the unit does not have effective practices in place to ensure that systems are appropriately maintained and administered, it could lead to ineffective and inefficient use of resources. This could, in turn, increase the risk of loss or compromise of information resources, compromise of Institute data, loss of productivity, etc. Just a few of these risks are:

- Loss of Information resources
- Loss of proprietary data
- Loss of productivity
- Hardware damage
- Software corruption of proprietary systems
- Compromise of systems
- Loss of reputation
- High turnover rates
- Decreased system efficiency
- Increased operational costs

Criteria: The Institute’s Computer and Network Usage Security Policy have several sections tailored to the operations and administration of all Institute information systems. The Institute policy establishes Institute guidance and authority for information systems administration. Units supplement this with specific guidance tailored to their information systems.

Auditor’s Overview: Operations are the daily tasks that are needed to keep an information system operational, efficient and effective. The key component in the scheme is the system administrator and their knowledge of the Information systems located within the unit. Effective operations will:

- Keep operation costs as low as possible
- Keep the Unit’s network tuned for maximum speed and efficiency
• Efficiently integrate information resources with the campus unit’s business office processes
• Keep networks reasonably secure

**Best Practices:**

1. Have an information systems plan
2. Have written policies regarding information systems usage
3. Hire qualified personnel
4. Document controls and incident response procedures
5. Have a formalized problem tracking and resolution process
6. Have an up-to-date list of authorized users and software
7. Conduct routine audits of system logs and individual work stations
8. Conduct routine tests of backup systems and procedures
9. Have procedures for identifying and authenticating users and deleting them
10. Have procedures to backup mobile assets such as laptops

**Process:**

**EMPOWER THE PEOPLE RESPONSIBLE:**
Designate your system administrators in writing and ensure they know what their responsibilities are. As the needs of equipment and personnel of the unit change, ensure that the lines of accountability are updated. While management has the overall responsibility for accountability, each individual member of the Georgia Tech team plays a vital role in actively managing our data resources.

**COMMUNICATE WITH EVERYONE IN THE UNIT:**
Communication of the need, responsibility, and accountability for information systems is one of the most effective tools for ensuring proper administration. Management has, at its disposal, several indirect communication channels such as email, the internet, and electronic messaging. We encourage the use of these indirect methods but also promote the direct face-to-face methods such as staff meetings, brown bags, and targeted training programs. A unit’s size, composition, and the risk assessment of information processed within the unit will assist in determining which of these methods is most appropriate

**DISSEMINATE POLICIES AND PROCEDURES:**
The Institute [Computer and Network Usage Security Policy](http://www.policylibrary.gatech.edu/computer-and-network-usage-and-security) provide guidance based on an enterprise perspective. While this may fit some units, it is not focused enough for all. If your campus unit handles special types of data (or special systems), there is a need for procedures for handling that data. Dissemination of procedures through direct and indirect communication is paramount to the success of information systems administration within the unit.

**Related Issues:**

Review the Georgia Tech and other Data related Policies:  
http://www.policylibrary.gatech.edu/information-technology/data-access  
http://legal.gatech.edu/topics
XXIV. Logical Security

**Description of Risk:** All units of the Institute are dependent on information systems and its infrastructure to conduct their daily business, whether it is education or administration. Workstations that are networked and standalone systems are subject to information security risks and need a minimum level of logical security in addition to physical access controls. Networked systems are more susceptible to compromises because of their network connections and therefore require an even more stringent monitoring of their logical security. Without proper logical security the integrity of the system, data, and availability of the information resources campus wide can be compromised. This will result in loss of funds, liability from the compromise of personal information to unauthorized sources, and embarrassment to the Institute. Such compromises result in:

- Theft of propriety data, source code as in working papers, research data, etc. by competing entities or snoopers.
- Unauthorized (malicious, non-malicious, or accidental) disclosure, modification, or destruction of information. Such as changing of data to corrupt results, change grades, change payment amounts, history or vendor info.
- Non-malicious errors and omissions.
- Denial of service, use of the computer or workstations access to the network to flood the network with traffic and thus prevent network access to a target organization or entity.

Examples in logical security failures both accidental and malicious abound in today’s news. Predictions are for these risks to only grow.

**Criteria:** The institute is subject to the guidance provided in the Office of Information Technology’s network usage policy that addresses requirements for logical controls at Georgia Tech:


Logical controls are those controls that prevent access by unauthorized parties to systems, programs or data. These are some examples of controls that can prevent unauthorized access.

- Authentication Controls: It is extremely important to ensure that a claimed identity is valid. The authentication control provides the means to verify the identity of a subject. These controls should provide a verified unique user ID.

  Example: A good control uses a Georgia Tech assigned ID, such as used in logging onto PRISM, Banner or PeopleSoft. In other words, a user ID issued by competent authority based upon the users proven eligibility. A bad practice is to use a homemade or generically assigned user ID as in GTLAB1, or STUD001, STU002, etc.
• Authorization: Authorization controls enable specification and subsequent management of the allowed actions for a given system. Examples of good controls are those that incorporate strong password policies; such as forced expiration with a maximum password life less than 91 days, passwords that are not easily guessed and passwords that meet the minimum criteria explained at http://www.policylibrary.gatech.edu/information-technology/passwords

Auditor’s Overview: The purpose of our audit in this area is to ensure that campus units are engaged in logical security practices that maintain a level of control consistent with Georgia Tech policy and accepted industry best practices.

Best Practices:
1. Maintain an active user awareness program that reinforces the concept that all users have security responsibilities.
2. Hold users responsible for basic security practices.
3. All operating systems must have logical security capabilities.
   Example: Windows 95 is not a securable system, whereas Windows 2000 and above, UNIX, MAC, and Linux systems allow for discreet network, individual file, and folder security.
4. Passwords should not be shared with others under any circumstance. Passwords should not be written or emailed.
5. All operating systems should be set up to enforce automatic password changes and implement “strong password” capacity.
6. Where possible a “layer security” concept should be in place by using individual user IDs, individual passwords and multi-layered security and firewalls.
7. Conduct a semi-annual risk self-assessment. Contact the Department of Internal Auditing.
8. Use automated tools to review your information security posture: i.e. Information Security Scanner (ISS), GFI LANGARD LAN scanner, NMAP, etc.
9. When in doubt seek assistance or advice from the professionals available at OIT or the Department of Internal Auditing.

Process:
EMPOWER THE PEOPLE RESPONSIBLE:
Establish routine reporting requirements on the status of the unit’s security posture that will enable the computer support personnel to communicate security issues in a timely and objective manner to management.

Do not ignore Information Systems issues as “too technical,” most are procedural and require all users, administrators, and support personnel to work together to maintain a secure environment.

Provide the CSS/CSR written support covering the areas of responsibility, clearly delineating the CSS/CSR relationship within management. Each unit should have a local policy based on the Institute’s Computer and Network Usage Policy and tailored to fit the unit’s information systems environment. Local policy should include written guidance on the unit’s procedures for software
management, backup and recovery, installation or modification of equipment, and other pertinent aspects of an information system.

Do not overload the CSS or CSR with conflicting duties. Where possible, segregate the administrative duties from information security requirements. For example, the systems administrator can set up and establish user IDs and accounts, but a second person should review the system, security and logs.

COMMUNICATE WITH EVERYONE:
Use communications to spread the wealth; make everyone a pro-active member of the team. Establish a pro-active security awareness program that includes everyone from senior management to Tech Temps.

Use security warning banners, screen savers and email to keep all users aware of the issues affecting the system and thereby affecting how they use it.

POLICIES AND PROCEDURES:
Ensure that your unit has reviewed the Institute’s Computer and Network Usage Policy and Data Access Policy and has formally documented your local policy and procedures for authorization, authentication and encryption. Don’t pay lip service to basic security requirements like user accounts and passwords.
- Strong passwords and password construction techniques can be found at: http://www.policylibrary.gatech.edu/information-technology/passwords
- Make sure all users are authorized by ensuring that the systems administrator is made aware of all personnel changes to the Unit.

USE A SYSTEMATIC APPROACH:
Review your unit’s info systems risks on a semi-annual basis; involving all elements of your Unit’s administrative, business and academic infrastructure. Do not relegate this duty solely to the CSS/CSR.

Related Issues:
- Physical Security
- Training
- Documentation

XXV. Physical & Environmental Security Controls

Description of Risk: If physical and environmental controls are not in place to ensure the proper conditions in which information systems should operate, systems may become unstable. If information systems assets are not properly identified and controlled, they may be misappropriated and/or damaged. This increases the risk that information systems resources could be unavailable and data may be compromised.
Criteria: Physical and environmental aspects are often one of the most overlooked areas of information technology operations. Heat, humidity, and inappropriate levels of dust in the area are a few examples of environmental factors that can wreak havoc on the Information Technology assets. To protect information systems assets, each campus unit must take into account environmental controls. There is no single standard for ensuring environmental protection, but a risk assessment can be used to point to vulnerable areas.

Auditor’s Overview: Physical Controls include authorized physical access to prevent theft, ensured accurate inventories, and implemented asset management controls so that theft can be prevented and or readily detected. Recent estimates of computer and information systems crime indicate that theft, abuse, and other computer crimes are more likely committed by insiders than someone breaking into the system. Physical security controls must be in concert with logical security controls.

Audits include a review of physical controls in the form of key control to locked spaces, appropriate information systems resources being under lock and key, or other physical access controls. Highly critical information resources should not be located in high traffic spaces, common areas, (stairways, lobbies, etc…) or any other openly accessible area.

Audits also review disposal processes for surplus equipment to ensure that residual information is appropriately removed from all information resources prior to being processed. Excess or outdated equipment must be appropriately accounted for and safely disposed of.

Environmental aspects are often one of the most overlooked areas of information technology operations. Heat, humidity, poor electrical support, and inappropriate levels of dust in the area are a few examples of environmental factors that can wreak havoc on the information technology assets. To protect information systems assets each campus unit must take into account environmental controls.

Best Practices:
1. Positive control of access to spaces containing sensitive information systems equipment by the use of swipe badges
2. Limit key control to only essential personnel
3. Use of key logs and serialized keys limited to those personnel responsible for rooms and labs
4. Ensuring spaces containing information resources are locked when vacant
5. All equipment should be clearly labeled and tagged
6. Timely disposal of excess equipment
7. Proper disposal procedures ensure all institute data is cleaned off of surplus media
8. Locations and configurations of equipment should be diagramed, cataloged, and stored in an external location
9. Maintain temperatures between 72 and 78 degrees.
10. Keep the area clean; do not allow open drinks, food or other contaminants within the immediate area of a valued information system resource.
11. Conduct routine periodic maintenance to ensure blower fans for power supplies are not blocked by furniture or carpet and that computers are kept free of dust and dirt.
12. Ensure personnel working on sensitive electronic gear take the appropriate measure to ensure they are protected from static electricity and high voltages.
13. Ensure diskettes and tapes are protected from damage due to temperature extremes, magnetic fields, water, etc.
14. Ensure units are protected by correctly rated un-interruptible power supplies (UPS) and surge protection.

**Process:**

**EMPOWER THE PEOPLE RESPONSIBLE:**
Both the Computer Services Specialist/Computer Services Representative (CSS/CSR) and the Capital Assets Management liaison member should maintain inventories. The CSS/CSR inventory should be reflective of changes to individual machines as well as those greater than $1000. Personnel responsible for individual rooms and spaces must be responsible for assisting the CSS/CSR with keeping an updated and accurate list of IS equipment in their areas of responsibility.

**COMMUNICATE WITH EVERYONE:**
Education is a basic step to ensure physical security. Regular unit communication educates the users and supports physical security controls by ensuing unit personnel know what to do in case of a natural anomaly (flood, fire, earthquake, etc.). Unit personnel should be instructed on procedures for handling human threats by knowing who can access restricted areas, and what to do if they suspect anything.

**DISSEMINATE POLICIES AND PROCEDURES:**
Management should ensure that the unit has a written policy that clearly delineates who is responsible for equipment, each area’s security; and emergency procedures.

Ensure equipment is properly loaned out using the Equipment Loan Agreement form: [Equipment Loan Agreement Link]

**POLICIES AND PROCEDURES:**
Using appropriate equipment manufacturer requirements and recommendations, units should prepare the appropriate procedure and schedules for ensuring environmental controls are maintained.

**ENSURE ACCURACY OF INFORMATION:**
Keep local inventories and network diagrams up to date. These aides are invaluable for managing theft and for turn over between Computer Services personnel. Use these controls in designing the physical security control strategy. Invite the Institute’s police department to perform a physical security survey and use that to reduce gaps in security.

Each piece of computer hardware should have manufacturer’s recommendations for proper maintenance and environmental settings. Evaluation of physical location against the environmental recommendations made by the manufacturer should provide adequate protection during normal usage. Examples of bad situations that must be avoided are:
• Locating Critical resources in areas with inadequate ventilation or inappropriate humidity levels.
  o Example 1: A server located in a broom closet with a sprinkler head in it. Heat will build up quickly on large computers with high power requirements. Even a momentary failure of a sprinkler system will destroy electrical equipment.
  o Locating an Uninterruptible Power Supply (UPS) that supports critical resources next to a HVAC air intake vent. The increased airflow results in increased chance of dust, static buildup, and humidity level.
• Critical Resource that is properly located but not adequately monitored.
  o Servers often have redundant power supplies in case of failures. Redundant power supplies often have a conditioning cycle that should be performed every six months or so. Failure to condition the power supplies properly may result in a momentary power spike, or brownout, causing loss to critical resources.
  o A machine placed in direct sunlight may experience significant temperature gain over the surrounding area. Although the temperature of the room may be acceptable the machine may overheat.

USE A SYSTEMATIC APPROACH:
  1. First identify assets to prioritize resources.
  2. Categorize assets into groups such as Critical Assets, Needed Assets, and Functional Assets.
  3. Develop a plan to support the most critical assets with appropriate environmental controls to address
     • Unit’s environmental issues.
     • Application of controls to mitigate these risks.
  4. Review environmental controls upon additions/deletions or changes in equipment locations.

Related Issues:
Environmental Controls
Back-up and Recovery
Logical controls
Business Continuity Plan
Physical controls
Documentation

XXVI. Data Stewardship Controls

Description of Risk: Data compromised or lost due to poor data stewardship may have adverse effects on business operations, competitiveness, and public relations. Monetary loss to individuals and the Institute may occur if the compromise is severe enough. It is the responsibility of Georgia Tech, through the chief data stewards, to implement procedures to effectively manage and provide necessary access to Institute data, while at the same time
ensuring the confidentiality, integrity, availability, accountability, and auditability (CIAAA) of
the information. Appropriate implementation of the policy will ensure Institute compliance with
the Federal Trade Commission’s Safeguards Rule under
  • the Gramm-Leach-Bliley Act (GLBA), as well as the Family Educational Rights and
    Privacy Act (FERPA), and the Health Insurance Portability and Accountability Act of
    1996 (HIPAA).

Criteria: Data is an important campus unit business asset. “Data stewardship,” for the purpose
of this section of this document, is defined as the prudent management of Georgia Tech’s data.
Georgia Tech’s data is defined as:
  • Data provided to external stakeholders (public and private organizations with which
    Georgia Tech conducts business such as other U.S. Department of Defense offices,
    Congress, other government agencies, laboratories, contractors, and the general public);
  • Data provided to internal stakeholders (individual organizational components that
    comprise Georgia Tech); and
  • Data that may be of a sensitive nature (budget, personnel, proprietary, credit card,
    reviewer, and procurement data).

Auditor’s Overview: It is management’s responsibility to ensure:
  • The confidentiality, availability, and integrity of Institute, propriety, and personnel data
    held by the unit or accessed through the unit’s information systems; and
  • That credit card and other financial instruments are protected and credit card information
    meets the requirements of Institute polices (no unit should be processing and storing
    credit card information outside of the Institute’s approved processing environment).

Best Practices: Maintain a policy that answers the following questions as they apply to your
unit:
  1. Can you identify what business, academic, or research functions are supported by
     applications running on departmental servers and individual workstations?
  2. Is there a single point of contact regarding the integrity of the data? Who assigns access
     to PeopleSoft, Banner, Data Warehouse, and other Institute systems?
  3. How are staff/faculty/students made aware of network security issues? Is that procedure
     documented?
  4. Who determines access to applications, files, and data stored on your file server?
  5. What are your safeguards to ensure that outside entities that are facilitated by access to
     the Georgia Tech information system infrastructure do not have access to sensitive files
     or data repositories within the unit?
  6. Does the unit use any type of nondisclosure agreement to protect data or intellectual
     property? Who keeps these?
  7. Do you accept/store or process credit card information in any of your unit activities?
“How do we do all that?”

EMPOWER THE PEOPLE RESPONSIBLE
Deans, vice presidents, and associate vice presidents are responsible for monitoring compliance with the Data Access Policy and associated guidelines by:

- Directing the reviews of, and responding to technical reports for, servers within units for which approval has been given to store sensitive information;
- Ensuring that all sensitive information and unit level servers are registered with OIT Information Security (email: dap@gatech.edu); coordinating with OIT Information Security to ensure that the server(s) providing this information to the campus network and Internet are secured through reasonable procedures; and
- Conducting periodic access control assessments of any sensitive information devices or services within their business units, in coordination with OIT Information Security.

COMMUNICATE WITH EVERYONE IN THE UNIT
Post policies and procedures. Hold routine training.

DISSEMINATE POLICIES AND PROCEDURES
Write it down to prevent confusion.

Under regulations promulgated in May 2000, colleges and universities are deemed to be in compliance with the privacy provisions of the GLB Act if they are in compliance with the Family Educational Rights and Privacy Act (FERPA). However, higher education institutions are subject to the provisions of the Act related to the administrative, technical, and physical safeguarding of customer information.

Related Issues
Review the Georgia Tech and other data-related policies:
http://www.policylibrary.gatech.edu/information-technology/data-access
http://legal.gatech.edu/topics
FERPA
HIPAA

XXVII. Training

**Description of Risk:** If users are not adequately trained, there is a risk that information systems may be used in a manner inconsistent with Institute policies and procedures. If users do not follow solid practices, there is an elevated risk that viruses or other adverse conditions could be introduced to the unit and the campus network. If systems administrators are not appropriately trained to effectively carry out their responsibilities of maintaining sound information systems, there is a risk that systems could be used inappropriately, ineffectively, and insecurely. These
conditions could cause Institute data to be compromised, systems to become unstable, a reduction in productivity, etc.

Criteria:  
For technology to create an enhanced learning and operational environment, those affected by it must understand how to use it. Advanced technologies such as integrated networks require a greater technical understanding than antiquated technologies such as the VCR or TV. Training must be provided for users to develop a comfort with these new tools and for control personnel (Systems Administrators) to manage or control it. Once trained, empowered users and control personnel can utilize the technology fully. In addition, effective training will:

- Build dependable thought partnerships with students and users, enabling them to add value through the essential development of excellent intra-organizational, intra-staff relations and effective utilization of resources.
- Provide a first class service of expert, technical and practical guidance which will enable our clients to protect their principle assets and thereby their business/education.
- Set clear standards of service and expectations of use.
- Promote and encourage discovery and creativity.

Auditor’s Perspective:  For technology to create an enhanced learning and operational environment, those affected by it must understand how to use it. Advanced technologies such as integrated networks require a great technical understanding. Training must be provided for users to develop a comfort with these new tools, and for administrative personnel (System Administrators) to manage or control it. Once trained, empowered users and administrative personnel can utilize the technology fully. In addition, effective training will:

- Build dependable thought partnerships with students and users, enabling them to add value through the essential development of excellent intra-organizational, intra-staff relations and effective utilization of resources.
- Provide a first class service of expert, technical and practical guidance which will enable our campus community to protect their principle assets and thereby their business/education.
- Establish standards of service.

Best Practices:
1. Develop a training plan for all employees that reflect the strategic direction of the campus and takes into account the technologies deployed or expected to be used in the local area.
2. Use local resources such as the Office of Organizational Development to support the training.

Process:  
EMPOWER THE PEOPLE RESPONSIBLE:  
Designate a training coordinator and ensure they know what their responsibilities are. As the needs, equipment, and personnel of the unit change ensure that the training plan is updated. Assign unit personnel to give input to their training requirements. The training plan should be reflected in the budget.
COMMUNICATE WITH EVERYONE IN THE UNIT:
Communication of the need and responsibility for continuing training in the area of technology is essential to success of the training plan. Ensure that staffs understand management’s support of ongoing training and that feedback is received from unit personnel on training needs.

XXVIII. Documentation

Area of Risk: Documentation consists of written materials that clearly describe procedures, forms and other aspects of an ongoing information system. Using a form, virtual or print, is a key element to the stability and reliability of any information system.

Key important factors are:
- It communicates knowledge about an Information System to people who interact with the system
- Prescribed procedures can be performed more reliably, efficiently and consistently since documentation standardizes communications
- Documentation helps to train users because it includes procedural manuals and user guides
- Audit trails can assist in spotting weaknesses and deficiencies in the system

Documentation aids the development of new systems and maintenance of existing ones. Documentation will provide quintessential elements of success during any recovery operation. Well-documented systems are protected against the risk of a single point of failure in human systems administration.

Description of Risk: Without proper documentation the following risks may be present:
- Users will need increased training because of the deficit of the documentation
- Lost productivity
- Increased errors in data entry
- Possible system breeches
- Software corruption of proprietary systems
- Compromises of systems
- High turnover rates
- Decreased system efficiency
- Increased operational costs

Criteria: Systems, configurations, proprietary user guides, and special software need to be documented because when they are actually needed it will most likely be a time with a demanding schedule. Documentation is subject to category “D” of the records retention series from the USG and Board of Regents. At a minimum, documentation should exist to fully support a restoration plan from zero operational state to a state of full capability.
The documentation should include adequate policies and procedures so that new personnel, being trained or otherwise, could operate the system in a manner that would support operations. Documentation should clearly outline the responsibilities of all managers, operators, administrators, and users.

**Auditor’s Overview:** We look for clear and current documentation in the form of:

1. Unit Users Guides
2. Network Diagrams
3. Inventory and accountability logs and forms
4. Availability of manuals and training guides
5. Crash Books describing details of the unit’s system administration
6. Guidelines for users on network security, user rights and responsibilities
7. Current lists of authorized users and access privileges
8. Business continuity plans and disaster recovery plans
9. Audit Trail, to include user id, resource access times, date, time, workstation location, and specific data modified or action taken.

**Process:**

**EMPOWER THE PEOPLE RESPONSIBLE**

System administrators, users, and management all play a constructive role in developing and maintaining each of the aforementioned documents. Local unit policy should specify what duties are associated with each of these roles.

**COMMUNICATE WITH EVERYONE:**

Make use of Information Systems:

- Use Web sites and Email to promulgate policies and procedures.
- Ensure accuracy and currency of information
- Keep your credibility by staying current!
  - Nothing is more discouraging than going to your home page and seeing a flashing new symbol against a 1997 piece of information.

**USE A SYSTEMATIC APPROACH:**

Actively schedule peer-to-peer reviews of your documentation on an Information Systems priority basis.

**READ, WRITE & REVIEW:**

From the ISO9000 series on quality systems:

- A quality process is documented by writing procedures.
- A system should be documented by writing procedures. If you document your current quality system procedures, changes in quality are easier to detect and to measure because they can be compared with the way things were done in the past.
- Documents provide objective evidence that:
  - A process has been defined
  - Procedures have been approved
  - Procedural changes are under control
Related Issues:
- Business Continuity Planning
- Software License Management

XXIX. Equipment Maintenance

**Description of Risk:** Loss of critical resources can occur if equipment is not properly and timely maintained. Losses due to improper maintenance are similar to those that can occur during a disaster:
- Loss of Information resources
- Loss of proprietary data
- Loss of productivity
- Hardware damage
- Software corruption of proprietary systems

Vendor support may be critical and can adversely affect the systems or render them inoperable if maintenance contracts are unsupported or neglected, warranties may be voided, and duplicated costs incurred.

**Criteria:** Physical devices such as computers are susceptible to failure. Information systems and associated computers have been designed to work in a controlled environment. Proper maintenance will extend the life, power, and capability of the system. Evaluations will be based upon manufacturer’s recommendations and industry best practices.

Software programs are complex and have many interfaces to hardware. Since hardware changes rapidly, these software systems must be updated quickly to maintain compatibility. Issues such as these are often difficult to control at a local level. Vendor support may be critical and can adversely affect the systems or render them inoperable if maintenance contracts are not kept up.

**Auditor’s Overview:** Information Systems’ hardware should be serviced in accordance with the manufacturer’s recommendations, which are usually included as specifications in the contract or as recommendations in the user’s manual. Manufacturer’s maintenance procedures are designed to adequately protect hardware against failure over the useful life of the hardware and are usually a requirement to maintain the manufacturer’s warranties. Maintenance records should be kept to assess system reliability and to assist in warranty claims. Equipment and software may also come with pre-paid vendor-provided maintenance.

**Best Practices:**
1. Develop a system of inspecting equipment to verify that maintenance procedures are adequate
2. Always review the contract specifications and warranties for maintenance-related requirements
3. The Computer Support Representative should work with the unit to schedule maintenance and hardware inspections on a regular basis.

4. Develop a maintenance calendar and a maintenance log to record when maintenance has been conducted, by whom, and what was done.

5. Ensure that systems users understand their responsibilities and role in equipment maintenance.

**Process:**

**IDENTIFY THE PEOPLE RESPONSIBLE:**
Management, users and computer support personnel share responsibility for hardware maintenance. Management must be aware of contract stipulations and make that information available to the appropriate personnel on a timely basis. Users are generally responsible for taking proper precautions, i.e. keeping liquids and other foodstuffs clear of the machine, cleaning dust build-up around the machine, and due care in the handling of sensitive equipment.

**POLICIES AND PROCEDURES:**
Local policy should include a section on maintenance procedures, how to schedule maintenance, end-users role in maintenance, and acceptable workplace practices.

**USE A SYSTEMATIC APPROACH:**
Identify assets to prioritize resources. Categorize assets into groups such as Critical Assets, Needed Assets, and Functional Assets. A unit can quickly devise a plan to support the most critical assets by ensuring maintenance resources are applied to the most valuable assets.

- ID unit environmental issues and apply controls to mitigate risk
- Review environmental controls upon additions/deletions or changes in equipment locations

**Related Issues:**
- Environmental Controls
- Physical Security

**XXX. Business Continuity Planning**

**Description of Risk:** If units do not have documented plans in place that have been clearly communicated to all key unit personnel and tested, there is the risk, in the event of a disruption in services due to power outages, fire, etc., that mission critical operations may be adversely impacted. This could result in loss of information resources, loss of proprietary data, loss of productivity, and damage to the reputation of the Institute.

**Criteria:** Technological emergencies may include interruption of utilities, hardware failure, theft of hardware or software or anything that causes downtime unexpectedly. Several guides to emergency management address backup and recovery. The National Institute of Standards and Technology’s [Contingency Planning Guide for Information Technology Systems](#) addresses all
aspects of backup and recovery. The Institute has not put out set criteria for backup and recovery of systems contained within campus units but does hold them responsible for backup and recovery. NIST’s guide provides guidance and templates for backup and recovery options.

**Auditor’s Overview:** Backing up software and having backup hardware devices is a large part of information systems availability. It is important to be able to restore data. For example, if a hard drive fails, a disaster takes place, or there has been some type of data corruption, a backup procedure enables rapid restoration. Auditors look for:

- Policies and procedures in place that indicate what gets backed-up, frequency and where these back-ups are safely maintained
- Testing procedures for these policies
- User workstations and portable devices containing important data are included in the back-up policy
- That users are aware of their responsibilities to backup their data

Policies and procedures should consider each of the following aspects of backing-up valuable IT resources: hardware, software, data, personnel and off-site facilities.

**Best Practices:**
Back-up procedures should answer the questions:

1. What happens if I have a server failure, what will be the most current backup I can restore to?
2. What happens if my Computer Support Specialist is unable to return to work for a period of time?
3. What happens if I am denied access to my workplace due to power outage, or other sudden impediment?
4. Can I get access to my backup capabilities?
5. Can my users access their important files, data and student/personnel records?
6. What happens in case one of my priority users’ workstations has an unrecoverable failure?
7. Where are my original disks maintained for source code? Are they up-to date with current patches?
8. What are the procedures for letting my internal and external business partners know when service will be restored?
9. Are my backups stored off-site?
10. Is my current system configuration documented?
11. Are my software licenses stored in a secondary location?
12. Are there procedures in place to ensure individuals back up data on their local PCs?
13. Is my recovery equipment interoperable with my current configuration?
14. Are servers configured to shut down gracefully upon power loss?
15. Is there redundancy between critical system components and capabilities?
16. Is there a test procedure for validating restoration data?
17. Is there a call tree for notification of key individuals upon system failure?

**Process:**
Campus units maintaining multiple servers and providing various services should have internal backup capabilities. These capabilities could include backup to tape or other media and/or remote network storage device. Whatever amount of work you can afford to replace dictates the frequency of your data backup.

Units should conduct a daily backup of differential changes, followed by a total backup weekly. Weekly backups should be stored in an off-site location where they can be accessed by authorized members of the unit in case of a needed recovery. Depending upon the needs of the unit, daily full backups might be required and should be rotated off-site as well.

Individual workstation data should be backed up by the user. The procedures that the user can employ to backup data should be a part of the local policy and procedures manual.

EMPOWER THE PEOPLE RESPONSIBLE:
Develop and put in place a training program where all information system users know where their data is maintained and how it is backed up. Be clear with individual users over their portion of the shared responsibilities. Be sure that all personnel in the recovery team are aware of the policy. Semi-annually, conduct a test, including all members of the team.

COMMUNICATE WITH EVERYONE:
Put out reminders of what the unit’s policy is via occasional email or bulletin board notices.

DISSEMINATE POLICIES AND PROCEDURES:
Write down your policy, publish it to all the team members and make sure it is exercised by conducting systematic tests.

USE A SYSTEMATIC APPROACH:
Human nature is such that the un-inspected gets put off. Schedule at least an annual exercise requiring personnel to respond and actually restore from backup.

Related Issues:
Information Systems backup and recovery operations are only a portion of your overall business recovery and disaster recovery plans. Each unit should have an updated disaster recovery and business continuity plan.

See the following websites for additional plans, sample policies:

www.oit.gatech.edu
www.fema.gov
www.drj.com
www.nist.gov
XXXI. Software Licensing

**Area of Risk:** Commercial software vendors are becoming increasingly aggressive in enforcing their rights under the copyright laws. Most Information Systems employed on the Georgia Tech campus make use of Commercial Off-The Shelf (COTS) software. Virtually all COTS software products are licensed to the user, not sold, under the copyright laws of the United States. While some software is “free for educational use”, this software is by far in the minority. All types of software are still covered under copyright laws. The unauthorized duplication, operation on machines other than for which licensed, or other “piracy” is a violation of Federal law, and may expose the individual and the Institute to legal actions which could lead to significant monetary loss, professional embarrassment and possible imprisonment.

**Criteria:** The Georgia Tech [Computer and Network Usage Security Policy](#) contains guidance regarding licensing as follows:
- No software may be installed, copied, or used on Institute resources except as permitted by the owner of the software
- Software subject to licensing must be properly licensed, and all license provisions (installation, use, copying, number of simultaneous users, terms of license, etc.) must be strictly adhered to
- Users are prohibited from using, inspecting, copying, storing, and redistributing copyrighted computer programs and other material, in violation of copyright laws

**Auditor’s Overview:** One of the most daunting conundrums for the educational environment is the monitoring and control over the installation of software.
- Is the operating system a secure operating system?
- Is there a software management system in place that details the authorized software, and a standard configuration for unit computers?
- Does the CSS/CSR have a spreadsheet or database that cross-references software licenses to specific computers?
- Are administrative controls limited to only those personnel authorized to install software?
- Are monitoring techniques in place to detect the un-authorized downloading or copying of installed software?
- Are routine inventories conducted of installed software?
- Can you show proof of purchase and license agreement for each piece of licensed software installed on any of your computers?
- Do you have the correct number of per-seat or server client licenses for the unit servers?

**Best Practices:**
1. Promulgate a unit policy on software management
2. A pro-active user education and training program that sets the standards for users to follow
3. Use a “secure” operating system that can be tailored to the users, and only allows specified personnel the ability to install software
4. The employment of automated license tracking software is highly recommended; this usually involves the installation of “agent software” that keeps an active inventory of installed software and changes to installed software.

5. Have your purchasing department or purchasing officer maintain a file of software purchase orders and vouchers.

6. Limit the authority of who can purchase software, especially with PCards.

**Process:**

**EMPOWER THE PEOPLE RESPONSIBLE:**
System administrators, users, and management all play a constructive role in developing and maintaining software licenses. Local unit policy should specify which positions are associated with software licensing duties.

**COMMUNICATE WITH EVERYONE:**
Make use of Information Systems:
- Use Web sites and Email to promulgate policies and procedures.
- Ensure accuracy and currency of information.
- Ensure due diligence by staying current!

**USE A SYSTEMATIC APPROACH:**
Conduct routine inventories. Insist proper procedures are followed for software purchases.

**Related Issues:**
Backup and recovery
XXXII. Web Site Operation / Development

Description of Risk: The risk associated with web presences are vast, some of them are:
- Damage to reputation
- Monetary loss
- Theft of data
- Corruption of data
- Loss of needed information resources
- Loss of proprietary data
- Loss of productivity
- Hardware damage
- Software corruption of proprietary systems
- Compromises of systems
- Decreased system efficiency
- Increased operational costs

Criteria: There are several resources regarding website operations and development. They can be found at:
- http://www.security.gatech.edu/ServerSecurity
- http://www.oit.gatech.edu/service/webhosting/web-hosting
- http://www.comm.gatech.edu/offerings/web.html
- Georgia Tech Computer and Network Security Usage Policy

Auditor’s Overview: The future growth and efficiency of educational efforts relies upon web-centric technologies and the application of advanced technologies such as communications and information systems to traditional education efforts. Advanced learning concepts such as distance learning are almost entirely dependent on web protocols. In addition, the World Wide Web (WWW) has a tremendous low cost marketing potential to each campus unit on Georgia Tech.

At the same time, however, these new technologies also create new vulnerabilities for campus units through accidental or deliberate service disruptions. Web-enabled servers may act as an open portal for those who would jeopardize Georgia Tech operations. Research, personal data, course information, and study material are all at risk of theft, destruction, or sabotage. In addition to these vulnerabilities the web-presence of each campus unit is a representation of how well it is aligned with Georgia Tech’s image as a whole.

The most ubiquitous software running on Georgia Tech’s Information System is the Network Browser and those applications supporting web services. This is the highest area for future misuse and potential compromise of Georgia Tech’s assets.

Best Practices:
1. Ensure the campus unit’s local web presence is in tune with official policy
2. Host the web site on OIT’s servers if at all possible
3. Keep all web servers patched
4. Use as few services on the primary web server as possible
5. Isolate vulnerable services such as FTP whenever possible
6. Use secure web protocols whenever possible

**Process:**
**EMPOWER THE PEOPLE RESPONSIBLE**
Ensure that there is a competent web administrator monitoring the logs and service of the web server. Ensure that that person has the appropriate level of skill and knowledge to take appropriate action when necessary.

**ENSURE ACCURACY OF INFORMATION**
Keep as current information as possible on the website. Old data presented as current has a discrediting effect.

**INTERNAL CONTROL GUIDANCE: PUBLIC RELATIONS**

**XXXIII. Public Relations Management**

**Description of Risk:** Misinformation can negatively impact the Institute’s image.

**Criteria:** Good business practice calls for a central voice to represent the Institute in providing information to the public. The Institute Communications Office web site at [http://www.comm.gatech.edu/](http://www.comm.gatech.edu/) provides a listing of contacts for media and other public relation inquiries.

**Auditor’s Overview:** The importance of this subject is to ensure that campus units are adequately addressing public relations.

**Best Practices:**
1. Empower one person with the responsibility and authority to oversee public relations management
2. Communicate the importance of this issue to the entire unit, enlisting their full cooperation and compliance in this matter
3. Develop internal policies and procedures on public relations management and disseminate to the entire unit to promote compliance in this area
4. Notify the Institute Communications Office of all media requests for information
5. Verify the accuracy and timeliness of information released to external sources by your unit
6. Verify the accuracy of information published on your unit’s website
7. Develop a process to monitor and/or advise employees speaking as experts in their areas
Process:
DEVELOPMENT OF AN AWARENESS CAMPAIGN
The development of an awareness campaign begins with management’s communication and dissemination of internal policies and procedures on telecommunications. Management establishes the tone from the top that will affect how the entire unit handles public relations. Management should communicate to faculty and staff the role of Institute Communications, and that good business practice calls for a central voice to represent the Institute in providing information to the public. Further, internal policies and procedures should also address the unit’s advisement to employees on speaking as experts in their areas. Additionally, the unit employees should be made aware that public relations encompasses the effective communications with prospective students, parents of prospective students, current students, parents of current students, other higher education institutions, general public, media, private and public agencies, foundations, alumni and friends etc.

Notify the Office of Institute Communications of all media requests
Contact the Director of Media Relations & Issues Management or the individual assigned to your unit within the communications office.

Accuracy and timeliness of information released
Internal policies and procedures may require all written communication be reviewed and approved prior to release.

Accuracy of information published on your unit’s website.
The Internet provides the general public with access to information regarding your unit potentially eliminating verbal communication. Care should be taken in ensuring the accuracy of information published on external web site.

XXXIV. Association with External Organizations

Area of Risk: Association with External Organizations

Description of Risk: Mismanagement of the fiscal matters of external organizations by Georgia Tech faculty, staff, or students could subject the Institute to financial loss and adverse publicity.

Criteria: In instances where faculty, staff, or students are involved with the financial management of external organizations (i.e. professional societies, student organizations, etc.), good business practice calls for basic fiscal internal controls. Some tips on basic fiscal controls are shown in a document prepared by the Department of Internal Auditing located at http://www.audit.gatech.edu/ under Best Practices.

Auditor’s Overview: The purpose of reviewing this area is to ensure that campus units communicate with faculty, staff and students the importance of exercising prudent fiscal controls when participating in the financial management of external organizations.
**Best Practices:**

1. The Unit Head communicates the importance of adequate fiscal controls when faculty, staff, and students participate in the financial management of organizations associated with Georgia Tech.

2. An individual, or individuals within the unit, are designated as contact points for employees to be referred to the appropriate level for counsel in instances where they have questions regarding fiscal matters of external organizations with which they assist in managing.

**Process:**

UNIT HEAD COMMUNICATION TO THE UNIT

Communicate with unit employees to ensure that everyone in the unit understands that if they are asked to serve as Treasurer, or in some other advisory capacity in an external organization that is prompted by their being a Georgia Tech employee, that certain fiscal controls need to be exercised to preclude financial liability and adverse publicity to the Institute.

DESIGNATE A PERSON WHO HAS RESPONSIBILITY FOR MONITORING THIS AREA AND WHO SERVES AS A CONTACT FOR THE UNIT ON THIS MATTER

Unit Head should designate an individual, for example someone in the business office, to serve as a point of contact and advise to employees who are asked to serve in some financial management capacity in an organization external to Georgia Tech. The designated person should establish a system to make sure that individuals report instances when they become financially responsible for external organization matters. If faculty, staff or students are identified as having financial responsibility for an external organization, a staff member should be designated to provide advice on fiscal controls.

**INTERNAL CONTROL GUIDANCE: STUDENTS**

XXXV. International Students

**Area of Risk:** International Student-Employees

**Description of Risk:** Failure to complete and maintain required documentation for non-U.S. citizen working students of the Institute could subject the Institute to fines and penalties imposed by the U.S. Immigration and Naturalization Service, a hold put on hiring of non-resident aliens, as well as adverse publicity.

**Criteria:** The Immigration Reform and Control Act of 1986 require employers to verify the identity and employment eligibility of anyone hired after November 1986. It is unlawful to knowingly hire, or to continue to employ, any individual not authorized to work in the U.S. Form I-9, Employment Eligibility Verification, was developed for verifying that persons are eligible to work in the United States. Institute requirements call for a new employee to complete
Form I-9 on the first day of employment and present required forms within the first three days of employment. Also, policy requires the tracking of expiration of employment authorization documents held by non-resident aliens. Institute hiring departments are responsible for advising new student employees of the time frame and documentation required to complete or update Form I-9s.

**Auditor’s Overview:** The purpose of reviewing this area is to ensure that campus units advise new student employees of the need to contact Human Resources to complete Form I-9, Employment Eligibility Verification, before they work in the unit and continuance of managing the process for required updates.

Many issues involving non-citizens, both students and non-students, working on campus can be complex. We encourage everyone who is responsible for new hire processing in his or her unit to contact the Office of International Education with any questions, [http://www.oie.gatech.edu/](http://www.oie.gatech.edu/). Another source of information is the Office of Human Resources at [www.ohr.gatech.edu](http://www.ohr.gatech.edu).

**Best Practices:**
1. The Unit Head empowers one person with the responsibility and authority to advise new student employees regarding the completion and updating of Form I-9, entitled Employment Eligibility Verification
2. The appointed administrator advises new student employees that they are to report to Human Resources to complete required paperwork, including Form I-9, before they are permitted to work in the unit
3. The appointed administrator establishes the appropriate contact with the Office of Human Resources in order to be informed on the tracking of expiration of employment authorization documents held by non-U.S. citizen student employees in the unit; the unit administrator advises applicable student employees of the need to update Form I-9s
4. The appointed administrator establishes the appropriate contact with the Office of International Education in order to be informed of changes in requirements regarding student employees and to promote an environment that proactively maintains good relationships while managing requirements

**Process:**
**EMPOWER THE PEOPLE RESPONSIBLE**
The Unit Head appoints a person within the unit to ensure compliance with the Immigration Reform and Control Act of 1986, which requires employers to verify the identity and employment eligibility of new student employees.

**EXECUTE POLICIES AND PROCEDURES**
The appointed administrator should put in place a process to ensure compliance with the Immigration Reform and Control Act. Some things an administrator might do to implement a compliance process follow:
- Formalize approach for assuring compliance with Form I-9 procedures; a suggestion to consider is developing and maintaining a checklist that is completed by responsible parties within the unit to record accomplishment of internal and federal requirements
- Communicate procedures to staff, faculty and students as applicable
• Communicate Form I-9 requirement to student employees in pre-employment correspondence and when they initially report to the unit
• Establish lines of communications with the Office of Human Resources in order to track and notify non-USA student employees of the expiration of work authorization documents and the need to update Form I-9s

XXXVI. Students/Sexual Harassment

**Area of Risk:** Sexual Harassment

**Description of Risk:** Sexual harassment can (1) alienate students, (2) create a hostile educational environment, (3) result in lawsuits, fines, and penalties for violations; and (4) cause adverse publicity.

**Criteria:** It is the policy of this Institute that no member of its community, including administrators, faculty, staff, or students, should be subjected to sexual harassment by another. This policy and procedure is intended to create an atmosphere in which individuals who believe that they are the victims of harassment are assured that their complaints will be dealt with fairly and effectively. Toward this end, the Georgia Institute of Technology supports the principle that sexual harassment represents a failure in ethical behavior and that sexual exploitation of professional relationships will not be condoned.

Sexual harassment is defined as unwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature when:

• Submission to such conduct is made, either explicitly or implicitly, a term or condition of an individual's employment or academic standing;
• Submission to or rejection of such conduct is used as the basis for employment or academic decisions affecting the individual; or
• Such conduct has the effect of unreasonably interfering with an individual's work or academic performance or creates an intimidating, hostile working, or academic, environment. Both men and women may be either the initiators or victims of sexual harassment.

Complaints are to be directed to the Employee Relations of the Office of Human Resources for faculty and staff members and to the Dean of Students for students. Institute officials require an investigation. Individuals subject to disciplinary action may exercise their appeal rights pursuant to the procedures set forth in the Faculty Handbook, the Classified Employee Handbook, or the Student Handbook as appropriate.

**Auditor’s Overview:** The purpose of reviewing this area is to ensure that campus units have in place a system that communicates with students the importance of an environment free of sexual harassment and a means of dealing with situations in which a person believes they have been subjected to sexual harassment.
**Best Practices:**

1. The Unit Head communicates the importance of the prevention of sexual harassment to students and staff of the unit on a periodic basis.
2. An individual (or individuals) within the unit is designated as contact point(s) for students to be referred to the appropriate level for counsel in instances where they believe they have been sexually harassed.

**Process:**

**SET THE TONE AT THE TOP**

Ensure that everyone in the unit understands that the Institute’s policy is that no member of its community should be subjected to sexual harassment by another and if an employee or student believes they have been subjected to such harassment there is a means to deal with the matter fairly and effectively.

**DEVELOP AND EXECUTE SEXUAL HARASSMENT PREVENTION PROCEDURES**

- Responsible unit staff should familiarize themselves with the Institute’s sexual harassment policy and procedures. The Institute’s policy can be found in the following:

- Unit should communicate to all students/employees, on a periodic basis, the Institute’s and the unit’s internal policies on sexual harassment. This may be accomplished through reminders at student orientation if held in the particular unit, faculty/staff meetings, correspondence with students/employees, bulletins, or through unit internal procedure manuals.

- The unit should develop internal procedures that support Institute policies and procedures to provide students, staff, and faculty direction on reporting sexual harassment.

- Deal effectively and fairly with any complaints of sexual harassment in accordance with Institute policy.

**XXXVII. Protection of Information**

**Area of Risk:** Protection of Information

**Description of Risk:** Inappropriate handling of private student information can (1) result in lawsuits, fines, and penalties for violations; and (2) cause adverse publicity.

**Criteria:** Much of student academic data is covered by the Family Education Rights and Privacy Act (FERPA), which protects student rights with regard to educational records maintained by the Institute. Students have a right of access to their educational records; they
have a right to challenge inaccurate information or information that might violate privacy; and have a right to be notified of their privacy rights.

Only certain Institute employees may have access to personally identifiable student information without student consent. These employees sign a statement that all student data obtained through the Warehouse is to be considered "Confidential" and that no personally identifiable information should be released without the written consent of the individual student. Further, the statement warns that failure to comply with FERPA guidelines will result in the loss of access privileges to the employee and possible loss of Federal Funds to the Institute.

**Auditor’s Overview:** The purpose of reviewing this area is to ensure that campus units have in place a system to protect private student information.

**Best Practices:**
1. The unit head communicates the importance of the protecting personal student information.
2. Secure private student information maintained by the unit.
3. Develop internal policies and procedures an access to and release of personal student information.

**Process:**
**SET THE TONE AT THE TOP**
Ensure that everyone in the unit understands that the unit’s internal policy relative to access and release of personal student information.

**SECURITY**
The unit should identify and classify student information as personal and employ a means to secure the information during business and non-business hours. If the information is maintained in hardcopy, the information should be stored in a facility secured by a lock or if the information is maintained in an electronic format, access to the electronic files should be restricted within the system to prevent individuals without a legitimate business need for the information from gaining access to the information.

**DEVELOP AND EXECUTE PROTECTION OF INFORMATION PROCEDURES**
Responsible unit staff should familiarize themselves with FERPA requirements. The FERPA policy can be located at: [http://www.catalog.gatech.edu/genregulations/ferpa.php](http://www.catalog.gatech.edu/genregulations/ferpa.php)
Document the unit’s protection of information procedures in internal policies and procedures.

Periodically communicate the subject in staff/faculty meetings to refresh individuals on student information privacy.

Develop an awareness campaign to inform students and parents of information maintained by the unit and your commitment to protect personal student information.
INTERNAL CONTROL GUIDANCE: GENERAL

XXXVIII. Policies and Procedures

Area of Risk: Policies and Procedures

Description of Risk: If policies and procedures are not clear and comprehensive, and effectively communicated, there is risk that decisions made and actions taken might not be in accordance with Institute policies, State and Federal laws, etc.

Criteria: It is a good business practice to have available policy and procedures to guide actions of the unit. Also, many of the Institute's policies and procedures are driven by law.

Auditor's Overview: The purpose of reviewing this area is to determine how Institute policy and procedures, and/or internally developed procedures, are used to guide the actions of the unit.

Best Practices:
1. The Unit Head empowers one person with the responsibility and authority to lead a unit group in composing internal policies and procedures
2. If a policy already exists at Georgia Tech, simply adhere to it; if you have circumstances that are unique to your unit, or feel that some Tech policies are not clear, address this in your internal policies and procedures
3. Each member of the staff should contribute a clearly written documentation of their job duties; individual job descriptions kept as part of a unit’s internal policies and procedures save time and grief during periods of unexpected absence on the part of a team member
4. Written policies and procedures increase efficiency, reduce errors, and make training of new personnel easier and faster

*****************************************************