# Department Review Guide

## TABLE OF CONTENTS

This document is a guide for review of how key areas of risk are managed within an organizational entity. It is structured to give information on:

### FISCAL

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Accuracy of Financial Records</td>
<td>7</td>
</tr>
<tr>
<td>B. Sponsored Programs</td>
<td>7</td>
</tr>
<tr>
<td>C. Capital Assets</td>
<td>7</td>
</tr>
<tr>
<td>D. Foundation Funds</td>
<td>7</td>
</tr>
<tr>
<td>E. Travel</td>
<td>8</td>
</tr>
<tr>
<td>F. Cash and Receivables</td>
<td>8</td>
</tr>
<tr>
<td>G. Distribution and Control of Payroll Checks/Advices</td>
<td>9</td>
</tr>
<tr>
<td>H. Procurement</td>
<td>9</td>
</tr>
<tr>
<td>I. Procurement Card</td>
<td>10</td>
</tr>
<tr>
<td>J. Communications</td>
<td>10</td>
</tr>
<tr>
<td>K. Risk Management/Insurance</td>
<td>10</td>
</tr>
</tbody>
</table>

### HUMAN RESOURCES

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Leave Reporting</td>
<td>11</td>
</tr>
<tr>
<td>B. Off-campus Assignments</td>
<td>11</td>
</tr>
<tr>
<td>C. Employment Eligibility Verification</td>
<td>11</td>
</tr>
<tr>
<td>D. Sexual Harassment</td>
<td>13</td>
</tr>
<tr>
<td>E. Consultants vs. Employees</td>
<td>13</td>
</tr>
<tr>
<td>F. Compliance with Equal Employment Opportunity Act</td>
<td>14</td>
</tr>
<tr>
<td>G. Annual Performance Evaluations</td>
<td>14</td>
</tr>
<tr>
<td>H. Conflict of Interest</td>
<td>15</td>
</tr>
</tbody>
</table>

### LEGAL AND REGULATORY

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Contracts</td>
<td>15</td>
</tr>
<tr>
<td>B. Gifts</td>
<td>16</td>
</tr>
<tr>
<td>C. Open Records Act</td>
<td>16</td>
</tr>
</tbody>
</table>

### HEALTH AND SAFETY

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Safety of Workplace</td>
<td>16</td>
</tr>
<tr>
<td>B. Chemical Safety</td>
<td>17</td>
</tr>
<tr>
<td>C. Hazardous Waste</td>
<td>17</td>
</tr>
<tr>
<td>D. Biological Safety (Laboratories only)</td>
<td>17</td>
</tr>
</tbody>
</table>

### INFORMATION SYSTEMS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Strategy and Vision</td>
<td>18</td>
</tr>
</tbody>
</table>
B. Logical Security ................................................................................................................................. 18
C. Physical and Environmental Controls .......................................................................................... 19
D. Data Stewardship ............................................................................................................................ 19
E. Equipment Maintenance ..................................................................................................................... 19
F. Business Continuity of Information Systems .................................................................................. 20
G. Training ........................................................................................................................................... 20
H. Software Licensing ............................................................................................................................ 21
I. Operations/Administration .................................................................................................................. 21
J. Web Site Operation/Development ...................................................................................................... 21

PUBLIC RELATIONS .......................................................................................................................... 22
A. Public Relations Management ........................................................................................................... 22
B. Association with External Organizations .......................................................................................... 22

STUDENTS ........................................................................................................................................... 22
A. International Students ....................................................................................................................... 22
B. Sexual Harassment ............................................................................................................................. 23
C. Protection of Information .................................................................................................................. 23

GENERAL .............................................................................................................................................. 24
A. Policies and Procedures ...................................................................................................................... 24
INITIAL INFORMATION NEEDED

Certain information is needed to prepare for the review, and will minimize the time spent at the unit. Please assemble or prepare the following information for the Auditor.

- List of contacts within the unit.
- Current Organizational chart. If associated centers and programs are not listed, please indicate how those units report to the Chair\Director.
- Listing of campus buildings or off-campus sites used by the unit (do not include incidental classroom or office assignments).
- Listing of all ledger accounts used by unit (In addition to expenditure accounts, include any receivable, liability, revenue, or other applicable accounts. DO NOT include employee spending accounts. Include Foundation account numbers and matching Institute account. If there is no matching Institute account, please provide a reason. Inactive accounts should be highlighted, marked as inactive, or shown separately from the active accounts.)
- Listing of whom in the unit has a PCard, and the results from Procurement’s last review of current PCard holders.
- The most current Payroll Authorization List Form.
- A copy of the most current Bellsouth (via DOAS) monthly telephone billing.
- Unique policies and procedures issued for guidance of unit (Do not include general Institute prepared materials, such as the Classified Employee Handbook.) This should include any flex time policy, internet or cell phone usage paid by the unit, etc.
- The School\Unit logo or seal. Please email or provide on disk.

MATERIALS/DOCUMENTS WE WILL REVIEW

Most information will be obtained during interviews with designated points of contacts in the unit. However, there are some materials that the Auditor will wish to examine during the review. You might have readily available the materials that follow:

- Current FY Vacation and sick leave records.
- Current FY employee travel records.
- Current FY Procurement Card (PCard) monthly reconciliations.
- Activity records from the last physical inventory of capital assets, and any loan agreements for School equipment taken off campus.
- Activity records from the last physical inventory of telephone equipment\outlets.
- Procurement’s Signature Authorization Form for all personnel currently handling the unit’s procurement activities, and any forms cancelled FY-to-date.
- Any unit approvals to pay for cell phone usage or home internet service.
- Activity records for any workers compensation claims in the last 2 years.
- Any EHS&D, IRB, or other reports affecting the unit in the last two years.
- Signed current FY conflict of interest\consulting approval forms.
- For academic units, signed & approved Grade Change Authorization forms.
- Strategic Information Systems Plan.
- Most recent internal Information System risk assessment.
- Current Business Continuity Plan with documentation of when it was last tested.
- Current copy of hardware inventory
- Current copy of purchased software inventory
DEPARTMENT REVIEW GUIDE – CONTACTS LISTING

<table>
<thead>
<tr>
<th>OTHER CONTACTS</th>
<th>NAME</th>
<th>PHONE NO.</th>
<th>INITIAL MEETING Date/Time</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FISCAL</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A. Accuracy of Financial Records</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B. Sponsored Programs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C. Capital Assets</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D. Foundation Funds</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E. Travel</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F. Cash and Receivables</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G. Distribution and Control of Payroll Checks/Advices</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H. Procurement</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I. P Card</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>J. Communications</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>K. Risk Management/Insurance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>HUMAN RESOURCES</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A. Leave Reporting</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B. Off-site Assignments</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C. Employment Eligibility Verification</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D. Sexual Harassment.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E. Consultants vs. Employees</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F. Compliance w/Equal Employment Opportunity Act</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G. Annual Performance Evaluations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H. Conflict of Interest</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>LEGAL AND REGULATORY</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A. Contracts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B. Gifts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C. Open Records Act</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>HEALTH AND SAFETY</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A. Safety of Workplace</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B. Chemical Safety</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C. Hazardous Waste</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D. Biological Safety (Laboratories only)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>INFORMATION SYSTEMS</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A. Strategy and Vision (Executive manager, Dean, Chair, etc…)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B. Logical Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C. Physical and Environmental Controls</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D. Data Stewardship</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E. Equipment Maintenance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F. Business Continuity of IS Resources</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G. Training</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Section</td>
<td>Subsection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H. Software Licensing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I. Operations/Administration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>J. Web Site Operation/Development</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PUBLIC RELATIONS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A. Public Relations Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B. Association with External Organizations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>STUDENTS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A. International Students</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B. Sexual Harassment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C. Protection of Information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GENERAL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A. Policies and Procedures</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
A. Accuracy of Financial Records
Objective: To determine whether the campus units verify the accuracy of Institute generated reports for their accounts. Also, to determine if differences and discrepancies are reported and/or corrected so that Institute records accurately show the financial condition of the unit.

Criteria: 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.

Risk: If errors are made in official Institute financial records, and go undetected, the Institute could be exposed to legal risk and adverse publicity. If the unit does not have systems in place to detect for errors or omissions and to ensure overall accuracy of reports, the Institute’s financial position could be inaccurately summarized.

B. Sponsored Programs
Objective: To ascertain how the unit verifies that costs charged to sponsored programs are proper and in accordance with both Institute procedures and Grants and Contracts stipulations and assess the condition of the late deliverables.

Criteria: OMB Circular A-21 and Grants and Contracts Policy and Procedures (Section 3.0) require that units be responsible for the reasonable and accurate reporting of their expenditures.

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

C. Capital Assets
Objective: To examine the strength of processes in place to ensure that the unit controls and accounts for capital assets.

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. (Section 7.0 - Equipment Management, Business Policies and Procedures Manual).

Risk: Failure to properly account for capital assets could result in the loss of equipment and a misstatement of the value of capital assets on Institute records.

D. Foundation Funds
Objective: To determine if the unit exercises reasonable and prudent care in the acceptance and administration of private, non-sponsored Foundation funds. All private gifts must be appropriately approved & the funds held by the GTF expended in accordance with the restrictions or intent of the donor and with GT policies and procedures.

Criteria: Georgia Tech policies and procedures require that all units encourage donors to make their gifts payable to the Georgia Tech Foundation, Inc. (GTF). 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 which 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 GIT (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. (Section 11.0 - Processing and Use of Georgia Tech Foundation Funds, Business Policies and Procedures Manual).

**Risk:** If this area is not well controlled, there is risk that Institute funds could be inappropriately diverted to Foundation accounts, and/or that Foundation funds could be used for purposes that are not consistent with the donor’s intent.

### E. Travel

**Objective:** To determine whether the unit is accomplishing travel in accordance with the Institute's policies and procedures.

**Criteria:** The Institute's travel policies and procedures are contained in Section 6.0 of the Business and Finance Manual. 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.

**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 in violation of State law. If such violations were to occur, this could result in financial loss for the Institute, personal liability for the traveler(s), and negative publicity for the Institute.

### F. Cash and Receivables

**Objective:** To assess the strength of procedures in place within the unit to ensure that all Institute assets are being properly collected, deposited, and recorded on the Institute’s records.

**Criteria:** The Business and Finance Policies and Procedures Manual, Section 1.4, Cash Receipts and Accounts Receivables, and Section 1.6, Non-student Accounts Receivables, specifies, in part, the following:

Each department/unit is responsible for the funds it receives for the Institute. Cash receipts must be officially recorded on a cash register, 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." Duties of employees should be appropriately separated between the receiving of Institute receipts and the recordkeeping and preparation of deposits for the Bursar's Office. One person should not be responsible for all these functions. Department heads should make certain that proper safe-keeping 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. Cash register procedures should be prepared by departmental personnel in the form of written documentation and approved by Accounting Services. Cash register tape retention practices and proper references of deposits to daily cash register totals are subject to review and/or audit by authorized personnel in Accounting Services or the Internal Auditing Department. Locations which operate cash registers or have average daily receipts over $250 should prepare a daily cash report and retain them for three years.

Funds received by schools, departments, or units of the Institute must be deposited at the Bursar's Office no later than the next business day following the date of receipt. (For instances in which a unit receives small amounts of cash or checks - total less than $100 - which would not warrant a daily trip to the Bursar's Office, the funds may be
held no more than five business days.) All checks payable to Georgia Institute of Technology must be deposited to Institute accounts. Funds may never be deposited to the account of an individual or any account which has not been specifically authorized by the Controller.

The Non-student Accounts Receivable section of Accounting Services is responsible for billing and collecting invoices for units of the Institute (except Continuing Education).

**Risk:** Cash and receivables are susceptible to loss if not properly controlled. If segregation of duties, supervisory oversight, and physical security do not exist in their processing and handling, and there are no procedures in place to prohibit unauthorized invoicing, there is an elevated risk of errors and/or misappropriation. If, at year-end, units do not record open invoices on the Institute’s financial records, a misrepresentation of the Institute’s assets may occur.

G. Distribution and Control of Payroll Checks/Advices

**Objective:** To determine the strength of procedures in place within the unit to ensure that payroll checks are not automatically deposited for individuals who are not employees.

**Criteria:** Employees at Georgia Tech are paid automatically by deposits to personal bank accounts. Necessarily each unit must ensure that fictitious employees are not added to the unit’s payroll. Also, units must ensure that employees are timely terminated from the payroll to preclude checks being deposited for terminated employees.

**Risk:** Payroll checks are susceptible to fraud and abuse if not properly controlled.

H. Procurement

**Objective:** To assess the procedures in place within the unit to ensure that appropriate practices are followed in all aspects of the purchase of goods and services in accordance with Institute policies and regulations.

**Criteria:**

Procurement 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 or purchase of real property, 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 may be 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
- Board of Regents Procedures Manual
- Georgia Institute of Technology Business and Finance Manual, Section 5.0

**Risk:** If the unit does not follow appropriate purchasing practices, State laws, rules, or regulations may be violated and funds may be expended in an inefficient and uneconomical manner. This could increase the risk to the Institute of financial loss, inefficient use of resources, and adverse publicity.
I. Procurement Card

Objective: To examine the procedures followed by the unit to ensure appropriate controls exist over the use of Georgia Tech procurement cards (PCard) in accordance with Institute policies and sound business practices.

Criteria: The Office of Procurement 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 departments and units of the Institute. One method of purchase is with the Georgia Tech Procurement Card (PCard). Policies and Procedures in the Business and Finance Manual, Chapter 5, Purchasing and Accounts Payable, Section 5.2.1.8, Procurement Cards spell out the various controls over the PCard. Staff may be issued a PCard by completing a request form which is signed by a Department Head to indicate authorization, cardholder limits and cost allocation information. All cards are distributed to employees after Unit Card Coordinators are trained and Employee Agreement Forms signed. When accepting a PCard, the cardholder agrees to obtain best value, protect the card, abide by certain dollar limits, make only allowable purchases, and to maintain a purchase log and receipts, to periodically reconcile purchases against the bank’s billing statement, and to make such information available for audit as requested. The Institute’s maximum limit on PCard purchases is $5,000 per transaction and $2,999.99 for non-inventoried equipment. The standard monthly dollar limit is $25,000. There are no further Institute cardholder spending limits, however, the Department Head, may set additional limits which are noted on the approved request form.

Risk: If campus units do not follow appropriate PCard practices, there is an elevated risk that State laws and other regulations may be violated, funds may be misappropriated, or funds may be expended in an uneconomical or inappropriate manner. This could increase risk to the Institute of financial loss, legal liabilities, and adverse public relations.

J. Communications

Objective: To determine the strength of procedures in place within the unit to ensure that communications charges, (e.g., phones, fax machines, wireless devices, cable/DSL services, etc.) are appropriately monitored and controlled.

Criteria: The Georgia Department of Administrative Services (DOAS) manages the statewide communications services for the State of Georgia. The Institute’s Business and Finance Manual, Section 14.1, contains criteria for cellular telephone usage. This guidance points out that each unit is to implement procedures to effectively use communication services and equipment, at the lowest possible cost.

Risk: If communication charges are not appropriately monitored and controlled, there is an elevated risk of fraudulent or inappropriate use as well as inefficient and ineffective use of resources. This increases risk to the Institute of financial loss and adverse public relations.

K. Risk Management/Insurance

Objective: To determine the strength of procedures in place within the unit to ensure that insurance and liability concerns have been given appropriate consideration and that there are measures in place to minimize risks to the Institute regarding the unit’s activities.

Criteria: Risk Management Policies are written for the faculty, staff and students of Georgia Tech. They are intended to assist those who may have questions concerning risk, liability, insurance coverage and workers compensation. (See Business and Finance Manual, Section 8.0.) Final approval of all claims rests with the State Department of Administrative Services. In addition, all suits and legal actions become the responsibility of the Board of Regents and the Department of Law.

Risk Management Services is charged with the responsibility of 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.

Risk Management is a managerial/administrative process designed to minimize the exposure to risk as well as the adverse effects of accidental injuries and losses. The four steps in this process include:
• Risk Identification
• Measurement and Evaluation
• Control through Reduction and Elimination
• Finance

Generally, Risk Management Services is called upon to provide the various types of insurance coverage required by Georgia Tech and its employees, and to investigate all claims including pursuit of subrogation against third parties.

At Georgia Tech, there are serious concerns about injuries to individuals, whether they are part of the academic community, or the population as a whole. There are concerns about property losses, whether or not insured, and finally there are concerns about financial exposures and liability that the Institute could face due to actions of a unit or the actions of others.

Risk 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 Georgia Tech group, department, or individual contemplating any activity such as described above or involved in activities promoted by others is to call 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 insurance needs.

Risk: If the unit is involved in extracurricular activities that are beyond the scope of what would be considered routine and if the Office of Risk Management has not examined these activities to determine the appropriate level of insurance coverage for these activities, the Institute could be exposed to significant financial and legal risks in the event of an adverse situation.

HUMAN RESOURCES
A. Leave Reporting
Objective: To determine whether the unit's management of compensated leave is in accordance with the Institute's prescribed policies and procedures.

Criteria: The Institute's Human Resources Policies and Procedures Manual and an August 13, 1997 memorandum from the Executive Vice President for Administration and Finance and the Provost and Vice President for Academic Affairs contains criteria that campus units have a leave record keeping and reporting system that includes the following: (1) the maintenance of leave records, (2) at least monthly reporting by all faculty/staff, (3) monthly reporting or updating of the unit's official Institute leave records, and (4) the sharing of leave balances with employees regularly to verify the accuracy of such balances.

Risk: If vacation and sick leave records are not accurately maintained on a monthly basis, there is a risk that compensation to individuals could be improperly inflated. While this risk may be immaterial on an individual basis, the impact to the Institute collectively could be substantial. The failure to report leave usage can result in an inflated leave liability footnoted in the Institute's financial statements.

B. Off-campus Assignments
Objective: To determine the unit’s compliance with Board of Regents Policies and Procedures (Board of Regents Policy Manual, Section 800: Personnel, 302.0804 Education and Professional Leave), which gives guidance for employees of the University System of Georgia engaged in work away from their respective campuses.

Criteria: The Board of Regents Policy Manual Section 800 Personnel, Section 803.15, discusses “Leaves for Professional Personnel” in general. Georgia Tech “Policy on Absences from Campus for Professional Activities” as of February 22, 2000, developed by the Task Force on Campus Absences contains more detailed policy for faculty, as follows:
Occasional absences from campus are necessitated by the professional activities of most faculty members in a Research I university and are consistent with the Duties, Responsibilities, and Privileges of faculty described in the Georgia Tech Faculty Handbook, Section 2.8.2.2. (b). At the same time, it is essential that supervisors be cognizant of absences of faculty from campus and the reason for those absences and that there be a clear prior approval and administrative oversight process ensuring that Board of Regents and Institute policies are followed. The following procedures and approvals are intended to accomplish these objectives.

A. Procedures

1. Absences from campus of more than one business day for professional activities, including consulting, should be documented in advance by submission of a Travel Authorization Request Form (TAR), or other acceptable document as required for approval under Section B. This procedure is consistent with Section 2.8.2.2. (c) of the Faculty Handbook.
2. The purpose of an absence and an itinerary should be provided. Any deviations from the original itinerary must be clearly indicated and explained when requests for reimbursement from Georgia Tech are submitted.
3. For absences from campus for professional activities of one business day or less the faculty member should notify his/her supervisor or designated representative as to his/her location. A Travel Authorization Form is not required unless reimbursement for expenses is expected.
4. It is the faculty member’s responsibility to arrange for his/her duties to be performed during absences from the campus. Cancellation of undergraduate classes due to absences from campus is strongly discouraged.
5. All absences for consulting must be reported monthly.

B. Approvals

1. Absences of more than one business day must be approved by the School Chair or his/her designated representative.
2. Absences of more than ten consecutive business days must be approved by both the School Chair and the Dean of the College, who will notify the Provost’s Office.
3. A proposed absence of greater than half a term in duration must be forwarded to the President’s Office by the Dean of the College for consideration for a Leave of Absence as defined by the Board.

For eligible staff, Institute policy in the Human Resources Manual, Section 20, Attendance and Time Off, Subsection 2.11 on Leave of Absence, and 2.12 on Family Leave, have many of the same policies and approval requirements as the Faculty leave provisions described above.

Risk: Failure to comply with Board of Regents’ and Institute Policies and Procedures regarding off-campus assignments could subject the Institute to risk of inappropriately compensating employees for activities that do not meet the criteria for off-campus assignments. This could result in financial loss, personal liability for the individual(s) off-campus, and negative publicity.

C. Employment Eligibility Verification

Objective: To determine the unit’s compliance with the employment eligibility verification and employer sanctions provisions of the Immigration Reform and Control Act of 1986, Public Law 603.

Criteria: The Immigration Reform and Control Act of 1986 requires 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 and other 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.
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.

D. Sexual Harassment

Objective: To determine the strength of measures taken by the unit to create an environment in which the risk of sexual harassment is minimized.

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 Director of Equal Opportunity Programs for faculty and staff members and to the Dean of Students for students. An investigation is required by Institute officials. 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 Manual, the Classified Employee Handbook, or the Student Conduct Code as appropriate.

Risk: If units do not have systems in place to ensure that the Institute’s policies on sexual harassment are clearly communicated to all employees, and periodically reinforced, the risk of a sexual harassment incident is elevated. Risks to the unit and the Institute if such a situation were to occur could be significant in that this could (1) alienate employees, (2) create a hostile work environment, (3) result in lawsuits, fines and penalties for violations, and (4) cause adverse publicity.

E. Consultants vs. Employees

Objective: To assess the strength of procedures within the unit to manage independent contractors appropriately and ensure compliance with Internal Revenue Service (IRS) provisions.

Criteria: The Business and Finance Manual, Section 5.3.3 provides guidelines for making payments to individuals who are not employees. When the Institute is required to make payments to individuals, the rules and regulations of a number of governmental regulatory bodies must be considered. A determination is to be made to ensure that payments to individuals for services (instructors or consultants) clearly meet the Internal Revenue Service (IRS) definition of Independent Contractor and that the regulations of the Internal Revenue Service and Bureau of Citizenship and Immigration Services respect to Non-Resident Aliens have been followed.

Any individual who performs services for the Institute is presumed to be an employee unless the relationship satisfies the IRS’s standards for Independent Contractor. A consultant should be used only when the services are not readily available from existing employees or where the services cannot be performed more economically or satisfactorily through the Institute employment process.

The department/unit must make the determination 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. The questions are modeled after and capture the contents of the IRS 20 common law factors.
• 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”, campus units are instructed to consult Human Resources regarding employment of the individual. If all answers are “no”, the Purchase Request for Services form is used to request the purchase of and encumber funds for the expenses of independent contractors that are to be funded from state funds (instructions below). If the independent contractor will be paid from sponsored funds, the agreement must be executed through the Office of Contract Administration on a “Request for Sub-Agreement Form”.

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

F. Compliance with Equal Employment Opportunity Act
Objective: To assess the procedures within the unit to ensure compliance with the Equal Employment Opportunity Act and amendments thereto and how this Act influences operation of the unit.

Criteria: The Georgia Institute of Technology 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 Institute policies. 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 criteria is in the Human Resources Manual, Section 1.1.

Risk: If the unit were found to be in non-compliance with the Equal Employment Opportunity Act, the Institute could be subjected to adverse legal actions, resulting in fines and penalties as well as adverse public relations.

G. Annual Performance Evaluations
Objective: To determine if the unit accomplishes the required annual performance evaluation process in accordance with Institute criteria.

Criteria: Institute policy disseminated in a February 27, 1998 memorandum (and including on the OHR Web page) from OHR to all units required that all classified employees be evaluated at least once a year. The stated objective for each evaluation was to:

• Provide employees with clear and realistic expectations.
• Support employee development through discussion of assigned opportunities and training that will help employees function more effectively in their role and grow to their maximum individual potential.
• Emphasize the Institute’s commitment to continuous improvement and learning.
• Ensure an appropriate relationship between pay levels and work performance.
• Avoid surprises: keep lines of communication open and conduct a mid-cycle (six month) performance review annually.
• Encourage self-assessment: While self-assessment is not a mandatory component of this program, it does facilitate employee/supervisor communications and helps focus on performance issues.

The Regents' policies, contained in Section 3.3.1 of the Faculty Handbook, require that all faculty receive an annual, written review by their unit head. In addition, the faculty member will discuss this review with the unit head and will sign a statement to the effect that the faculty member has received the written review. The faculty member will have 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.

Risk: If the unit fails to properly prepare annual performance evaluations and follow-ups for all employees, there is a risk that future personnel decisions may be unsupported. In addition, it is a sound business practice to provide ongoing feedback to employees to ensure Institute objectives are being met.

H. Conflict of Interest
Objective: To determine if the unit administers Conflict of Interest policy in accordance with Institute criteria.

Criteria: Institute policy contained in Human Resources Manual, Section 5.4 entitled Conflict of Interest, emphasizes that for proper operation of democratic government, public officials must be independent and impartial and this objective could be impaired if a conflict exists between the private interests of a government employee and his or her duties. Institute procedures cover potential conflicts of interest pertaining to consulting services and an employee conducting business on behalf of the Institute with a business in which that person has a substantial financial interest. The Institute guidance specifies that no employee shall undertake any activity which constitutes a conflict of interest except as may be expressly approved and/or managed pursuant to the provisions of the stated policy.

Specifically, this guidance requires faculty to disclose any conflict of interest which arises during the course of the employee's employment to a responsible representative of the Institution. The reporting of a conflict of interest shall be aided by the completion of the "Georgia Institute of Technology Report on Outside Professional activity and Potential Conflict of Interest" form. Every faculty member must submit a completed request form at least annually on July 1 of each year to the responsible representative of the Institution. The Request Form shall be updated by the faculty member if the facts reported in the form change. The responsible representative of the Institution to whom a financial disclosure or report of a conflict of interest is made shall review the disclosure and shall make a determination whether a conflict of interest exists. A conflict of interest exists when the representative determines that a significant financial interest could directly and significantly affect the design, conduct, or reporting of the research or reduction activities funded or purposed for funding by a potential sponsor. Should a conflict of interest exist, the responsible representative of the Institution shall determine what restrictions, if any, should be imposed by the Institution to manage, reduce or eliminate such conflict of interest prior to the Institution's expenditure of any such funds.

Risk: If the unit fails to obtain and administer conflict of interest statements from employees the Institute could be at risk if there is conflict between the private interests of an Institute employee and his or her duties. It is essential to the proper operation of democratic government that public officials be independent and impartial. If a conflict exists, the conduct of impartial government business may be impaired and the Institute and individual could be subjected to fines and adverse publicity.

LEGAL AND REGULATORY
A. Contracts
Objective: To assess the procedures within the unit to ensure that individuals do not obligate the Institute inappropriately by entering into formal unauthorized commitments on behalf of Georgia Tech.

Criteria: According to the Business and Finance Manual, Section 5.4, few people within the Georgia Tech community are authorized to sign contracts on behalf of the Institute. Those authorized to sign contracts include the President; the Senior Vice President for Finance and Administration; the Vice President for Research; Purchasing Agents; and certain staff of the Office of Contract Administration.
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.

**Risk:** There are only a few individuals authorized to act as agents of the Institute in contracting with third parties. If units do not have processes in place to ensure that all employees understand and abide by these restrictions, individuals may become personally liable if they unknowingly contract in the name of the Institute. This could, in turn, cause adverse financial, legal, and public relations impacts for the Institute.

### B. Gifts

**Objective:** To assess the processes in place within the unit to ensure that the unit’s employees are aware of an adhere to both the State policy on the prohibition of accepting gifts, and to the Human Resources Manual, Section 5.1, which states “Georgia Tech policy is that the practice of accepting gifts or gratuities is unnecessary, undesirable, and contrary to the interest of the Institute.”

**Criteria:** Georgia Board of Regents' Personnel Manual, Section 8.2.13.1, Gratuities contains the following: An employee of the Board of Regents shall not directly or indirectly solicit, receive, accept, or agree to receive a thing of value by inducing the reasonable belief that the giving of the thing will influence his/her performance or failure to perform any official action.

The Governor of Georgia on January 10, 2011, issued an Executive Order establishing a code of ethics for executive branch officers and employees which rescinded a 1999 Executive Order pertaining to ethics. In the 2011 Executive Order, no gifts could be accepted by any person with whom the employee interacts on official business, including lobbyists and state vendors. A gift was defined as anything of value exceeding $25, including but not limited to, food, lodging, transportation, personal services, gratuities, subscriptions, memberships, trips, loans, extensions of credit, forgiveness of debts, or advances or deposits of money.

**Risk:** Acceptance of gifts by employees is against the law. It gives the appearance of improper preference or treatment in the conduct of normal business activities. If units do not have in place a process to communicate and routinely refresh this message with its employees, there is a risk that individuals may inappropriately accept gifts, increasing their risk of criminal liability as well as adverse public relations for the Institute.

### C. Open Records Act

**Objective:** To assess the processes in place to ensure that unit employees are made aware of their responsibilities regarding the Open Records Act (ORA).

**Criteria:** Guidance regarding ORA requests is in Open Record Act Request policy http://www.policylibrary.gatech.edu/legal/open-records-act-policy

Employees receiving ORA requests are instructed to contact their supervisor and Office of Legal Affairs for assistance in a correct response.

**Risk:** Institute records may be requested, through the ORA, virtually anywhere on campus. If units do not have processes in place to ensure that their employees are properly informed of ORA requirements and procedures, there is an elevated risk that individuals fielding those requests could be found personally liable if they did not properly comply with the terms of the law. This could, in turn, create adverse consequences and negative publicity for the Institute.

### HEALTH AND SAFETY

#### A. Safety of Workplace

**Objective:** To determine whether: (1) the unit has established reasonable policies and procedures for ensuring safety in the workplace for reducing and/or preventing injuries and illnesses; (2) the unit has ensured that all employees have received required training in the area of workplace safety; and (3) the unit has in place a practice to ensure that all employees comply with rules and regulations regarding workplace safety.
Criteria: The Institute Safety policy http://www.policylibrary.gatech.edu/safety-security promotes the development of a safety program. The Environmental Health and Safety Department (EHSD) may be contacted to provide guidance in the development of unit safety programs. Further, the Institute has policies that deal with the areas of fire/life safety, environmental health, occupational health and safety, and laboratory safety, to ensure that employees receive all required training and comply with the various rules and regulations pertaining to each of these areas.

Risk: Significant property damage, occupational injury, illness, or even death can result if individuals are not properly trained or if the unit fails to provide a safe work environment. This could subject the Institute to substantial fines from regulatory enforcement agencies and negative publicity which in turn could adversely affect research activity and the reputation of the Institute.

B. Chemical Safety
Objective: To determine whether: (1) the unit/Principle Investigator (PI) has established reasonable policies and procedures for ensuring safety when individuals are exposed to chemicals in the workplace or laboratory; (2) the unit/PI has ensured that all individuals working with chemicals have received the required training in the area of chemicals and equipment (e.g. lasers, fume hoods, etc.) safety; and (3) the unit/PI has in place a practice to ensure that all individuals comply with rules and regulations regarding chemical and equipment safety.

Criteria: It is the policy of Georgia Institute of Technology 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 Institute has other policies that deal with the areas of fire/life safety, environmental health, occupational health and safety, and laboratory safety. Each department is responsible for working with the EHSD, to ensure that employees receive all required training and comply with the various rules and regulations pertaining to each of these areas.

Risk: Significant property damage, injury, illness, or even death, can result if individuals who come in contact with chemicals are not properly trained in chemical safety. This could subject the Institute to substantial fines from regulatory enforcement agencies and negative publicity which in turn could adversely affect research activity and the reputation of the Institute.

C. Hazardous Waste
Objective: To determine whether: (1) the unit has established reasonable policies and procedures for ensuring environmental protection safety and compliance; (2) the unit has ensured that all employees have received required training in the area of environmental protection and hazardous materials; and (3) 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.

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. The Institute policy for protecting the environment is contained in www.policylibrary.gatech.edu/campus-use-facilities/environmental-health-and-safety

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 asbestos emissions. If units do not ensure that appropriate procedures are followed for the handling of hazardous wastes, the Institute could be subject to fines from regulatory enforcement agencies and negative publicity that could adversely affect research activity and public reputation.

D. Biological Safety (Laboratories only)
Objective: To determine whether: (1) the unit has provided necessary information and guidance to Institute administrators responsible for governance of the environmental, health, and safety of Institute faculty, staff, and students; and (2) the unit has ensured that all employees have received required and appropriate training in the area of environmental protection and bio hazardous materials.
Criteria: Since the tragedy of September 11, 2001, recent national security measures relative to biological agents have created federal laws such as the Patriots Act, Bioterrorism Bill (HR 3448), Public Laws 42 CFR 73 and 72 (Center for Disease Control regulations), 7 CFR 331 (USDA regulation – relative to plants), and 9 CFR 121 (USDA regulation – relative to animals). The Institutional Biosafety and Biohazards Board will be establishing Institute policy in support of these new federal laws. Further, it is the policy of Georgia Tech that hazardous chemical and biological 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.

Risk: Georgia Tech is obligated to protect the general and Institute environments by properly managing and disposing of hazardous chemical and biological waste. Furthermore, the Institute could be subject to negative publicity and fines from regulatory enforcement action that could adversely affect research activity and student population.

INFORMATION SYSTEMS
A. Strategy and Vision
Objective: To determine the strength of processes in place over the planning and guidance given by management for the oversight and expected direction of the information technology deployed within 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

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.

B. Logical Security
Objective: To assess the strength of logical controls within the information systems of the unit. Logical controls focus on the processes by which access to data is controlled, systems files are organized, etc.

Criteria: Logical controls are those controls that exist to prevent access by unauthorized parties to data. These are some examples of controls that can prevent the security breach from ever happening:

• Authentication - It is often extremely important to ensure that a claimed identity is valid. The authentication control provides the means to verify the identity of a subject.
• Authorization - The authorization control enables specification and subsequent management of the allowed actions for a given system.
**Risk:** If units do not ensure systems are in place to establish proper logical security, the integrity of the system, data, and availability of systems may be compromised. Such compromises could result in theft of propriety data: unauthorized (malicious, non-malicious, or accidental) disclosure, modification, or destruction of information; and/or non-malicious errors and omissions. These conditions could have an adverse impact on the unit’s ability to achieve its objectives and subject the Institutes to negative publicity should sensitive information be compromised.

**C. Physical and Environmental Controls**

**Objective:** To assess the strength of physical and environmental controls as they are used to provide an environmentally conditioned, physically safe, and physical access-controlled environment for information systems assets in the unit. To determine the degree to which the unit has taken into consideration the vulnerabilities of their systems to fire damage, water damage, inadequate temperature and humidity controls, malicious physical access, and reasonable steps to mitigate these risks.

**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.

**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.

**D. Data Stewardship**

**Objective:** To assess the strength of processes in place within the unit to ensure that Institute data to which the unit has access and over which the unit has responsibility is appropriately controlled and protected.

**Criteria:** Data is an important campus unit business asset. “Data stewardship,” for the purpose of this section, is defined as the prudent management of Georgia Tech’s data. Georgia Tech’s data is defined as:
- Data provided to external stakeholders. External stakeholders are defined as public and private organizations with which Georgia Tech conducts business. Examples include other DOD offices, Congress, other government agencies, laboratories, contractors, and the general public.
- Data provided to internal stakeholders. Internal stakeholders are the individual organizational components that comprise Georgia Tech.
- Data that may be of a sensitive nature. Examples of sensitive data include budget, personnel, propriety, reviewer and procurement data.

**Risk:** The responsibility to secure Institute data is shared by all members of the Institute community who have access to the data. If unit data is not properly protected, the unit’s ability to accomplish its organizational objectives may be hindered. If sensitive data is not appropriately protected from unauthorized access, the Institute could be subject to significant financial penalties and legal liability.

**E. Equipment Maintenance**

**Objective:** To assess the procedures in place within the unit to ensure that hardware and software are monitored for vulnerabilities and routinely maintained in accordance with manufacturers’ guidelines and solid business practices.

**Criteria:** Physical devices such as computers are susceptible to failure. Information systems and associated computers have been designed to work in a controlled environment and will fluctuate in reliability as they age. Proper maintenance will extend the life, power, and capability of the system.

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.
Risk: If systems are not appropriately maintained, there is an elevated risk of hardware failure, system degradation, loss of information, loss of productivity, and software corruption.

F. Business Continuity of Information Systems
Objective: To assess the steps the unit has taken to ensure the timely recovery of information systems in the event of information systems service interruption or loss of resources. Recovery of information systems should be viewed as a subset of a more comprehensive plan that each unit should have to ensure the continuity of key operations in the event of power outages, inaccessibility to facilities, fire, etc.

Criteria: According to the National Institute of Standards in Technology:

“IT systems are vulnerable to a variety of disruptions, ranging from mild (e.g., short-term power outage, disk drive failure) to severe (e.g., equipment destruction, fire) from a variety of sources such as natural disasters to terrorists actions. While many vulnerabilities may be minimized or eliminated through technical, management, or operational solutions as part of the organization’s risk management effort, it is virtually impossible to completely eliminate all risks. In many cases, critical resources may reside outside the organization’s control (such as electric power or telecommunications), and the organization may be unable to ensure their availability. Thus effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability.”

NIST Contingency Planning Guide SP 800-34

There are several guides to emergency management that address backup and recovery and business continuity and although no single guide is a solution they all reference similar critical steps to aide in emergency management and business continuity. Internal Auditing most often references NIST Contingency Planning Guide SP 800-34. Internal Auditing does not audit adherence or compliance to the NIST publication but rather uses it as a resource to provide a framework for evaluating backup and recovery and business continuity plans. NIST Contingency Planning Guide SP 800-34 is a publicly available guide located at www.nist.gov.

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.

G. Training
Objective: To assess the procedures in place in the unit to ensure that: (1) users of information systems are adequately trained and informed on proper use of the unit’s information systems; and (2) systems administrators are adequately trained to ensure the appropriate administration of the unit’s information systems.

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 (System 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 principal assets and thereby their business/education
- Set clear standards of service expectation of use
- Promote and encourage discovery and creativity

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.

H. Software Licensing
Objective: To ascertain the strength of controls in place within the unit to ensure that all software on the unit’s computers adheres to licensing agreements.

Criteria: The Georgia Tech Computer and Network Usage 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 guidance.
- Software 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.

Risk: Commercial software vendors are becoming increasingly aggressive in enforcing their rights under the copyright laws. If the unit does not have procedures in place to ensure that only licensed software is installed on the unit’s computers, there is an elevated risk of the unit being in violation of Federal law for copyright infringement. If violations were found, the financial and legal penalties to the Institute, as well as adverse publicity, could be significant.

I. Operations/Administration
Objective: To assess the strength of procedures in place to ensure appropriate management, administration, and operation over the unit’s information systems resources.

Criteria: Operations are the daily tasks that are needed to keep an information system operating and effective. The key component in the scheme is the system administrator and his knowledge of the information systems located within the unit. Effective operations will:

- Keep operation costs as low as possible
- Keep the subnet tuned for maximum speed and efficiency
- Mesh information resources to the campus unit’s business style
- Keep networks reasonably secure
- Provide reasonable means to accomplishing desired use

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.

J. Web Site Operation/Development
Objective: To determine the strength of procedures in place within the unit to effectively and securely operate and maintain a Web presence in accordance with sound practices and Institute policies.

Criteria: It is well understood that much of the future growth and efficiency of educational efforts will rely on 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) offers a tremendous low cost marketing potential to each Georgia Tech campus unit.

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 visual presentation of information and the methods of delivery are usually the first thing potential students see of Georgia Tech.

**Risk:** If the unit operates a Web server, it is critical to establish appropriate security. If systems are not adequately secured, there is a high risk of compromise of Institute data, compromise of the campus network, corruption of systems, loss of productivity and adverse public relations.

**PUBLIC RELATIONS**

**A. Public Relations Management**  
**Objective:** To determine the strength of procedures in place within the unit to inform faculty and staff of Institute policies regarding dissemination of information to the public.

**Criteria:** The Institute's Media Communications and Marketing website www.comm.gatech.edu.

**Risk:** If the unit does not have procedures in place to ensure that all faculty and staff are aware of: (1) who can speak on behalf of the Institute and in what circumstances, and (2) who is authorized to share Institute data, there is a risk of misinformation resulting in adverse impact to the reputation of the Institute.

**B. Association with External Organizations**  
**Objective:** To determine if there are procedures in place to advise faculty and staff of their responsibilities to appropriately represent Georgia Tech if they are involved in the financial management of external organizations (e.g., professional societies, etc.).

**Criteria:** Good business practice calls for basic fiscal internal controls.

**Risk:** If faculty and staff have financial control over external organizations and their involvement in those organizations is due to their association with Georgia Tech and supported by their supervisors, this increases risk to the reputation of the Institute in the event of mismanagement of those external funds.

**STUDENTS**

**A. International Students**  
**Objective:** To assess the strength of procedures in place within the unit to ensure that student employees within the unit are in compliance with the Immigration Reform and Control Act of 1986, Public Law 99-603, and amendments thereto.

**Criteria:** Regulations of the U.S. Citizenship and Immigration Services (formerly Immigration and Naturalization Service) impose certain record-keeping and reporting requirements on Institutes who enroll non USA citizens or enroll and provide employment to non USA citizens, or non-resident aliens.

At Georgia Tech, Admissions is responsible for issuing the I-20 Form (Certificate of Eligibility) for non-working students. Office of International Education is responsible for the IAP-66 Form (based on a request from the sponsoring organization) for a working student. Either form enables a student of another country to obtain a non-immigrant status visa, F-1 visa status for the non-working student and J-1 for the working student and an entry permit I-94 Form. The Office of International Education also represents the Institute in providing copies of I-94 Forms, passports and other documentation required by Immigration and Naturalization Services for non-USA students. The Office of Human Resources is responsible for having all employees complete the I-9 Form, Employment Eligibility Verification, which documents a working students' citizenship.

**Risk:** If the unit does not ensure that its students and student employees have maintained required documentation and complied with reporting requirements for non-resident alien students, it could subject the Institute to fines and penalties imposed by the federal government, jeopardize the student’s ability to pursue his/her academics, as well as increase the risk of adverse publicity for the Institute.
B. Sexual Harassment

Objective: To assess the strength of procedures within the unit to create an environment in which the risk of sexual harassment involving students (e.g., students within academic programs in the unit and/or students employed within the unit) is minimized and all employees are made aware of Institute policies on a safe work environment.

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. This policy 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 tolerated.

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 to be -- either explicitly or implicitly -- a term or condition of an individual's employment or academic standing;
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, their academic performance, or by creating 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 Director of Equal Opportunity Programs for faculty and staff, and to the Dean of Students for students. All complaints will be investigated by Institute officials. 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 Manual, the Classified Employee Handbook, or the Student Conduct Code as appropriate.

Risk: If units do not have systems in place to ensure that the Institute's policies on student sexual harassment are clearly communicated to all employees (including student employees), and periodically reinforced, the risk of a sexual harassment incident is elevated. If such a situation were to occur, risks to the unit could be significant in that this could (1) alienate employees, (2) create a hostile work environment, (3) result in lawsuits, fines and penalties for violations, and (4) cause adverse publicity.

C. Protection of Information

Objective: To assess the strength of policies and procedures in place within the unit to ensure that student information is appropriately safeguarded.

Criteria: Much of student academic data is covered by the Family Education Rights and Privacy Act of 1974 (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.

Risk: Given the stringent Federal regulations (e.g., FERPA) regarding the protection of student data, if this data were disseminated inappropriately, it could negatively impact the student and potentially subject the Institute to significant financial penalties, legal liability, and negative publicity.
GENERAL

A. Policies and Procedures

Objective: To assess the strength of the unit's documented internal policies and procedures and to assess the degree to which these are used to guide the actions of the unit.

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.

Risk: If policies and procedures are not clear and comprehensive and effectively communicated, there is a risk that decisions made and actions taken might not be in accordance with Institute policies, State and Federal laws, etc. In addition, in the event of turnover, there is risk that individuals new to the organization may not have clear guidance on the performance of key tasks which could lead to loss of productivity.