DEPARTMENTAL REVIEW

SCHOOL OF WISE THOUGHTS

March 17, 2003

GEORGIA INSTITUTE OF TECHNOLOGY

Department of Internal Auditing
Web Site: www.audit.gatech.edu
Office: 404/894-9480

206 Administration Bldg.
Atlanta, GA 30332-0254
Fax: 404/894-6990

TABLE OF CONTENTS

EXECUTIVE SUMMARY

INTRODUCTION

The Department of Internal Auditing conducted an Institute-wide risk assessment to identify significant areas of risk facing the Institute. Through discussions with many members of senior management and academic officials, different key areas of risk were identified as being applicable in most organizational units across campus.

The Department of Internal Auditing developed a Departmental Audit process through which we review, in each Department on campus, the controls in place to ensure that these risks are appropriately mitigated and managed. The material contained in this report reflects the results of the departmental review of the School of Wise Thoughts. The Chair of the School of Wise Thoughts reports directly to the Dean of the College of Deep Theoretical Studies.

OBJECTIVE AND SCOPE

The objective of our review within the School of Wise Thoughts was to examine each of these areas of risk to determine the strength of the controls for appropriate risk mitigation.

To that end, the steps in our review process included:

- Meeting with key individuals within the School of Wise Thoughts to examine the controls over each of these areas;
- Reviewing policies, procedures, and practices followed;
- Examining selected samples of transactions to verify policies and procedures are being adhered to; and
- Conducting selected physical examinations of the control environment within the School of Wise Thoughts.

Our review was conducted in accordance with the *Standards for the Professional Practice of Internal Auditing.*

SUMMARY

Through our review, we found that there were **reasonable to strong controls** in place in 24 (61.6 %) of the areas reviewed. Some of the areas in which controls were particularly strong included:

- Procedures for ensuring Accuracy of Financial Records
- Procedures and controls over Leave Reporting
- Procedures pertaining to Annual Performance Evaluations

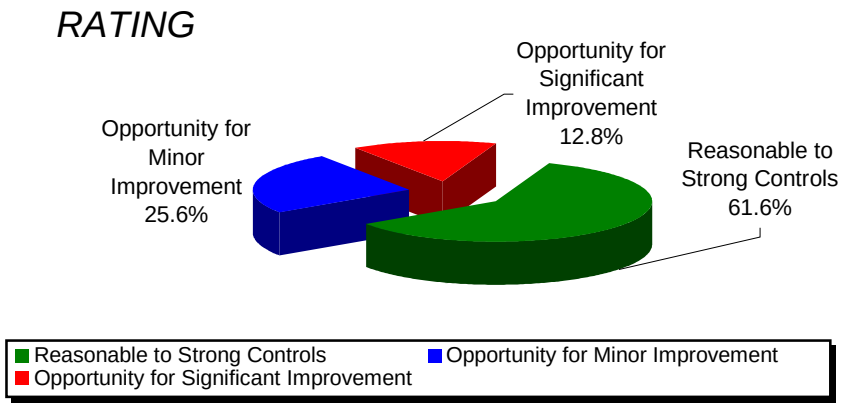
We noted **opportunities for minor improvement** in 10 (25.6%) of the areas reviewed. These areas were as follows:

- Procedures regarding management of Risk Management
- Procedures relating to Gifts, Public Relations and Sexual Harassment
- Procedures relating to the following Information Systems areas – Data Stewardship, Management, Equipment Maintenance, Vendor Relations, Software Licensing
- Policies and Procedures

Finally, we noted **opportunities for significant improvement** in 5 (12.8%) of the areas reviewed. These areas were Information Systems areas – Logical Security, Backup and Recovery, Training, Operations/Administration, and Web Site Operations/Development

One area, Environmental Protection, was determined to be "Not Applicable."

The chart below provides a visual depiction of the results of our review.



Our detailed discussion on each of the 39 areas reviewed is shown in the following pages.

On the final pages of the report, beginning on Page 24 is an **Action Plan**. This plan summarizes the Recommendation made and includes, with Management's input, the specific tasks that should be accomplished to address the areas.

We are confident that, with Management's cooperation and their commitment to address these issues, the School of Wise Thoughts will be well positioned to have strong risk mitigation procedures in place over each of the areas reviewed.

COLOR LEGEND FOR AUDIT CONCLUSIONS

- Audit conclusions which appear in a regular **black** font denote risk areas within the School which were found to be **reasonably to strongly managed** (**green coloring was used for chart purposes**).
- Audit conclusions which appear in a **blue** font color denote risk areas within the School which show **opportunities for minor improvement**.
- Audit conclusions which appear in a **red** font color denote risk areas within the School for which there are **opportunities for significant improvement**

AREAS OF FISCAL RISK

Accuracy of Financial Records

Objective: To determine whether the School verifies 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 School.

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

Observation: The School maintains an internal shadow system. Approximately once per month the shadow system is reconciled to the Institute general ledger. The School employs the Project Expense and Budget (PEB) Report and the Monthly Project Cost Detail Report for the purposes of reconciliation. As requests for account information or adjustments are received from professors, the Accountant checks these accounts to ensure they are being reconciled. In addition she uses a checklist of active accounts to ensure that all accounts are reconciled monthly.

Conclusion: The School appears to be taking appropriate measures to mitigate risk in the area of Accuracy of Financial Records.

Sponsored Programs

Objective: To ascertain how the School verifies that costs charged to sponsored programs are proper and in accordance with both Institute procedures and Grants and Contracts stipulations.

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

Observation: The shadow system spreadsheet has a built-in calculation that verifies costs charged to sponsored programs. All accounts are reviewed during the monthly reconciliation. Outline information regarding each sponsored agreement is kept in the business office of the School. Any questions related to charges are referred to the Office of Sponsored Projects. Currently any adjustments are made on-line via PeopleSoft. Before the PeopleSoft system was available all adjustments were made via hard copy requests sent to the Office of Grants and Contracts. The individual identifying a need for transfer (faculty or staff) must write a justification for the transfer and submit it to the Chair. The Chair authorizes all transfers. The transfer request is then sent to the Office of Grants and Contracts. The monthly reconciliation process is used to discover postings that should be transferred on the Appropriation Ledger. The Principal Investigator must authorize all cost transfers either verbally or in writing. The monthly reconciliation assures a timely processing of any cost transfers.

Conclusion: The School appears to be taking appropriate measures to mitigate risk in the area of sponsored programs.

Capital Assets

Objective: To determine how the School controls and accounts for capital assets.

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.

Observation: The Unaccounted Equipment Summary Report dated June 4, 2001, indicated that the School of Wise Thoughts had no missing equipment at this time. The Georgia Tech Schedule of Investment in Plant for the year ended June 30, 2000 showed that the School had a total investment of $1,500,222.00. The School follows Georgia Tech policies and procedures in all respects of dealing with capital assets. When an

item of equipment enters the School, the Computer Services Specialist tags it. He then enters the data into the on line capital assets tracking system. He also keeps paper copies of the documentation on file in his office and maintains a database file of the capital assets in the School. When the School conducts its annual inventory, location corrections are made to the list at that time. The School is currently located in one building so that any equipment moves are from one room to another. Equipment moves are reported on the hard copy version of the form designed for that purpose. The School staff makes its best effort to account for every item on the inventory list. Any equipment that cannot be found is reported to Capital Assets Accounting with an explanation. Any staff or faculty members who remove equipment from the building are required to complete a Loan Agreement. The decision to surplus a piece of equipment is made by either the Chair or the director of the laboratory where the equipment is located. From that point the Computer Services Specialist completes the appropriate paperwork and contacts Capital Assets Accounting for a pick up.

Conclusion: The School appears to be taking appropriate measures to mitigate risk in the area of Capital Assets.

Foundation

Objective: To determine if the School exercises reasonable and prudent care in the acceptance and administration of private, non-sponsored Foundation funds.

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.

Observation: The Administrative Manager is responsible for overseeing Georgia Tech Foundation funds. She uses the School shadow system and monthly reconciles this to the Institute records. In addition she compares the shadow system to statements received from the Foundation. The School does not solicit gifts, but works through the Office of the Dean of the College of Deep Theoretical Studies. An Institute form containing an explanation of the gift, along with the check itself and the donation letter are all sent to the Foundation when any gifts are received in the School. A copy of the donation letter is kept on file in the office of the School. These letters usually contain the donor’s major points of interest and any restrictions. The Administrative Manager keeps a copy of the donor restrictions in her office. Visibility is maintained by using the monthly reconciliation process. The Administrative Manager reconciles Institute and Foundation accounts.

Conclusion: The School appears to be taking appropriate measures to mitigate risk in the area of Foundation funds.

Travel

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

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. Such violation is probably not likely to occur often; however, if such violations were to occur, it could result in financial loss for the Institute, and could generate negative publicity.

Observation: A sample of travel vouchers was selected based on auditor judgment. No discrepancies were noted in this documentation. Each individual desiring travel completes a Travel Authority Request (TAR) form. The School Chair approves all TARs. Either the Accountant or the traveler themselves will make the travel arrangements. The TAR is filed in the Accountant's office until the travel is complete. At this point the traveler completes a Travel Expense Statement (TES) and attaches original receipts to the TES. The traveler submits the TES to the Accountant. The Accountant verifies the charges by examining the receipts to ensure

that they are original, related to the trip in business terms, and match the figures on the TES. During her review of the TES, the Accountant specifically looks for items that might be personal expenses. Also she checks the receipt dates against the dates listed on the TAR. She also foots and cross foots the TES and checks to ensure that travel expense dates listed on the TES match the dates requested on the TAR. Finally the Accountant makes copies of all the documentation and forwards the original material to Accounts Payable. The Accountant processes each Travel Expense Statement as it is submitted. She estimates a one to two day process time. This depends on whether the TES has errors that must be corrected. She keeps the copy of the material in a pending file and checks every few days to see if a check has been cut for the TES.

Conclusion: The School appears to be taking appropriate measures to mitigate risk in the area of Travel.

Cash and Receivables

Objective: To determine if the School is ensuring that all Institute assets are being properly collected, deposited, and recorded on the Institute's records.

Risk: Cash is susceptible to loss if not properly controlled. Invoicing by unauthorized individuals can result in loss of receipts if not prohibited. Plus, units may not realize that open invoices at year-end must be recorded on the Institute's financial records.

Observation: The School sometimes collects cash on behalf of student organizations housed within the School. The collections range from $8 to $15, and are dues the students owe to these School organizations. The funds are locked in a desk drawer in the Accountant's office until they are deposited. Deposits are usually made the same day the funds are received. The Accountant collects and deposits the funds. The club Treasurer is responsible for reconciliation. The School does not have procedures for reporting shortages or thefts.

The School also operates a petty cash account. This account is a checking account located at Bank of Norway. The account is used for paying research subjects for their participation in research projects conducted by School professors. The cycle of payment is as follows.

A professor conducting a research project completes a "Request for Petty Cash or Check(s)" form used within the School. The Accountant generates the checks using a system developed by the Computer Services Specialist. The checks are sometimes complete (i.e. payee, amount, date, etc.). Sometimes the payee is omitted. This situation is dictated by the needs of the professor and is the result of being able to determine, in advance of the experiment, who will be a subject and who will not. Amounts are NEVER left blank. Once the checks have been prepared, someone from the laboratory conducting the experiment picks them up from the office. Along with the checks, this individual receives a check roster listing all the checks they have received. The person collecting the checks must also sign a "Petty Cash Log" that is kept in the office stating the numbers of the checks they took. The lab conducts the experiment and pays the subjects on the spot. The subject must sign the roster to indicate that they received their check. The completed check roster is returned to the School business office along with any void or unused checks. The Accountant reconciles the roster and returned checks to her listing of checks that were issued to ensure that all checks are accounted for. A list of completed and voided checks is sent to Accounting Services. Accounting Services receives the statement on the account from Bank of America and reconciles this statement to the list sent from the School. The School completes a request to Accounting Services to replenish the account whenever needed.

The Chair, the Administrative Manager, and the Department of Internal Auditing discussed various alternatives to the situation of controlling a large cash account through the School. The Chair stated that participation by subjects was greatly reduced if payment was mailed. People will not participate in these studies if the reward (the check) is delayed for any period of time. We discussed the possibility of giving the subjects vouchers and letting them collect their checks at the Bursar's office. The Chair stated that much of the research done in his School is related to senior citizens. Again, asking senior citizens to traverse the campus reduces the number of participants significantly. In addition to this the Administrative Manager stated that the Bursar's Office was openly reluctant to assume this duty. She also stated that in all the time

this system had been in place, the School did not have any instances of missing checks that had been cashed by unknown persons.

The Department of Internal Auditing and the Director of Accounting Services discussed the issue involving payments to research subjects. The Director of Accounting Services did not offer an alternative to the current practice. He stated that his concern was primarily that the account that the School operated for this purpose sometimes ran minimal or even deficit balances due to slow submission of reimbursement requests.

Conclusion: The School appears to be taking appropriate steps to mitigate risk in the area of Cash and Receivables.

Recommendation: We recommend the School compose a set of written procedures to follow in the event of shortage or theft. We also recommend that the School make every effort to process the requests for reimbursements as expeditiously as possible.

Management Response: *We are in the process of composing written procedures to deal with possible theft or shortage. These procedures will also include steps for processing reimbursement so as to assure expeditious handling of that matter.*

Distribution and Control of Payroll Checks

Objective: To determine if the School properly controls and distributes payroll checks.

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

Observation: Either the Accountant or the Administrative Manager retrieves the checks from the Payroll Department. The Accountant verifies the checks and advises received against the check roster. All checks are kept in a locked drawer in the Accountant's office until the payee collects them. Payees must initial the check roster to show that they received their check. Anyone who is collecting a check that is not the payee must have written authorization from the payee to get the check. The initialed check rosters are kept for approximately one year. The Accountant makes an attempt to locate a forwarding address for any uncollected checks. If this is unsuccessful, the uncollected checks are returned to the Payroll Department within thirty days.

Conclusion: The School appears to be taking appropriate measures to mitigate risk in the area of Distribution and Control of Payroll Checks.

Procurement

Objective: To determine if the School follows reasonable practices in all aspects of the purchase of goods and services, including the use of procurement cards.

Risk: If the School does not follow sound purchasing practices, they may violate State laws, rules, or regulations, and expend funds in an uneconomical manner.

Observation: For any purchase greater than $1,000, or items on State contract, the School sets up a purchase order. The purchase order is processed through the PeopleSoft system. For smaller purchases, a check request is used. Copies of all invoices sent to the School are forwarded to the professor in charge of the purchase so that this professor may verify receipt of the goods and/or services. P-cards are used whenever possible and this eliminates the need for either a purchase order or check request. The Accountant compares the receipts for purchase to statements received from the card company. She sends an email to cardholders for any missing receipts. She enters the transactions into the School's shadow system and reconciles this to the Institute general ledger. Each cardholder is asked to review his statement and compare them to the receipts in order to verify that the statement is correct. The cardholder signs the statement to indicate that they have reviewed the transactions. Any invoice that is received that contains State sales tax is paid for an amount minus the tax.

Conclusion: The School appears to be taking appropriate measures to mitigate risk in the area of Purchasing/P-Cards.

Telecommunications

Objective: To determine if the School has reasonable controls over its telecommunication costs.

Risk: Telecommunication charges are posted to the School's expenditure records without review. In the absence of a post review of such charges, errors, omissions, or abuses could go undetected.

Observation: All faculty and staff are given printouts listing their monthly charges. They are asked to review the charges for accuracy and then sign the printout indicating that they have reviewed it. In addition they are asked to identify any personal charges and reimburse the School for those charges. The Chair also reviews the entire bill for the School in order to identify any charges that look unusual. These records, including copies of any reimbursement checks are kept on file in the office of the Administrative Manager. The School has no phones accessible to the public. There is one telephone on the counter in the business office. It is not enabled for long distance service. The School has no cell phones. The Administrative Manager conducts an annual inventory of all the lines in the School and compares that to the invoice.

Conclusion: The School appears to be taking appropriate measures to mitigate the risk related to Telecommunications.

Risk Management

Objective: To determine the adequacy and reasonableness of the School's management of insurance and liability concerns.

Risk: Institute assets may be put at risk should the School incur liability above the Institute's self-insured limits.

Observation: The School holds a picnic for the new graduate students every year. This event is open to the entire department. Currently the School does not address the issue of insurance coverage for this event. The School does not collect waivers of liability from participants in extra-curricular events.
All keys not issued to an individual are kept locked in a key cabinet in the office of the Administrative Assistant. The Administrative Assistant keeps a log of all the keys and individuals must sign in order to receive a key. When an employee leaves, the School uses an exit checklist to process them out. One of the items on the checklist is the return of all keys.

Conclusion: Due to lack of input from the Office of Risk Management, the School is currently experiencing some risk in the area of Risk Management.

Cause: Historically the School has not had a major incident in this area and has not viewed it as a risk.

Recommendation: We recommend the School contact Chuck Squarejaw in Risk Management (BR-549) for consultation regarding the picnic.

Management Response: We will contact Chuck regarding the picnic and any other activity that we may be uncertain about the risk factors involved.

AREAS OF HUMAN RESOURCES RISK

Leave Reporting

Objective: To determine whether the School's management of compensated leave is in accordance with the Institute's prescribed policies and procedures as outlined in an August 13, 1997 memorandum from the Senior Vice President for Administration and Finance and the Provost and Vice President for Academic Affairs. This memorandum stated that campus units should 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 Institute official leave records, and (4) the sharing of leave balances with employees regularly to verify the accuracy of such balances.

Risk: Inflated compensation can result from improper vacation and sick leave record keeping, which may be immaterial individually, but material for the Institute in total. The failure to report leave usage can result in an inflated leave liability footnoted in the Institute's financial statements.

Observation: On a monthly basis, all employees receive a vacation and sick leave report listing their individual data; time available beginning, vacation/sick leave accumulated, vacation/sick leave taken, and ending balance. The employee is asked to sign this report in verification of the figures listed. The leave information is then updated in the PeopleSoft system. The Administrative Manager monthly compares this information to the information contained in the report from the Institute Business Office.

Conclusion: The School appears to be taking appropriate measures to mitigate risk in the area of Leave Reporting.

Off-Campus Assignments

Objective: To determine the School's compliance with Board of Regents Policies and Procedures 803.15, which gives guidance for employees of the University System of Georgia, engaged in work away from their respective campuses.

Risk: Failure to comply with Board of Regents 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 and/or negative publicity.

Observation: The Chair has been in his position for six years and has never had anyone from the School assigned off-campus. He also does not foresee this situation occurring in the near future. He is confident that if such a situation were to occur that he would follow the Georgia Tech policies and procedures for administering the process.

Conclusion: The School neither has a person currently in an off-campus assignment status, nor has it had anyone in this status in the past. The Chair recognizes the importance of following established Institute policies and procedures with regard to this matter.

Employment Eligibility Verification

Objective: To determine the School's compliance with the employment eligibility verification and employer sanctions provisions of the Immigration Reform and Control Act of 1986, Public Law 99-603.

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 (INS), a hold put on hiring of non-resident aliens, as well as adverse publicity.

Observation: All new hires are sent immediately to the Office of Human Resources to complete necessary paperwork. The School sends a confirmation sheet with the new hire for the Office of Human Resources to sign indicating that the employee is clear to begin work. The School relies on communications from the Office of Human Resources to notify them of upcoming work eligibility expiration. When this occurs the

Administrative Manager contacts the individual in question and directs them to go to the Office of Human Resources to ensure that they are in compliance.

Conclusion: The School appears to be taking appropriate measures to mitigate risk in the area of Employment Eligibility Verification.

Sexual Harassment

Objective: To determine whether measures are being taken by the School to create an environment in which the risk of sexual harassment is minimized.

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.

Observation: All of the School staff has attended formal Office of Human Resources training in sexual harassment prevention. The Chair includes this material in staff meetings at various times. Part of the faculty has also completed this Office of Human Resources training program. Also the Chair discusses the issue at faculty meetings with some degree of regularity. In addition the Chair takes the initiative to talk with faculty members on an individual basis when circumstances seem to merit. The Chair disseminates the information during faculty and staff meetings. Also he annually circulates a reminder of the Institute's web page policy.

Conclusion: The School appears to be taking appropriate measures to mitigate risks in the area of Sexual Harassment.

Consultants vs. Employees

Objective: To ascertain whether the School manages independent contractors appropriately and complies with Internal Revenue Service (IRS) provisions.

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.

Observation: If a faculty member hires a contractor, the transaction goes through the Office of Sponsored Programs. If the contractor is hired using State funds, the transaction is processed through Procurement. The faculty member who writes the grant proposal is responsible for determining the classification of the consultant/employee and the scope at that time. The faculty member supervising the work must authorize payment. It is up to that person to monitor and report on the work.

Conclusion: The School appears to be taking appropriate measures to mitigate risk in the area of Consultants vs. Employees.

Compliance w/Equal Employment Opportunity Act

Objective: To determine how aware the School is of the Equal Employment Opportunity Act, and amendments thereto, and how this Act influences operation of the School.

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

Observation: For faculty: All positions that the School is trying to fill are advertised in a broad array of professional Wise Thoughts journals. This is done so as to attract as wide a variety of applicants as possible. The Chair cites his record of hiring as proof of the success of this effort. In his six years as Chair, he has hired six faculty members, four of whom have been female.

For staff: The School tries to employ a broad range of advertising mediums in order to ensure that a diverse group is attracted. The Chair again cites his record of hiring and notes that he has a rich mix of male, female, and minority members working in his School. The Chair also relies on guidance and council from the Office of Human Resources in maintaining a diverse work force.

With regard to promotional opportunities, the Chair makes a conscious effort to promote qualified people without regard for race, gender, or other non-job related factors. In terms of training, the Chair's policy is to support any training one of his employees desires so long as it relates in some manner to improving the work processes of the School.

Conclusion: The School appears to be taking appropriate measures to mitigate risk in the area of Compliance with the Equal Opportunity Employment Act.

Annual Performance Evaluations

Objective: To determine that the School accomplishes required annual performance evaluation process in accordance with Institute criteria.

Risk: If the School fails to properly prepare annual performance evaluations and follow-ups for all employees, they may not have a basis for personnel decisions.

Observation: For the faculty: Annually each faculty member reports to the Chair using a form devised within the School. The information on which a faculty member reports consists of items such as; number of classes taught, number of papers written and published, grants secured, etc. This information is submitted to a personnel committee that the Chair has assembled. The committee consists of three faculty members. They examine the report, provide comments and input, and then forward the report to the Chair. The Chair then examines the same report and takes into consideration the comments from the committee. The Chair composes a response to the report and sends it to the faculty member as a means of evaluation and feedback. The Chair is open to any faculty member who feels they would like to meet personally for discussion.

For the staff: The Administrative Manager evaluates all staff members. She completes her evaluation and discusses them with the Chair. She then discusses the evaluations with each individual employee. The employee signs the evaluation and receives a copy. A copy is forwarded to the Office of Human Resources. The Chair evaluates the Administrative Manager.

Conclusion: The School appears to be taking appropriate measures to mitigate risk in the area of Performance Reviews.

AREAS OF LEGAL AND REGULATORY RISK

Contracts

Objective: To determine whether the School has procedures to preclude unauthorized commitments on behalf of Georgia Tech and whether campus School staff understand who can obligate the Institute and under what circumstances.

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

Observation: The Administrative Manager stated that no School employee is authorized to initiate agreements between Georgia Tech and outside organizations. All contracts must be processed through the School's accounting office. The Administrative Manager forwards all contracts to the Institute Business

Office. No laboratories conduct business transactions on their own. The School Chair reminds the faculty during meetings that they are to conduct all business through the Administrative Manager.

Conclusion: The School appears to be taking appropriate measures to mitigate risk with respect to Contracts.

Gifts

Objective: To determine whether the School's employees adhere to State policy on the prohibition of accepting gifts. The Governor issued, in January 1999, strict guidelines prohibiting gifts to State employees.

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 this law were broken, the individuals involved would be criminally liable and this occurrence could bring significant adverse publicity for the Institute.

Observation: Any business conducted by the School is routed through the Administrative Manager. She is aware that it would be inappropriate to accept gifts from those doing business with the School. Annually the faculty is asked to sign a conflict of interest statement saying that they have no involvement with companies doing business at the Institute. The School, however, has no formal communication of the Governor's gift restriction policy in place.

Conclusion: Due to a need for explicit communication with all staff regarding gift acceptance, the School is experiencing some risk in the area of Gifts.

Cause: The School has not historically had any problems in this area and has not viewed it as a point of risk.

Recommendation: We recommend the School periodically refresh the topic at faculty and staff meetings. In addition they should distribute the Governor's memo to all faculty and staff.

Management Response: *Copies of the Governor's memo have been distributed to all faculty and staff. In addition, a copy is being kept in the business office for future reference. We will schedule the topic for inclusion in future staff and faculty meetings.*

Open Records Act

Objective: To determine whether School employees are aware of their responsibilities regarding the Open Records Act (ORA).

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

Observation: The School staff is aware of its responsibilities concerning the Open Records Act. They understand the time restrictions involved and have plans to contact pertinent parties regarding any request.

Conclusion: The School appears to be taking appropriate measures to mitigate risk in the area of Open Records Act.

AREAS OF HEALTH AND SAFETY RISK

Safety of Workplace

Objective: To determine:

- Whether the School has established reasonable policies and procedures for ensuring safety in the work place;
- Whether the School has ensured that all employees have received required training in the area of work place safety; or
- Whether the School has in place a practice to ensure that all employees comply with rules and regulations regarding work place safety.

Risk: Occupational injury or illness, or death as well as significant property damage can result from improper training or failure of the Institute to provide a safe work environment. Furthermore, the Institute could be subject to fines from regulatory enforcement action and negative publicity that could adversely affect research activity and student population.

Observation: All exits are well lit. The Computer Services Specialist ensures that there are no tripping hazards on the floors, such as loose tiles or misplaced equipment. The School handles no hazardous materials. The School has no confined working areas.

Conclusion: The School appears to be taking appropriate measures to mitigate risk in the area of Safety of Workplace.

Environmental Protection

Objective: To determine:

- Whether the School has established reasonable policies and procedures for ensuring environmental protection safety and compliance;
- Whether the School has ensured that all employees have received required training in the area of environmental protection and hazardous materials; and
- Whether the School has in place a monitoring process through which to ensure that all employees comply with rules and regulations regarding environmental protection and hazardous materials.

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.

Observation: The School produces and handles no hazardous materials.

Conclusion: This area is not applicable.

AREAS OF INFORMATION SYSTEMS RISK

Logical Security

Objective: To assess the adequacy of logical controls within the School. Logical controls are not physical, meaning that logical controls focus on the data, systems, file organization, etc.

Risk: Without proper logical security the integrity of the system, data, and availability of the system may be compromised. Such compromises may result in:

- Theft of proprietary data
- Unauthorized (malicious, non-malicious, or accidental) disclosure, modification, or destruction of information
- Non-malicious errors and omissions
- Unauthorized access to other network systems and devices through a compromised system

Observation: We noted the following:

1. The School does not enforce password policy in accordance with Institute network usage policy. That policy states, in part: "The Georgia Tech campus policy requires password changes every 90 days. However, changing your password once a month is a good habit to start. This will keep hackers on their toes and keep someone from being able to access your account if by some means they have acquired your previous password."
2. The School has no formal procedure or routine monitoring of unauthorized access.
3. The School has no procedure or policy in place to ensure minimum user safeguards like time limits or time outs after a minimum period of activity.

Conclusion: The School is experiencing considerable risk in the area of Logical Security because procedures for changing passwords, establishing safeguards and reviewing administrative access are not in place as they should be.

Cause: As is the case, worldwide, with the rapid growth in reliance upon information systems for operations, research, and administration, the school's information systems security is struggling to keep up pace with the threats to systems administration and security. The organization's manning has not kept up with the growth and security challenges.

Recommendation: We recommend:

1. Establishing a minimum password policy in accordance with the Office of Information Technology for user access to Georgia Tech domain network resources.
2. Reviewing logs for anomalies and system policy violations. Suggest using automated tools available at http://www.tntsoftware.com/ or Microsoft tools utilities, PsTools or http://www.systemtools.com/elm/elm_main.htm to reduce manual review time. Other products are available for Linux/Unix.
3. Reviewing access requirements for all users. Consider limiting administrative and staff (users requiring access to the Institute's administrative services) to access after hours only on an exception basis. Instituting screen saver/energy saver capabilities of Windows and Unix workstations/clients to lock terminals after a 15-minute period of inactivity to safeguard against users leaving workstations unattended while they are logged on.

Management Response:

1. *We have reviewed the policies regarding passwords and are in the process of implementing corrective actions.*

2. *The CSR will review logs regularly in the future.*
3. *We are evaluating user access requirements and will adjust access according to the outcome of our review.*

Environmental Controls

Objective: To assess the adequacy of environmental controls as they are used to provide a conditioned environment for information systems assets in the School.

Risk: If environmental concerns are inadequately addressed, information systems assets and data may be lost because of:

- Fire damage
- Water damage
- Hardware failure

Observation: Each server has an uninterruptible power supply, good for ten to twelve minutes. The school uses the rule of thumb that if the room occupants are comfortable and dry, then so is the equipment. Backup diskettes and tapes are protected from extremes in temperature, magnetic fields, water, etc., by being stored in a safe.

Conclusion: Environmental controls are adequate.

Physical Security Controls

Objective: To assess the adequacy of controls over physical information systems resources and how secure they are against physical dangers such as theft-based upon the vulnerability/risk assessment of the School.

Risk: If information systems assets are not properly controlled and identified the campus unit may:

- Incur loss due to theft, intentional or unintentional misuse, and litigation
- Have unpredictable system operation or downtime
- Software may be stolen or counterfeited

Observation: Information systems items with a value less than $1,000 are not monitored by the Capital Assets program. However, the Computer Services Specialist, who does double duty as the Capital Assets representative, tracks small value information systems items on a separate Excel spreadsheet. Physical access controls are adequate.

Conclusion: Overall physical security of servers and labs is adequate.

Data Stewardship

Objective: To assess the adequacy of management's understanding of their responsibility in protecting data sensitive to Georgia Tech operations. Management's understanding of stewardship responsibilities and the resulting propagation of policy and awareness are critical to success of Georgia Tech.

Risk: Data compromised or lost due to poor data stewardship may pose adverse effects on business operations, competitiveness, and public relations. Monetary loss may occur if the compromise is severe enough.

Observation: School data is not categorized or classified**.** There are no data stewards. The Computer Support Specialist was not aware of individual requirements for the system to support the School's data. Individuals are responsible for identifying and protecting the School's proprietary data.

Conclusion: School management and staff have not put in place a system to make sure data sensitive to the Institute's operations are protected. This area needs further review.

Cause: School managers are unfamiliar with data categories and data management.

Recommendation: We recommend the School read and comply with Institute data management policies and procedures located at: http://www.security.gatech.edu/policy/data_access.html. This policy states in part, "each employee at the Institute will be responsible for being familiar with the policy as it relates to his or her position and job duties." This may be accomplished by holding staff meetings in which this policy is reviewed with the staff, by notices, emails and memos circulated to the staff to remind them of data protection requirements and consequences for the compromise of Institute data access policies. New personnel should be afforded the opportunity and time to read the Institute's data access and network usage policies.

Management Response: *We are currently reviewing the above listed policy and will compose emails and meeting agendas to comply.*

Management

Objective: To assess the management oversight of information systems local to the School.

Risk: Information systems play a critical role in all campus unit operations. Inadequate management may lead to:

- Loss of Information resources
- Loss of proprietary data
- Loss of productivity
- Hardware damage
- Software corruption of proprietary systems
- Compromises of systems
- Damage to reputation

Observation: Management has not developed any formal strategic plan for Information Systems acquisition, development or security.

Conclusion: The School is experiencing some risk in the area of management because of the absence of a strategic plan.

Cause: Insufficient attention has been given to the information systems infrastructure.

Recommendation: We recommend the School provide the time and resources to review current and future information systems support requirements and develop a plan that encompasses acquisition, budgeting, staffing, and administration of the School's information system hardware and software.

Management Response: *We are currently in the process of scheduling meetings. The purpose of these meetings will be to discuss plans for future information systems requirements. Acquisition, budgeting, staffing, and administration of the School's hardware and software will be considered during these meetings and the results of the meetings will be reduced to writing.*

Equipment Maintenance

Objective: To assess the adequacy of maintenance controls and procedures for information systems, software and hardware.

Risk: Loss of critical resources can occur if maintenance is not applied. Losses due to poor 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

Observation: The School does not perform scheduled preventive maintenance on its information system hardware.

Conclusion: Because the School does not have a preventive maintenance program in place they are experiencing some risk in this area.

Cause: Insufficient personnel resources prevent the planning and performance of routine preventive maintenance of information system resources.

Recommendation: We recommend the School develop a plan to conduct preventive maintenance on information systems hardware.

Management Response: *A preventive maintenance schedule will be developed and reduced to writing.*

Backup and Recovery

Objective: To assess the steps a campus unit has taken to assure the proper timely recovery of their information systems.

Risk: Information systems play a critical role in all campus unit operations. Even a minor glitch in power can cause operations to be interrupted. Such interruptions can cause:

- Loss of Information resources
- Loss of proprietary data
- Loss of productivity
- Hardware damage
- Software corruption of proprietary systems

Observation: The School has not developed a business continuity plan. As a result, the School does not have procedures for the backup and recovery of information systems in the event of a substantial or total loss of those systems. Backups are done on the server but remain in the same room as the server. No backup policy or guidance is provided to individual users of individual workstations.

Conclusion: Because of the absence of a backup and recovery plan for information systems, the School is not assured timely recovery of its normal operations.

Cause: The increased importance of and dependence on information systems has outgrown the current organization's methods for recovery of information systems.

Recommendation: We recommend the following:

1. School should develop a backup and recovery plan that considers, at a minimum, the following:
    a. Identifying critical information systems resources
    b. Developing a backup scheme which would provide for total recovery of critical resources (additional information and guidance can be found on the web site of Internal Auditing at http://audit.gatech.edu/)
2. School should conduct a user awareness program to remind users of their responsibilities towards backing up the data on their workstations.

Management Response: *A backup and recovery plan such as the one listed above is currently under development. Included in this plan will elements of a user awareness program.*

Training

Objective: To assess the adequacy of training given to system users and control personnel.

Risk: Information systems play a critical role in all campus unit operations. Inadequate training may lead to:

- Loss of information resources
- Loss of proprietary data
- Loss of productivity
- Hardware damage
- Software corruption of proprietary systems
- Compromises of systems
- Damage to reputation
- High turnover rates
- Decreased system efficiency
- Increased operational costs

Observation: No formal or informal training is in place for users or information system support personnel. Users are not made aware of information security issues or good information systems practices.

Conclusion: Users are not making the best use of systems and security is not maintained current. There is a high probability that users are unaware of their individual requirements for backing up data, proprietary data, and software license infringements.

Cause: The School has no formalized training or indoctrination program.

Recommendation: We recommend the School develop a formal plan for the indoctrination of new staff and students into the School's information system responsibilities and requirements. The School should routinely post notices and bulletins/emails to staff and students highlighting information system trends, issues and tips.

Management Response: *We will revise current new employee orientation material to include indoctrination to the School's information systems responsibilities and requirements.*

Vendor Relations

Objective: To assess the adequacy of vendor focused relationships for systems located within the School. This is not to assess the adequacy of vendor relations for which the School does not have system administration responsibility.

Risk: Poor vendor relations may adversely affect the campus unit and expose the unit to risk such as:

- Theft of proprietary data
- Unauthorized (malicious, non-malicious, or accidental) disclosure, modification, or destruction of information.
- Non-malicious errors and omissions

- Public Relations issues
- Business continuity issues

Observation: The School's Computer Support Specialist is not responsible for monitoring contracts or vendor relationships.

Conclusion: The School is experiencing some risk in the area of vendor relations because the Computer Support Specialist does not monitor this area.

Cause: The School has no procedure in place regarding vendor relations.

Recommendation: We recommend the School ensure that contract warranties and vendor guarantee/service information is made available for the Computer Support Specialist to track. We also recommend using a project management chart like a Gant chart or Excel spreadsheet to reflect equipment/service milestones.

Management Response: *We are in the process of locating all contract warranties and vendor guarantee/service information. This information will be made available to the CSS. The CSS will establish and maintain an Excel spreadsheet to reflect equipment/service milestones.*

Software Licensing

Objective: To ascertain whether the School has controls that ensure that all software on Institute computers have proper licenses and that use of software adheres to all licensing agreements.

Risk: Commercial software vendors are becoming increasingly aggressive in enforcing their rights under the copyright laws. Virtually all software products are licensed to the user under the copyright laws of the United States. 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 monetary loss and adverse publicity.

Observation: The School has a semi-formal plan for maintaining copies of software licenses purchased. There is no effort to monitor the installation of software and license compliance outside the labs.

Conclusion: The systems administrator is on the right track but an adequate formalized software management program is not completely in place.

Cause*:* As the School has placed more reliance on information systems; emphasis on proper adherence to software licensing had not kept pace.

Recommendation: We recommend the School Chair allocate resources to put the appropriate software management program in place to control licensing agreements. This program should include:

1. A system to verify that all software on unit computers is properly licensed and employees adhere to software license restrictions to include installation, use, copying, number of simultaneous users, terms of license, etc.
2. An inventory of software showing name, type, and license number for each item of software by computer. Some automated software inventory systems are commercially available. Some suggestions for review include: Timbuktu/Netoctopus, LANAUDIT, and GASP.

Management Response: *A software management program is currently being developed. Once complete, the program will comply with the above listed qualifications.*

Operations/Administration

Objective: To assess the controls in place to ensure operations are adequate for the School's information resources.

Risk: Operations/administration risk can affect the information system in every way. It has a drastic effect on the effectiveness, efficiency, confidentially, and reliability of information resources. 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
- Compromises of systems
- Damage to reputation
- High turnover rates
- Decreased system efficiency
- Increased operational costs

Observation: The Computer Support Specialist is knowledgeable about the requirements and has pro-actively solicited the aid of other employees and students in operations of his subnets. The number of workstations and servers under his cognizance is more than the assigned personnel can expect to efficiently manage. There are no "cyclical operations" or central program support requirements. The Computer Support Specialist is expected to manage the system, conduct troubleshooting and repairs as well as monitor system usage.

Conclusion: The personnel requirements for this size of network should support at least three separate functions, Administration, Security and Equipment Maintenance. This School is severely undermanned.

Cause: There has been insufficient priority of resources to adequately fund these positions.

Recommendation: We recommend the School review staffing, job descriptions and actual manpower available to determine where additional resources should be applied within the existing budget.

Management Response: *As a course of the previously mentioned meetings we will also review staffing, job descriptions, and available manpower and reallocate resources accordingly.*

Web Site Operation/Development

Objective: To assess the adequacy of website security, operation and its alignment with Georgia Tech policy.

Risk: The risks associated with web presences are vast. Some of these follow:

- Damage to reputation
- Monetary loss
- Theft of data
- Corruption of data
- Loss of needed information resources
- Loss of productivity
- Hardware damage

- Software corruption of proprietary systems
- Compromises of systems
- Decreased system efficiency
- Increased operational costs

Observation: The School is not aware of the Georgia Tech web policy. There is no dedicated web server or web master that reports to the Computer Support Specialist. The web server and homepages are high vulnerabilities.

Conclusion: The web page is not in compliance with Georgia Tech Policy.

Cause: The School staff is not aware of Georgia Tech policy regarding website operations.

Recommendation: We recommend the School conduct a risk assessment over its web services. Through this review, a determination should be made as to whether the service justifies the risk. For those web servers that are deemed essential, care should be taken to ensure they are maintained to the appropriate level of security. The School should also review its web services with an Office of Information Technology webmaster to ensure compliance with Institute policy. See guidance at:

http://www.security.gatech.edu/policy/

Management Response: *Our staff will review the Georgia Tech policies regarding web sites and bring our site into compliance. In addition, we will contact the Office of Information Technology for advice on how to proceed.*

AREAS OF PUBLIC RELATIONS RISK

Public Relations Management

Objective: To determine how the School informs faculty and staff of Institute policy regarding dissemination of information to the public.

Risk: Misinformation can negatively impact the Institute's image.

Observation: The School has no organized approach for dealing with public relations management. In addition, the School has not yet established a working relationship with Institute Communications and Public Affairs.

Conclusion: Due to the lack of a tangible policy on the issue, the School is experiencing some risk in the area of Public Relations Management.

Cause: Historically the School has had little or no opportunity to employ an organized approach to this area. As a result the area has not been viewed as one of risk.

Recommendation: We recommend the School establish a relationship with the Director of Institute Communications and Public Affairs and seek input from this organization regarding the best method for preparing a communications plan.

Management Response: *We will contact the Director of Institute Communications and Public Affairs for consultation regarding preparation of a communications plan for the School.*

Association with External Organizations

Objective: To determine the adequacy of internal controls over financial management of external organizations (e.g., professional societies, student organizations, etc.).

Risk: Mismanagement of fiscal matters concerning external organizations by Georgia Institute of Technology employees could subject the Institute to financial loss and adverse publicity.

Observation: The Chair is not aware of any members of his staff or faculty that participate in the financial management of any external organizations.

Conclusion: The School does not appear to be experiencing risk in the area of Association with External Organizations.

AREAS OF RISK DEALING WITH STUDENTS

International Students

Objective: To discuss the School's management practices regarding compliance with the Immigration Reform and Control Act of 1986, Public Law 99-603, and amendments thereto.

Risk: Failure to maintain required documentation or comply with reporting requirements for non-resident alien students could subject the Institute to fines and penalties imposed by U.S. Immigration and Naturalization Service as well as adverse publicity.

Observation: The Academic Advisor at the School of Wise Thoughts begins the process by completing the necessary paperwork that the foreign student will use to obtain a visa. This package is forwarded, along with instructions for any remaining information to be completed, to the potential student. This student signs the forms, completes any remaining information, and obtains their visa. Once the student's visa is successfully obtained, s/he may enter this country to study. The School conducts a student orientation. Any foreign students are provided assistance from School staff in completing any remaining paperwork they are required to have. Then they are sent to the Office of Human Resources for final processing. The School informs students of the stipulation of immunization, but the actual immunization process is handled by the Student Health Center. There is a hold on the students' accounts that can only be removed once there is proof of immunization.

Conclusion: The School appears to be taking appropriate measures to mitigate the risk associated with International Students.

Sexual Harassment

Objective: To determine measures taken by the School to reduce the risk that students may be subjected to or involved in sexual harassment.

Risk: Sexual harassment can (1) alienate students, (2) create a hostile educational environment, (3) cause lawsuits, (4) subject the Institute to fines and penalties for violations, and (5) cause adverse publicity.

Observation: The School conducts a new graduate student orientation during which the subject is addressed. The School has a female Associate Chair. The Chair believes that this fact provides balance and encourages female students to report issues that they might otherwise be reluctant to discuss. The School has no formal approach for informing the employees/students of the Institute's sexual harassment policy.

Conclusion: Due to a lack of reinforcement, the School is experiencing some risk in the area of Sexual Harassment.

Cause: The School has not had serious problems with this issue and as a result has not viewed it as an opportunity for improvement.

Recommendation: We recommend the School refresh the policy periodically by circulating emails or hard copy brochures to the students.

Management Response: *We will include this topic in new student orientation and post copies of the brochures on public bulletin boards.*

Protection of Information

Objective: To ascertain measures taken by the School to protect private student information.

Risk: If private student data is disseminated inappropriately, it could negatively impact the student and possibly subject the Institute to legal liability, negative publicity, and the loss of Federal funding.

Observation: All student files are kept in the office of the Academic Advisor. This office is kept locked whenever he is not in the office. He allows no files to be taken from his office. Anyone who wants to examine his or her file must do so in the Academic Advisor's office. The Academic Advisor, the Chair, and the Administrative Manager hold the only keys to the office.

Conclusion: The School appears to be taking appropriate measures to mitigate risk in the area of Protection of Information.

AREAS OF GENERAL RISK

Policies and Procedures

Objective: To determine how Institute policies and procedures, and/or internally developed policies and procedures, are used to guide the actions of the School.

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.

Observation: Georgia Tech policies and procedures are referenced on frequent occasions. If policies and procedures do not effectively address the issue under scrutiny, the Administrative Manager will contact either the Dean's office or the business unit specializing in the matter (i.e. Legal, OHR). The School has internal policies and procedures addressing a number of issues. These issues include, but are not limited to; cash processing, p-card use, telephone policy, job descriptions, and a host of other subjects. They are not centrally located, but are distributed to user locations. For example, the telephone policies are kept in the telephone invoice file. However, there is no documentation to support information systems training, operations, or planning.

Conclusion: Because information systems policies and procedures are not documented, Computer Support Specialist personnel and users are left too work in a vacuum and often are poorly informed of appropriate controls, or there are no controls.

Cause: The School does not sufficiently emphasize maintaining adequate, current information systems documentation.

Recommendation: We recommend that School management develop information systems documentation to support as a minimum: Local operating procedures, adaptation of Institute network usage policy, a local

security policy, network diagrams, appropriate inventory of hardware and authorized software, and procedures for providing feedback to Computer Support Specialist personnel.

Management Response: *School policies and procedures will be developed and reduced to writing. Included in this documentation will be documentation to support: local operating procedures, adaptation of Institute network usage policy, a local security policy, network diagrams, appropriate inventory of hardware and authorized software, and procedures for providing feedback to Computer Support Specialist personnel.*

****

We would like to thank the staff of the School of Wise Thoughts for their cooperation and assistance during this review process. We are confident that, with management's cooperation and their commitment to address these issues, the School of Wise Thoughts will be well positioned to have strong risk mitigation procedures in place over each of the areas reviewed.

Sincerely,

Robert N. Clark, Jr.
Director of Internal Auditing

RNCJr/bch-DR-03-000/2003-0000

ACTION PLAN

RECOMMENDATION SUMMARY		TASK	RESPONSIBLE PERSON	TARGETED DATE	STATUS
1.	**AREAS OF FISCAL RISK – Cash and Receivables:** We recommend the School compose a set of written procedures to follow in the event of shortage or theft. We also recommend that the School make every effort to process the requests for reimbursements as expeditiously as possible.	General guidelines for the use of the petty cash system for subject payments are already in place; however, more explicit instructions regarding shortage/theft of funds will be distributed to the labs.	Admin. Manager	July 2002	Completed 7/17//02
2.	**AREAS OF FISCAL RISK – Risk Management:** We recommend the School contact Freddie Everett in Risk Management (404-894-3483) for consultation regarding the picnic.	Contact Risk Management regarding each School picnic or off-campus event.	Admin. Manager	August 2002	Completed 8/24/01
3.	**LEGAL AND REGULATORY RISK – Gifts:** We recommend the School periodically refresh the topic at faculty and staff meetings. In addition they should distribute the Governor's memo to all faculty and staff.	The department Chair will annually (each fall) distribute an email reminder to faculty/staff regarding the Governor's policy on gifts.	Chair	September 2002	In Progress
4.	**INFORMATION SYSTEMS RISK – Logical Security:** We recommend: 1. Establishing a minimum password policy in accordance with the Office of Information Technology for user access to Georgia Tech domain network resources. 2. Reviewing logs for anomalies and system policy violations. Suggest using automated tools available at	Each of the suggested software will be reviewed. The appropriate software will be installed and used by the Computer Specialist to review and maintain the security event logs of the Department's computers/servers. • Each PI is responsible for his research computers. • The Institute Password policy will be reviewed and an appropriate password policy will be applied to the Departmental Servers.	Computer Specialist and individual PI's	January 2003	In Progress

RECOMMENDATION SUMMARY	TASK	RESPONSIBLE PERSON	TARGETED DATE	STATUS
http://www.tntsoftware.com/ or Microsoft tools utilities, PsTools or http://www.systemtools.com/elm/elm_main.htm to reduce manual review time. Other products are available for Linux/Unix. 3. Reviewing access requirements for all users. Consider limiting administrative and staff (users requiring access to the Institute's administrative services) to access after hours only on an exception basis. Instituting screen saver/energy saver capabilities of Windows and Unix workstations/clients to lock terminals after a 15-minute period of inactivity to safeguard against users leaving workstations unattended while they are logged on.	• The restriction of login hours is not appropriate to this department. Graduate Students and Faculty need access at all times. Much of the work done in this department is done after normal working hours and on weekends. • The screen savers are implemented on staff computers. This is not applicable to research computers and lab computers.			

RECOMMENDATION SUMMARY		TASK	RESPONSIBLE PERSON	TARGETED DATE	STATUS
5.	**INFORMATION SYSTEMS RISKS – Data Stewardship:** We recommend the School read and comply with Institute data management policies and procedures located at: http://www.security.gatech.edu/policy/data_access.html. This policy states in part, "each employee at the Institute will be responsible for being familiar with the policy as it relates to his or her position and job duties." This may be accomplished by holding staff meetings in which this policy is reviewed with the staff, by notices, emails and memos circulated to the staff to remind them of data protection requirements and consequences for the compromise of Institute data access policies. New personnel should be afforded the opportunity and time to read the Institute's data access and network usage policies.	An e-mail will be sent on a regular basis to the staff with a URL link to the GA Tech Website Policy.	Chair	January 2003	In Progress
6.	**INFORMATION SYSTEMS RISKS – Management:** We recommend the School provide the time and resources to review current and future information systems support requirements and develop a plan that encompasses acquisition, budgeting, staffing, and administration of the School's information system hardware and software.	The Computer Specialist, along with the Chair, will develop a plan to manage the information system equipment.	Chair and Computer Specialist	January 2003	In Progress

RECOMMENDATION SUMMARY		*TASK*	*RESPONSIBLE PERSON*	*TARGETED DATE*	*STATUS*
7.	**INFORMATION SYSTEMS RISKS – Equipment Maintenance:** We recommend the School develop a plan to conduct preventive maintenance on information systems hardware.	Currently relationships are in place with vendors to maintain current equipment. The computers in the department are bought with a three-year maintenance agreement with the vendor. These computers are used for research and at the end of three years the computers are budgeted to be replaced by current computers. Computers in use that are over three years old require purchasing of an extended warranty/maintenance agreement. Several computers in the deptartment over three years old are used by Graduate students. The value of the computers do not warrant acquisition of a maintenance agreement; thus, they will be used until they are obsolete at which time they will be sent to surplus and replaced.	Computer Specialist	January 2003	In Progress

RECOMMENDATION SUMMARY		TASK	RESPONSIBLE PERSON	TARGETED DATE	STATUS
8.	**INFORMATION SYSTEMS RISKS – Backup and Recovery:** We recommend the following: 1. School should develop a backup and recovery plan that considers, at a minimum, the following: a) Identifying critical information systems resources b) Developing a backup scheme which would provide for total recovery of critical resources (additional information and guidance can be found on the web site of Internal Auditing at http://audit.gatech.edu/) 2. School should conduct a user awareness program to remind users of their responsibilities towards backing up the data on their workstations.	A plan will be developed by the Computer Specialist to inform users of their responsibilities to their data. This will be sent out by e-mail and will be posted. A back-up plan currently exists with regard to data maintenance on the department's servers. Daily back-ups are done and the data cartridges are kept in a fire resistant case and stored in a locked cabinet. A monthly backup will be placed in another building on campus.	Computer Specialist	January 2003	In Progress
9.	**INFORMATION SYSTEMS RISKS – Training:** We recommend the School develop a formal plan for the indoctrination of new staff and students into the School's information system responsibilities and requirements. The School should routinely post notices and bulletins/emails to staff and students highlighting information system trends, issues and tips.	Currently when something pertains to IT for the Wise Thoughts School (e.g.,-notices of new viruses) an e-mail is sent to whole School with the warning of the new computer virus program. This is also true for any information that is needed by the students, staff and faculty for the School.	Computer Specialist	January 2003	In Progress

RECOMMENDATION SUMMARY		TASK	RESPONSIBLE PERSON	TARGETED DATE	STATUS
10.	**Information Systems Risks – Vendor Relations:** We recommend the School ensure that contract warranties and vendor guarantee/service information is made available for the Computer Support Specialist to track. We also recommend using a project management chart like a Gant chart or Excel spreadsheet to reflect equipment/service milestones.	A database will be setup by the Computer Specialist to track departmental equipment warranties and reflect maintenance records on departmental equipment.	Computer Specialist	January 2003	In Progress
11.	**INFORMATION SYSTEMS RISKS – Software Licensing:** We recommend the School Chair allocate resources to put the appropriate software management program in place to control licensing agreements. This program should include: 1. A system to verify that all software on unit computers is properly licensed and employees adhere to software license restrictions to include installation, use copying, number of simultaneous users, terms of license, etc. 2. An inventory of software showing name, type, and license number for each item of software by computer. Some automated software inventory systems are commercially available. Some suggestions for review include: Timbuktu/Netoctopus, LANAUDIT, and GASP.	A Database will be setup by the Computer Specialist to track Software licenses for all departmental computers. Each staff employee will be informed of the license policy which is to adhere to the terms of the license for each piece of software used. Each PI will be responsible for the use of software in his research labs and offices.	Computer Specialist Appropriate PI.	January 2003 January 2003	In Progress In Progress

	RECOMMENDATION SUMMARY	TASK	RESPONSIBLE PERSON	TARGETED DATE	STATUS
12.	**INFORMATION SYSTEMS RISKS – Operations/Administration:** We recommend the School review staffing, job descriptions and actual manpower available to determine where additional resources should be applied within the existing budget.	The Chair along with the Administrative Manager and Computer Specialist will develop any appropriate actions in this area after determining manpower needs.	Chair, Administrative Manager, Computer Specialist	September 2002	In Progress
13.	**INFORMATION SYSTEMS RISKS – Web Site Operations/Development:** We recommend the School conduct a risk assessment over its web services. Through this review, a determination should be made as to whether the service justifies the risk. For those web servers that are deemed essential, care should be taken to ensure they are maintained to the appropriate level of security. The School should also review its web services with an Office of Information Technology webmaster to ensure compliance with Institute policy. See guidance at: http://www.security.gatech.edu/policy/	This URL will be sent out in an e-mail by the Chair for review by the Faculty and Staff.	Chair	January 2003	In Progress
14.	**RISK DEALING W/AREAS OF PUBLIC RELATIONS – Public Relations Management:** We recommend the School establish a relationship with the Director of Institute Communications and Public Affairs and seek input from this organization regarding the best method for preparing a communications plan.	The Associate Chair will be the point person for all P.R. for the School of Wise Thoughts and will establish a relationship with John Smith and his team at ICPA regarding our PR efforts.	Associate Chair	March 2002	(Initial meeting with John Smith 3/21/02.) Completed

RECOMMENDATION SUMMARY		*TASK*	*RESPONSIBLE PERSON*	*TARGETED DATE*	*STATUS*
15.	**RISK DEALING W/STUDENTS – Sexual Harassment:** We recommend the School refresh the policy periodically by circulating emails or hard copy brochures to the students.	The department Chair will annually in the fall distribute the policy on sexual harassment.	Chair	September 2002	In Progress
16.	**AREAS OF GENERAL RISK – Policies and Procedures:** We recommend that School management develop information systems documentation to support as a minimum: Local operating procedures, adaptation of Institute network usage policy, a local security policy, network diagrams, appropriate inventory of hardware and authorized software, and procedures for providing feedback to Computer Support Specialist personnel.	Computer Specialist will develop diagrams of Department Network. Faculty, Staff and students will be informed of GA Tech's network usage policy on a reoccurring basis.	Computer Specialist	January 2003	In Progress