INTERNAL CONTROL GUIDANCE: INFORMATION SYSTEMS

I. Strategy and Vision

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

- Loss of monetary resources
- Loss of proprietary data
- Loss of productivity
- Hardware damage
- Software corruption of proprietary systems
- Compromises of systems
- Expenditure of resources on equipment inadequate to support the business goals of the unit

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

- GAO/AIMD-10.1.13 Assessing Risk and Returns: A guide for evaluating federal Agencies' IT investment Decision Making
- GAO/AIMD-10.1.23 Information Technology Investment Management
- GAO/AIMD-94-115 Executive Guide to Improving Mission Performance through Strategic Information Management and Technology
- ISO 27001 Standard: Information Security Management - Specification With Guidance for Use
- The IT Infrastructure Library (ITIL): A cohesive set of best practices for IT service management. It is comprised of a series of ITIL Books and is intended to assist organizations in developing a quality IT framework.

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

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

Best Practices:

As an overall process:

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

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

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

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

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

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

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

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

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

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

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

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

Process:

EMPOWER THE PEOPLE RESPONSIBLE:

Strategic planning encompasses several areas of accountability: information systems, budget, technical, business, and vision. While management should designate a responsible party for each area of the strategic plan, management remains responsible for the overall strategic plan.

COMMUNICATE WITH EVERYONE IN THE UNIT:

In order to maintain a relevant strategic plan, feedback/input from technical members, users and business managers is a necessity. Management is encouraged to use direct face-to-face methods of communications such as staff meetings, brown bags, and targeted training programs. Management also has at its disposal several supporting methods for communications such as email, the internet, and electronic messaging.

USE A SYSTEMATIC APPROACH:

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

Related Issues:

Georgia Tech Strategic Plan

II. Operations / Administration

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

- Loss of Information resources
- Loss of proprietary data

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

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

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

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

Best Practices:

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

Process:

EMPOWER THE PEOPLE RESPONSIBLE:

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

COMMUNICATE WITH EVERYONE IN THE UNIT:

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

DISSEMINATE POLICIES AND PROCEDURES:

The Institute Computer and Network Usage Security Policy provide guidance based on an enterprise perspective. While this may fit some units, it is not focused enough for all. If your campus unit handles special types of data (or special systems), there is a need for procedures for handling that data. Dissemination of procedures through direct and indirect communication is paramount to the success of information systems administration within the unit.

Related Issues:

Review the Georgia Tech and other Data related Policies:
http://www.policylibrary.gatech.edu/computer-and-network-usage-and-security
http://www.policylibrary.gatech.edu/information-technology/data-access
http://legal.gatech.edu/topics
FERPA
HIPAA

III. Logical Security

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

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

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

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

http://www.policylibrary.gatech.edu/computer-and-network-usage-and-security

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

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

  Example: A good control uses a Georgia Tech assigned ID, such as used in logging onto PRISM, Banner or PeopleSoft. In other words, a user ID issued by competent authority based upon the users proven eligibility. A bad practice is to use a homemade or generically assigned user ID as in GTLAB1, or STUD001, STU002, etc.

- Authorization: Authorization controls enable specification and subsequent management of the allowed actions for a given system. Examples of good controls are those that incorporate strong password policies; such as forced expiration with a maximum password life less than 91 days, passwords that are not easily guessed and passwords that the meet the minimum criteria explained at

  http://www.policylibrary.gatech.edu/information-technology/passwords

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

Best Practices:

1. Maintain an active user awareness program that reinforces the concept that all users have security responsibilities.
2. Hold users responsible for basic security practices.
3. All operating systems must have logical security capabilities.

   Example: Windows 95 is not a securable system, whereas Windows 2000 and above, UNIX, MAC, and Linux systems allow for discreet network, individual file, and folder security.
4. Passwords should not be shared with others under any circumstance. Passwords should not be written or emailed.
5. All operating systems should be set up to enforce automatic password changes and implement "strong password" capacity.

6. Where possible a "layer security" concept should be in place by using individual user IDs, individual passwords and multi-layered security and firewalls.
7. Conduct a semi-annual risk self-assessment. Contact the Department of Internal Auditing.
8. Use automated tools to review your information security posture: i.e. Information Security Scanner (ISS), GFI LANGARD LAN scanner, NMAP, etc.
9. When in doubt seek assistance or advice from the professionals available at OIT or the Department of Internal Auditing.

Process:

EMPOWER THE PEOPLE RESPONSIBLE:

Establish routine reporting requirements on the status of the unit's security posture that will enable the computer support personnel to communicate security issues in a timely and objective manner to management.

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

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

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

COMMUNICATE WITH EVERYONE:

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

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

POLICIES AND PROCEDURES:

Ensure that your unit has reviewed the Institute's Computer and Network Usage Policy and Data Access Policy and has formally documented your local policy and procedures for authorization, authentication and encryption. Don't pay lip service to basic security requirements like user accounts and passwords.

- Strong passwords and password construction techniques can be found at: http://www.policylibrary.gatech.edu/information-technology/passwords
- Make sure all users are authorized by ensuring that the systems administrator is made aware of all personnel changes to the Unit.

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

Related Issues:

- Physical Security
- Training
- Documentation

IV. Physical & Environmental Security Controls

Description of Risk: If physical and environmental controls are not in place to ensure the proper conditions in which information systems should operate, systems may become unstable. If information systems assets are not properly identified and controlled, they may be misappropriated and/or damaged. This increases the risk that information systems resources could be unavailable and data may be compromised.

Criteria: Physical and environmental aspects are often one of the most overlooked areas of information technology operations. Heat, humidity, and inappropriate levels of dust in the area are a few examples of environmental factors that can wreak havoc on the Information Technology assets. To protect information systems assets, each campus unit must take into account environmental controls. There is no single standard for ensuring environmental protection, but a risk assessment can be used to point to vulnerable areas.

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

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

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

Environmental aspects are often one of the most overlooked areas of information technology operations. Heat, humidity, poor electrical support, and inappropriate levels of dust in the area are a few examples of environmental factors that can wreak havoc on the information technology

assets. To protect information systems assets each campus unit must take into account environmental controls.

Best Practices:

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

Process:

EMPOWER THE PEOPLE RESPONSIBLE:

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

COMMUNICATE WITH EVERYONE:

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

DISSEMINATE POLICIES AND PROCEDURES:

Management should ensure that the unit has a written policy that clearly delineates who is responsible for equipment, each area's security; and emergency procedures.

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

POLICIES AND PROCEDURES:

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

ENSURE ACCURACY OF INFORMATION:

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

Each piece of computer hardware should have manufacturer's recommendations for proper maintenance and environmental settings. Evaluation of physical location against the environmental recommendations made by the manufacturer should provide adequate protection during normal usage. Examples of bad situations that must be avoided are:

- Locating Critical resources in areas with inadequate ventilation or inappropriate humidity levels.
    - Example 1: A server located in a broom closet with a sprinkler head in it. Heat will build up quickly on large computers with high power requirements. Even a momentary failure of a sprinkler system will destroy electrical equipment.
    - Locating an Uninterruptible Power Supply (UPS) that supports critical resources next to a HVAC air intake vent. The increased airflow results in increased chance of dust, static buildup, and humidity level.
- Critical Resource that is properly located but not adequately monitored.
    - Servers often have redundant power supplies in case of failures. Redundant power supplies often have a conditioning cycle that should be performed every six months or so. Failure to condition the power supplies properly may result in a momentary power spike, or brownout, causing loss to critical resources.
    - A machine placed in direct sunlight may experience significant temperature gain over the surrounding area. Although the temperature of the room may be acceptable the machine may overheat.

USE A SYSTEMATIC APPROACH:

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

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

V. Data Stewardship Controls

Description of Risk: Data compromised or lost due to poor data stewardship may have adverse effects on business operations, competitiveness, and public relations. Monetary loss to individuals and the Institute may occur if the compromise is severe enough. It is the responsibility of Georgia Tech, through the chief data stewards, to implement procedures to effectively manage and provide necessary access to Institute data, while at the same time ensuring the confidentiality, integrity, availability, accountability, and auditability (CIAAA) of the information. Appropriate implementation of the policy will ensure Institute compliance with the Federal Trade Commission's Safeguards Rule under

- the Gramm-Leach-Bliley Act (GLBA), as well as the Family Educational Rights and Privacy Act (FERPA), and the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Criteria: Data is an important campus unit business asset. "Data stewardship," for the purpose of this section of this document, is defined as the prudent management of Georgia Tech's data. Georgia Tech's data is defined as:

- Data provided to external stakeholders (public and private organizations with which Georgia Tech conducts business such as other U.S. Department of Defense offices, Congress, other government agencies, laboratories, contractors, and the general public);
- Data provided to internal stakeholders (individual organizational components that comprise Georgia Tech); and
- Data that may be of a sensitive nature (budget, personnel, proprietary, credit card, reviewer, and procurement data).

Auditor's Overview: It is management's responsibility to ensure:

- The confidentiality, availability, and integrity of Institute, propriety, and personnel data held by the unit or accessed through the unit's information systems; and
- That credit card and other financial instruments are protected and credit card information meets the requirements of Institute polices (no unit should be processing and storing credit card information outside of the Institute's approved processing environment).

Best Practices: Maintain a policy that answers the following questions as they apply to your unit:

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

"How do we do all that?"

EMPOWER THE PEOPLE RESPONSIBLE

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

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

COMMUNICATE WITH EVERYONE IN THE UNIT

Post policies and procedures. Hold routine training.

DISSEMINATE POLICIES AND PROCEDURES

Write it down to prevent confusion.

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

are subject to the provisions of the Act related to the administrative, technical, and physical safeguarding of customer information.

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

VI. Training

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

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

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

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

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

Best Practices:

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

Process:

EMPOWER THE PEOPLE RESPONSIBLE:

Designate a training coordinator and ensure they know what their responsibilities are. As the needs, equipment, and personnel of the unit change ensure that the training plan is updated. Assign unit personnel to give input to their training requirements. The training plan should be reflected in the budget.

COMMUNICATE WITH EVERYONE IN THE UNIT:

Communication of the need and responsibility for continuing training in the area of technology is essential to success of the training plan. Ensure that staffs understand management's support of ongoing training and that feedback is received from unit personnel on training needs.

VII. Documentation

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

Key important factors are:

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

Documentation aids the development of new systems and maintenance of existing ones. Documentation will provide quintessential elements of success during any recovery operation.

Well-documented systems are protected against the risk of a single point of failure in human systems administration.

Description of Risk: Without proper documentation the following risks may be present:

- Users will need increased training because of the deficit of the documentation
- Lost productivity
- Increased errors in data entry
- Possible system breeches
- Software corruption of proprietary systems
- Compromises of systems
- High turnover rates
- Decreased system efficiency
- Increased operational costs

Criteria: Systems, configurations, proprietary user guides, and special software need to be documented because when they are actually needed it will most likely be a time with a demanding schedule. Documentation is subject to category "D" of the records retention series from the USG and Board of Regents. At a minimum, documentation should exist to fully support a restoration plan from zero operational state to a state of full capability.

The documentation should include adequate policies and procedures so that new personnel, being trained or otherwise, could operate the system in a manner that would support operations. Documentation should clearly outline the responsibilities of all managers, operators, administrators, and users.

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

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

Process:

EMPOWER THE PEOPLE RESPONSIBLE

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

COMMUNICATE WITH EVERYONE:

Make use of Information Systems:

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

USE A SYSTEMATIC APPROACH:

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

READ, WRITE & REVIEW:

From the ISO9000 series on quality systems:

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

Related Issues:

Business Continuity Planning

Software License Management

VIII. Equipment Maintenance

Description of Risk: Loss of critical resources can occur if equipment is not properly and timely maintained. Losses due to improper maintenance are similar to those that can occur during a disaster:

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

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

Criteria: Physical devices such as computers are susceptible to failure. Information systems and associated computers have been designed to work in a controlled environment. Proper

maintenance will extend the life, power, and capability of the system. Evaluations will be based upon manufacturer's recommendations and industry best practices.

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

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

Best Practices:

1. Develop a system of inspecting equipment to verify that maintenance procedures are adequate
2. Always review the contract specifications and warranties for maintenance-related requirements
3. The Computer Support Representative should work with the unit to schedule maintenance and hardware inspections on a regular basis
4. Develop a maintenance calendar and a maintenance log to record when maintenance has been conducted, by whom, and what was done
5. Ensure that systems users understand their responsibilities and role in equipment maintenance

Process:

IDENTIFY THE PEOPLE RESPONSIBLE:

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

POLICIES AND PROCEDURES:

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

USE A SYSTEMATIC APPROACH:

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

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

Related Issues:
Environmental Controls
Physical Security

IX. Business Continuity Planning

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

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

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

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

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

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

1. What happens if I have a server failure, what will be the most current backup I can restore to?
2. What happens if my Computer Support Specialist is unable to return to work for a period of time?
3. What happens if I am denied access to my workplace due to power outage, or other sudden impediment?

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

Process:

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

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

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

EMPOWER THE PEOPLE RESPONSIBLE:

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

COMMUNICATE WITH EVERYONE:

Put out reminders of what the unit's policy is via occasional email or bulletin board notices.

DISSEMINATE POLICIES AND PROCEDURES:

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

USE A SYSTEMATIC APPROACH:

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

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

See the following websites for additional plans, sample policies:

www.oit.gatech.edu
www.fema.gov
www.drj.com
www.nist.gov

X. Software Licensing

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

Criteria: The Georgia Tech Computer and Network Usage Security Policy contains guidance regarding licensing as follows:

- No software may be installed, copied, or used on Institute resources except as permitted by the owner of the software
- Software subject to licensing must be properly licensed, and all license provisions (installation, use, copying, number of simultaneous users, terms of license, etc.) must be strictly adhered to
- Users are prohibited from using, inspecting, copying, storing, and redistributing copyrighted computer programs and other material, in violation of copyright laws

Auditor's Overview: One of the most daunting conundrums for the educational environment is the monitoring and control over the installation of software.

- Is the operating system a secure operating system?
- Is there a software management system in place that details the authorized software, and a standard configuration for unit computers?

- Does the CSS/CSR have a spreadsheet or database that cross-references software licenses to specific computers?
- Are administrative controls limited to only those personnel authorized to install software?
- Are monitoring techniques in place to detect the un-authorized downloading or copying of installed software?
- Are routine inventories conducted of installed software?
- Can you show proof of purchase and license agreement for each piece of licensed software installed on any of your computers?
- Do you have the correct number of per-seat or server client licenses for the unit servers?

Best Practices:

1. Promulgate a unit policy on software management
2. A pro-active user education and training program that sets the standards for users to follow
3. Use a "secure" operating system that can be tailored to the users, and only allows specified personnel the ability to install software
4. The employment of automated license tracking software is highly recommended; this usually involves the installation of "agent software" that keeps an active inventory of installed software and changes to installed software
5. Have your purchasing department or purchasing officer maintain a file of software purchase orders and vouchers
6. Limit the authority of who can purchase software, especially with PCards

Process:

EMPOWER THE PEOPLE RESPONSIBLE:

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

COMMUNICATE WITH EVERYONE:

Make use of Information Systems:

- Use Web sites and Email to promulgate policies and procedures.
- Ensure accuracy and currency of information
- Ensure due diligence by staying current!

USE A SYSTEMATIC APPROACH:

Conduct routine inventories. Insist proper procedures are followed for software purchases.

Related Issues:

Backup and recovery

XI. Web Site Operation / Development

Description of Risk: The risk associated with web presences are vast, some of them are:

- Damage to reputation
- Monetary loss
- Theft of data
- Corruption of data
- Loss of needed information resources
- Loss of proprietary data
- Loss of productivity
- Hardware damage
- Software corruption of proprietary systems
- Compromises of systems
- Decreased system efficiency
- Increased operational costs

Criteria: There are several resources regarding website operations and development. They can be found at:

http://www.security.gatech.edu/ServerSecurity
http://www.oit.gatech.edu/service/webhosting/web-hosting
http://www.comm.gatech.edu/offerings/web.html
Georgia Tech Computer and Network Security Usage Policy

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

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

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

Best Practices:

1. Ensure the campus unit's local web presence is in tune with official policy
2. Host the web site on OIT's servers if at all possible
3. Keep all web servers patched
4. Use as few services on the primary web server as possible

5. Isolate vulnerable services such as FTP whenever possible
6. Use secure web protocols whenever possible

Process:

EMPOWER THE PEOPLE RESPONSIBLE

Ensure that there is a competent web administrator monitoring the logs and service of the web server. Ensure that that person has the appropriate level of skill and knowledge to take appropriate action when necessary.

ENSURE ACCURACY OF INFORMATION

Keep as current information as possible on the website. Old data presented as current has a discrediting effect.