IT - General Controls Questionnaire

Internal Control Questionnaire

Question	Yes	No	N/A	Remarks
G1. ACCESS CONTROLS				
Access controls are comprised of those policies and procedures that are designed to allow usage of data processing assets only in accordance with management's authorization. Protection of these assets consists of both physical and logical access controls that prevent or detect unauthorized use, damage, loss, or modifications. The data processing resources to be protected include the system software, application programs and tables, transaction detail and history files, databases, documentation, hardware, and tape or cartridge libraries. Access to these resources should be limited to those individuals authorized to process or maintain a particular system.				
PHYSICAL SECURITY				
1. Does the university maintain written procedures relating to controls over the physical security of the computer equipment?				
2. Is the physical location of the computer/server/storage/training rooms appropriate to ensure security?				
3. *Are physical access devices (i.e., card-key or combination lock systems) used to restrict entrance to the computer room?				
4. Obtain documentation listing all individuals with access to the computer room.				
a. Are only those with a legitimate need included?				
b. Are terminated or transferred employees' access codes cancelled in a timely manner?				
5. Does the university have any policies for temporary access by employees, visitors, or outside vendors? (e.g., are these individuals escorted during their activities, or are ID badges or sign-in logs used?)				

Question	Yes	No	N/A	Remarks
6. Does the university utilize monitoring software linked to the physical access device to electronically monitor computer room entrances?				
a. Are access reports generated?				
b. Are these reports reviewed by appropriate IT management?				
7. Does the university use plate glass or other techniques (e.g., surveillance cameras) to visually monitor computer room access?				
8. Does the university utilize procedures and devices to secure sensitive equipment and storage media from the risk of environmental damage, such as:				
a. Halon, CO2, or dry-piped water suppression systems?				
b. Hand held fire extinguishers?				
c. Smoke and heat sensors?				
d. Water detectors and humidity controls?				
e. Temperature controls and dedicated air conditioning units?				
f. An uninterruptible power supply (UPS), diesel or gas generators, or power generators?				
9. For any other sensitive areas, are access controls to these areas adequate? Examples of sensitive areas (besides the computer room) would include communications closets, any UPS equipment, and tape libraries.				
LOGICAL ACCESS				
10. Does the university maintain written policies or procedures related to the security controls over access to the system?				
11. *Does the university utilize various levels of security products (e.g., security software, application and database security)?				

Question	Yes	No	N/A	Remarks
12. *Determine the types of controls that are in place over the issuance, maintenance, and termination of passwords. Do such controls include:				
a. A security administrator designated to control password security?				
b. Informing employees of proper password security through training or signed security statements?				
c. Unique passwords?				
d. Passwords changed on a periodic basis?				
e. Passwords cancelled or access rights modified in a timely manner upon an employee's termination or transfer?				
13. *Are reports generated by the system's security software?				
a. Are these reports regularly reviewed by the security administrator?				
b. Are procedures in place to follow up on these reports?				
14. Is sensitive data protected by restricted access or other controls?				
15. If student data is maintained on unit computers, is security over the data sufficient to ensure compliance with the Family Educational Right to Privacy Act (FERPA)?				
G2. PROGRAM CHANGE CONTROLS				
Program change control is the process of the programmer making changes to computer programs based upon requests from users or due to general computer maintenance requirements. The change process involves authorization and approval procedures, audit trail of the requests, program testing, segregation of duties and documentation of the process.				

Question	Yes	No	N/A	Remarks
1. Does the university maintain written procedures for controlling program changes through IT management and programming personnel?				
2. *Do program change authorization forms or screens prepared by the user (usually called a Request for Services) include:				
a. Authorizations by user management before proposed program changes are made?				
b. Testing program changes?				
c. IT management and user personnel review and approval of testing methodology and test results?				
3. *Does the university use library control software or other controls to manage source programs and object programs, especially production programs?				
4. *Does the university have procedures for emergency program changes (or program files)?				
G3. BACKUP AND RECOVERY CONTROLS				
Backup and recovery controls are the provisions to provide reasonable assurance that an organization will be able to recover from loss or destruction of data processing facilities, hardware, software, or data. These continuation provisions include the retention of copies of data files and software, arrangements for access to backup hardware on short notice and tested recovery plans.				
1. *Are critical files and programs regularly copied to tapes or cartridges or other equivalent medium to establish a generation of files for audit trail purposes and removed to off-site storage to ensure availability in the event of a disaster?				
2. Is a periodic inventory taken to verify that the appropriate backup files are being maintained?				
3. Are controls in place at the off-site storage location to ensure that it is fireproof and secure?				

Question	Yes	No	N/A	Remarks
DISASTER RECOVERY PLAN 4. Does the university have a documented disaster recovery plan for processing critical jobs in the event of a major hardware or software failure?				
a. Has the disaster recovery plan been updated on a regular basis?				
b. Has the recovery plan been tested?				
5. Is the disaster recovery plan maintained off-site and updated when changes occur?				
6. Does the backup and recovery plan include the following:				
a. Personnel assigned to disaster teams with operating procedures and emergency phone numbers to reach them?				
b. Arrangements for a designated physical facility?				
c. A risk analysis identifying the critical applications, their exposures, and an assessment of the impact on the entity?				
d. Arrangements with vendors to support the needed hardware and software requirements?				
e. Forms or other control documents to use in case of a disaster?				
G4. SYSTEM DEVELOPMENT AND ACQUISITION CONTROLS				
Systems development is the process of creating new computerized applications in-house (i.e., within the organization). The development life cycle consists of several phases. Each phase has objectives, processes, products and reviews. The reviews provide a mechanism for determining at each phase whether user needs are being met and whether cost, control, and audit objectives are being achieved. Systems acquisition is the process of purchasing and implementing an				

Question	Yes	No	N/A	Remarks
application that has been developed by a third-party software vendor. The effective implementation of purchased applications also requires the entity to adopt a formal methodology to control the process. This methodology closely resembles that of in-house developed systems				
1. Interview IT management to determine whether any new financial applications were either: 1.) developed in-house or acquired from a vendor or 2.) are being planned or investigated during the current audit period.				
If no planning related to the development or acquisition of new financial systems was performed during the audit period, do not complete this control module.				
2. Did the university's procedures for developing new applications include:				
a. System requirements analysis?				
b. System specifications?				
c. Technical design?				
d. Technical procedure development?				
e. User procedure development?				
f. System and acceptance testing?				
g. Transition?				
3. *Were user personnel involved in new systems development (acquisition), particularly during design, development, testing, and conversion?				
4. *Were audit and security concerns considered during the initial analysis phase? (If university has an internal audit staff, were internal auditors involved in new systems development (acquisition)?)				

Question	Yes	No	N/A	Remarks
5. Did IT management adequately document:				
a. Systems documentation?				
b. Program documentation?				
c. Operations documentation?				
d. Users documentation?				
G5. COMPUTER OPERATIONS CONTROLS				
Computer operations controls are designed to ensure that systems continue to function consistently, as planned. They include controls over the use of the correct data, programs, and other resources, and the proper performance of this function by operators, particularly when a problem occurs.				
1. Does the university maintain general operational documentation relating to the following procedures for which the operations staff are responsible?				
a. System start-up procedures				
b. Backup assignments				
c. Emergency procedures				
d. System shutdown procedures				
e. Error message debugging instructions				
f. System and job status reporting instructions				
2. Does the university maintain application-specific operational instructions including:				

Question	Yes	No	N/A	Remarks
a. Definitions of input sources, input data, and data formats?				
b. Descriptions of restart procedures and checkpoints?				
c. Descriptions of data storage requirements?				
d. Types of console message instructions?				
e. Copies of system flowcharts?				
3. *Are operating logs maintained, retained and reviewed on an ongoing basis?				
4. Are workloads properly managed by using manual or automated processing schedules to ensure that all jobs are processed and that deadlines and priorities are considered?				
G6. DATABASE CONTROLS				
A database is a collection of related data organized in a manner intended to be accessed by multiple users for varied purposes. Database controls are designed to ensure that activities related to the security, integrity, accountability and recoverability of the database are controlled.				
1. Does the university have a Database Administrator (DBA)? Is the DBA responsible for managing the entity's databases, including the following:				
a. Design and implementation?				
b. Monitoring and availability?				
c. Integrity and security?				

Question	Yes	No	N/A	Remarks
2. *Are Database Management Systems (DBMS) security features used to protect data against unauthorized access or manipulation?				
3. *Are DBMS utilities and commands restricted to those responsible for the maintenance of the DBMS (usually a designated DBA)?				
4. *For change control procedures for the Data Dictionary and DBMS:				
a. Is proper authorization obtained prior to modification?				
b. Are modifications tested?				
c. Are modifications reviewed and approved?				
d. Are changes documented?				
5. Is the database and its data backed-up on a regular basis, and are backups secured off-site?				
G7. TELECOMMUNICATION CONTROLS				
Telecommunication controls relate to the risk and control considerations for the transmission media, hardware and software that compose a communication system, as well as the management of a communication system. ***Complete this section only if the university processes material financial activity using this technology.***				
1. Does the university have written telecommunication policies and procedures? Do policies and procedures include:				
a. Methodology to implement telecommunication projects (hardware and software)?				

Question	Yes	No	N/A	Remarks
b. Construction and software change management controls?				
c. Security controls?				
d. Problem/incident reporting?				
e. Contingency planning?				
2. *Has telecommunication software (VTAM) been defined to the access control software and is access restricted to only authorized users?				
3. Is communication equipment physically secured and adequately protected from environmental concerns?				
4. *Are data transmissions logged to provide for an audit trail and to provide the ability to recover all activity, which may have failed to be properly sent or received?				
5. *Are data transmission errors reported to management for problem analysis and corrective action?				
6. *Is there a process of data communications change management (e.g., changes in configuration)?				
7. Do requests for changes in the telecommunications configuration include:				
a. Proper authorization prior to the change?				
b. Testing of changes?				
c. Review and approval of changes?				

Question	Yes	No	N/A	Remarks
d. Documentation of changes?				
8. Are there recovery procedures for a failure of data communications equipment or software?				
9. Do the back-up and recovery procedures include:				
a. Back-up copies of communications software?				
b. Alternate line/carrier facilities (public or private)?				
c. Multiple paths to critical sites on the network?				
d. Responsive reconfiguration procedures?				
G8. NETWORK CONTROLS				
Network controls address the threats and risks to sensitive and critical data that are accessed and transmitted through networks. Network controls ensure proper security performance and reliability of all network components. ***Complete this section only if the university processes material financial activity using this technology.***				
1. Do the LAN administrator's responsibilities include support for:				
a. User training?				
b. Policies and procedures?				
c. Security?				

Question	Yes	No	N/A	Remarks
2. Is the physical security adequate for the:				
a. File server?				
b. Cabling?				
c. Modems?				
d. Any external devices?				
3. *Do individual users have unique identification on the LAN? (e.g., user sign-on, password)				
4. *Are there methods to prevent unauthorized access by other groups into individual files and department-shared files?				
5. *Are there procedures for limiting access to LAN and network operating software?				
6. *Are there procedures for obtaining and securing modem dial-up access to the network?				
a. Confidential modem telephone numbers				
b. Change modem telephone numbers periodically				
c. Automatic “call back” system				
d. Modem disconnect policy				

Question	Yes	No	N/A	Remarks
7. If the LAN file server logs network activity, is this information periodically reviewed by the LAN administrator?				
8. Does the university adequately backup files and software? (Consider its location, security, and that the proper files are being retained.)				
9. Are there procedures to prevent and detect computer viruses, including:				
a. Anti-virus or virus-detection software?				
b. Guidelines on using shareware, bulletin boards, personal diskettes/CD/jump drives/ and other data medium?				
c. Awareness training on computer viruses?				
10. *Are there procedures to ensure compliance with the provisions of software licenses?				
G9. PERSONAL COMPUTER AND END-USER COMPUTING (EUC) CONTROLS				
The term personal computer, or PC, refers to a small computer equipped with all the system, utility, and application software, and the input/output devices and other peripherals that are needed to perform one or more tasks. End-user computing (EUC) is any development, programming, or other activity where the end-users create or maintain their own systems or applications, usually on their own personal computers. These systems function outside the traditional information systems controls and, therefore, need close scrutiny. EUC controls at the organizational level would include strategic planning by management, policies and procedures regarding traditional general control activities, and technical support and training. At the organizational level the auditor would typically interview IT management. ***Complete this section only if the university processes material financial activity using this technology.***				

Question	Yes	No	N/A	Remarks
PERSONAL COMPUTERS				
1. *Does the university maintain written policies and procedures relating to:				
a. PC security (including virus protection)?				
b. User-developed, commercial, or shareware software?				
c. Maintaining PC software?				
d. Backup and recovery?				
2. Does the university provide physical security over PCs by using such controls as:				
a. Locked doors?				
b. Cables?				
c. Anchor pads?				
d. Alarms?				
e. Keyboard locks?				
3. Does control over storage media include:				

Question	Yes	No	N/A	Remarks
a. Using write-protecting and read-only properties				
b. Using secured storage?				
4. *Determine whether access control software is used. If not, what other controls prevent misuse of critical data and applications? If used, are the security features of the package being utilized for:				
a. Passwords?				
b. Directory locking/restricting?				
c. Restricted access to operating system command prompts?				
d. Boot protection?				
5. Is appropriate hardware backup available?				
6. Are duplicate copies of PC software and documentation maintained off-location?				
7. Are users receiving adequate technical support and training?				
8. Is the use of external modems restricted?				
9. Is the use of remote access software restricted?				

Question	Yes	No	N/A	Remarks
END-USER COMPUTING (EUC)				
1. For critical PC applications, is there documentation describing data, programs, hardware, and system requirements?				
2. Is a disciplined approach taken in acquiring or developing new applications in an EUC environment? Do procedures include:				
a. Cost/benefit analysis?				
b. Design?				
c. Testing?				
d. Controls?				
3. *Are there procedures for controlling end-user changes to applications? Are the following conditions performed:				
a. Changes authorized by user management?				
b. Changes tested?				
c. Changes identified to show an audit trail?				
d. Documentation modified to reflect any changes?				
4. If upload/download PC software is available, do procedures require the following:				

Question	Yes	No	N/A	Remarks
a. Authorization and approvals?				
b. Virus detection/prevention?				
G10. INTERNET & ELECTRONIC COMMERCE CONTROLS				
The Internet is an enormous system of world-wide linked computer networks that facilities data communication services such as remote login, electronic mail, the World Wide Web and file transfer. Electronic commerce (e-commerce) on the Internet generally includes the electronic exchange of payments, invoices, orders and other documents. The security exposures of the Internet and the risks of electronic transactions require control techniques that ensure data is transmitted, translated, and passed to financial systems in a secure, accurate manner. ***Complete this section only if the university processes material financial activity using this technology.***				
INTERNET				
1. Does the university maintain written policies or procedures related to the security controls over access to the Internet, use of Internet resources (e.g., electronic mail), etc.? If the university maintains a Web site, then continue with Step 2, otherwise continue with Electronic Commerce section.				
2. Does management provide guidance for the development and maintenance of a Web site?				
3. *Does the university utilize various levels of security to control activity on the Web site and to prohibit access to the host computer from the site (e.g. firewall)?				
4. Are these policies and procedures requiring Web site review, approval and testing by an independent person?				

Question	Yes	No	N/A	Remarks
5. *Are updates to the Web site independently reviewed, approved and tested?				
6. Are the contents of the Web site backed-up to ensure an orderly recovery if the site is corrupted?				
ELECTRONIC COMMERCE				
If the university conducts financial transactions on the Internet, then continue with Step 1, otherwise skip this section.				
1. Does the university have a methodology for developing an electronic commerce application to conduct internet business?				
2. *Does the university utilize various levels of security to control access to sensitive information (e.g., encryption)?				
3. *Is transaction approval adequately controlled, preferably using electronic signatures?				
4. *Are there controls in place to ensure the accuracy, completeness, and timeliness of transactions?				
5. Are there guidelines established for the retention of data?				
6. Does the university have alternative processing procedures to rely on in case of processing disruptions?				
7. *Does the university have trading partner agreements? If so, review for the following provisions:				
a. Error detection and correction				
b. Security breaches				
c. Processing disruptions				