ENTITY 2017 ICQs

June 30, 2017 **IT**

QUESTION	YES	NO	N/A	REMARKS
OBJECTIVE: To obtain knowledge about specific information system policies and procedures management has established to provide reasonable assurance specific entity objectives are achieved. The objectives include:				
• **Proper authorization of transactions and activities related to information technology.**				
• **Segregation of duties in functions related to information technology.**				
• **Design and use of adequate IT documents and records.**				
• **Adequate safeguards over access to and use of the information system, assets and records.**				
• **Independent checks on performance of IT functions.**				
Accounting System				
A. Does the entity use a computer system to prepare its financial information?				
B. Are all funds, classes of transactions and/or account balances included in this system? If not, identify additional systems.				
C. Is a computer log maintained to determine who recorded a transaction, based on an employee's login name? (A computer log could be the identification of the employee who recorded a transaction based on their login name or it may be for a group of transactions. This information should be attached to the transaction in the data file.)				
D. Are all source documents numbered with a unique number when printed by the computer system?				
E. Are source documents, including error corrections, completed and signed or initialed by the preparer before being entered in the computer system?				
F. Are adequate procedures in place to trace and correct input errors?				
G. Are corrections identified and recorded in such a manner that duplicate correction will not occur?				
H. If operating or financial reporting personnel rely on PC software reports generated by end users through the use of spreadsheets (for example, Excel, Lotus 1-2-3 and Quattro), are there procedures to ensure such reports are accurate?				

ENTITY 2017 ICQs

June 30, 2017 **IT**

QUESTION	**YES**	**NO**	**N/A**	**REMARKS**
Computer Systems				
A. Applicable Computer Systems				
1. Are computer systems being used by the entity for the following transaction cycles? Please document if the transaction cycle uses a computer (Yes) or manual (No) and, if a computer is used, mark "M" if mainframe, "S" if server based system (LAN/WAN) or "PC" for personal computer. Also, document what computer software is used for each of the following:				
• Cash				
• Investments				
• Inventories				
• Capital Assets				
• Long-term debt				
• Receipts/Revenues/Receivables				
• Taxes and Special Assessments				
• Disbursements/Expenditures/Payables				
• Payroll				
• Transfers				
• Budgets				
• Working Trial Balances and Adjusting Journal Entries				
• Financial Reporting				
• Other (specify)				
B. Segregation of Duties				
1. Do users control who can perform various computer system functions, such as data entry, error correction or on-line edit and update?				
2. Determine/verify access to programs, and functions within programs, is limited to those who have a legitimate need. Obtain a user profile report which lists all users, their user ID's and any software applications to which they have access.				
3. Are user profiles reviewed periodically?				
4. Are background checks done for System Administrators? Background checks could involve contacting state or federal authorities to find out if a person has a criminal record.				

QUESTION	**YES**	**NO**	**N/A**	**REMARKS**
5. If the entity makes Electronic Funds Transfers (EFTs), are the personal bank account numbers of the employee making the EFTs restricted? (The System Administrator would set the entity's computer software to restrict the entry of the personal bank account numbers of the employee making the EFTs.)				
6. If the entity utilizes an Information Technology (IT) department with programmers developing software for the entity, is there a written policy the software developed by the programmers is the property of the entity?				
7. If the entity utilizes an IT department, are the following functions segregated WITHIN the IT department when an IT programmer would be writing the software programming:				
a. System design?				
b. Application programming?				
c. Systems programming (operating system/utilities)?				
d. Quality assurance/testing?				
e. Approval of changes?				
f. Movement of changes into production?				
g. Computer operations/data input?				
8. If the entity utilizes an IT department, are the following functions performed only OUTSIDE the IT department:				
a. Initiation of transactions?				
b. Authorization of transactions?				
c. Preparation of source documents?				
d. Custody of assets?				
e. Changes to master files?				
f. Error correction?				
9. If the entity purchases software from a vendor, are the following functions performed only by the entity (no IT department):				
a. Placing programs into production (loading the programs into the entity's computer system)?				
b. Initiation of transactions?				
c. Authorization of transactions?				
d. Preparation of source documents?				
e. Custody of assets?				
f. Changes to master files?				
g. Error correction?				

QUESTION	YES	NO	N/A	REMARKS
C. Procedural Controls				
1. Are employees trained to challenge an unknown person using computer terminals or PC's?				
2. Is there a time out and/or log off function which will protect a terminal if left unattended? If no, does the entity have a written policy for logging off unattended terminals?				
3. If the above procedure is not done, do entity policies require the use of screen saver passwords to protect a terminal if left unattended?				
4. Determine the procedures for computer logins and passwords as follows:				
a. Does a login name and a password uniquely identify users when they sign on to the system (e.g., no group users IDs)?				
b. Are the procedures for setting up new user/login ID names restricted to one person? Document who can authorize access. (System Administrator)				
c. Are employee login identification numbers (IDs) removed immediately when their employment terminates?				
d. Is login access given to consultants removed when their work is completed?				
e. When an employee's job duties change, is the login access changed so they have access only to the information needed for their current job duties?				
f. Are policies and procedures established to ensure when passwords need resetting:				
• Only an authorized employee can request a password be reset?				
• An employee cannot request another employee's password be reset and then gain access?				
g. Does the entity have a written policy instructing employees on their responsibilities to maintain password privacy and confidentiality, including sharing their password with the employee's supervisor?				
h. Are employee passwords not shared with others, including the employee's supervisor?				
i. Are passwords changed at least every 60 to 90 days?				
j. Does the software force the user to change their password after every 60 to 90 days? (Recommended the software force the user to change their password.)				

QUESTION	YES	NO	N/A	REMARKS
k. Is the password length set at a minimum of at least 8 characters? (The more characters in a password the more difficult it is for someone else to determine the password. Strong passwords will make it more difficult for password cracking tools to break a password.)				
l. Are the characters allowed to be used in a password set to all characters on the keyboard? (The System Administrator would set the characters that could be used for a password.)				
m. Are generic passwords used for new employees required to be changed? (Recommend to be changed in at least 30 days.)				
n. Is password history used to prevent someone from using the same password?				
o. If an employee incorrectly enters their password three times in a row, does the computer system deny them access to the computer system until reset by the System Administrator?				
5. System backup procedures:				
a. Are backups created and saved for each of the following: (A common practice would be to have seven days of backup tapes, which would be rotated and reused. The oldest tape would be used to backup today's activities. At the end of each week, another series of tapes would backup each week (four tapes for the month) until the month end backup. There should be monthly backups for the last twelve months. Those tapes would be rotated with the next fiscal year with the oldest tape used for the current month end backup. The fiscal year backup should also be saved.)				
• Daily?				
• Weekly?				
• Monthly?				
• Yearly?				
b. Are all backup tapes stored in a secured off-site location? Recommend backup tapes be stored in a fireproof vault or safe.				
c. Are all backup tapes stored off-site daily?				
d. Are copies of network and financial software stored off-site as well?				
e. Are critical files which reside on a LAN (Local Area Network) backed up?				

ENTITY 2017 ICQs

June 30, 2017 **IT**

QUESTION	YES	NO	N/A	REMARKS
f. Are critical files which reside on a stand-alone PC (not on a LAN) required to be backed up to the LAN?				
6. Is the computer system capable of remote data communications (i.e. dial-in-remote access/VPN (Virtual Private Network))? If yes, are there appropriate controls?				
D. Physical Access				
1. Do hardware controls include:				
a. Suitable physical environment, as follows:				
• Temperature and humidity control?				
• Sufficient power?				
• UPS (Uninterrupted Power Supply)?				
• Surge protection?				
• Protection from water sources (potential water pipe breaks)?				
b. Does the entity have adequate fire protection, as follows:				
• Fire extinguishers?				
• Fire alarms?				
• Smoke detectors?				
• Halon gas or other non-water based fire suppression system?				
• Water sensor devices?				
c. Are annual inspections of fire extinguishers performed?				
d. If power is interrupted, does the entity have an alternative power source?				
2. Are there policies and procedures which restrict physical access to computer facilities to authorized personnel?				
3. Are PC systems with hard disks in areas where they are accessible to the public controlled/monitored when left unattended?				
4. Are terminals for public use restricted to read access only?				
5. Is there adequate security over computer output to ensure only intended users of data are receiving data? (This would include terminals restricted for public use.)				
6. Have procedures been established to ensure proper disposal of sensitive media (e.g. shredding of printouts, complete removal of data and software from hard disks, diskettes and magnetic tapes)?				

QUESTION	YES	NO	N/A	REMARKS
E. If the entity utilizes an IT department to write its IN-HOUSE software, are these procedures established for Systems Development and Software Program Change Control:				
1. Is there a uniform systems development policy, including acceptance testing, that is followed for all new programs?				
2. Is a uniform systems change policy, including acceptance testing, followed for all changes to existing programs?				
3. Are procedures in place to control “emergency fixes” to a production program?				
4. Are there controls ensuring superseded programs are segregated from the current version and removed from the production library?				
5. Do IT policies and procedures require up-to-date documentation for each application, as follows:				
a. System flowchart?				
b. Record and report layouts?				
c. Program source code?				
d. Operator and user instructions?				
e. Program change sheets?				
6. Do systems development policies require the active participation of users in important phases of development or change, including final approval?				
F. If the entity purchases software from a VENDOR, are procedures established for acceptance of software:				
1. Is a uniform policy, including acceptance testing, followed for all new/upgraded programs?				
2. Do IT policies and procedures require the following, up-to-date documentation for each application:				
a. Record and report layouts?				
b. Operator and user instructions?				
3. Do systems development policies require the active participation of users in important phases of acquisition, including final approval regarding selection of vendor software?				
G. Personal Computers (PC’s) and Local Area Networks (LAN’s)				
1. Anti-Virus Programs:				
a. Is the entity using an anti-virus program on its PC’s?				
b. Does the entity have a policy and procedure for employees to run the anti-virus program on a regular basis?				

QUESTION	YES	NO	N/A	REMARKS
c. Are regular updates obtained from the software vendor for new virus definitions? Anti-virus software needs to be updated to identify new viruses. Updates can usually be obtained from the software vendor's Internet web site.				
d. How frequently are virus definitions obtained? (Ideally, virus definitions should be updated on a live basis.)				
e. Are employees instructed to scan diskettes and upgrade diskettes for programs before loading on to the system?				
f. Are employees instructed to scan downloaded files from bulletin boards and the Internet before opening or uncompressing (unzipping) the files? Certain files may be compressed (zipped) so they download faster.				
g. Does the entity maintain a security awareness program, including precautions that should be taken with e-mail?				
2. Are there policies to ensure software not licensed to the entity is not installed on a PC? (e.g. software installed and owned by an employee)				
3. Is the entity monitoring software-licensing requirements to determine if it is in compliance? Entities should read and understand the software licensing requirements for purchased software so they are not illegally copying software.				
4. If the entity has an Internet service provider:				
a. Is there a written policy on the usage of the Internet?				
b. Is the anti-virus program run for downloaded files?				
5. If the entity has an Internet web page:				
a. Does the entity or the Internet service provider have a firewall established? A firewall could prevent a person who accesses the web page from gaining access to the entity's computer system.				
b. If the entity is doing electronic business through its web page, have adequate safeguards been established?				
H. Contingency Planning (Disaster Recovery Controls)				
1. Is there a written disaster recovery plan?				
2. Has the plan been approved by management?				
3. Determine if the disaster recovery plan includes the following:				
a. Identification of critical applications.				
b. Identification of staff responsibilities.				
c. Identification of steps for recovery of the system.				

QUESTION	YES	NO	N/A	REMARKS
d. Identification of computer equipment needed for temporary processing.				
e. Identification of business location(s) which could be used to process critical applications in the event of an emergency. Is there a written agreement?				
f. Requirement a copy of the disaster recovery plan be kept off site.				
g. Requirement to keep system backups current and off site.				
h. Inventory of all hardware and components (e.g.: make, model numbers, serial numbers, etc.).				
i. Inventory of all software applications (e.g.: operating system and software applications, release versions and vendor names).				
j. Requirement copies of all user documentation and policy and procedures manuals be located off site.				
k. Requirement extra stocks of paper supplies, such as checks, warrants, purchase orders, etc., be located off site.				
l. A determination of whether the disaster recovery plan is adequately tested.				
m. Has a copy been provided to all appropriate personnel?				
4. Are all employees trained for appropriate responses to emergency situations?				
5. Does the record retention policy require records be retained for at least as long as they are needed to meet operational and legal requirements?				