MENTAL HEALTH REGION 2017 Audit Programs

June 30, 2017

INTERNAL CONTROL QUESTIONNAIRE
INFORMATION TECHNOLOGY

QUESTION	YES	NO	N/A	REMARKS
OBJECTIVE: To obtain knowledge about specific computer system policies and procedures management has established to provide reasonable assurance specific Region objectives are achieved. The objectives include:				
A. Proper authorization of transactions and activities related to the IT systems.				
B. Segregation of duties in functions related to the IT systems.				
C. Design and use of adequate IT documents and records.				
D. Adequate safeguards over access to and use of the IT systems, assets and records.				
E. Independent checks on performance of IT functions.				
Accounting System				
A. Does the Region use a computer system to prepare its financial information?				
B. Are all funds, classes of transactions and/or account balances included on 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 identifies the employee who recorded a transaction based on their login name.)				
D. Are source documents, including error corrections, completed and signed or initialed by the preparer before they are entered in the computer?				
E. Are adequate procedures in place to trace and correct input errors?				
F. Are adequate procedures in place to reconcile fiscal agent (County) financial activity to amounts recorded to the Community Services Network (CSN)?				
G. Are corrections identified and recorded in such a manner 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?				

MENTAL HEALTH REGION 2017 Audit Programs

June 30, 2017

INTERNAL CONTROL QUESTIONNAIRE
INFORMATION TECHNOLOGY

QUESTION	YES	NO	N/A	REMARKS
Computer Systems				
A. Applicable Computer Systems				
1. Are computer systems being used by the Region for the following transaction cycles? Document if the transaction cycle uses a computer (Yes) or manual (No). If a computer is used, mark "M" if mainframe application, "S" if server based system (LAN/WAN) or "PC" for personal computer application. Also, document the software program used for each of the following:				
• Cash				
• Investments				
• Inventories				
• Capital Assets				
• Long Term Liabilities/Debt				
• Receipts/Revenues/Receivables				
• Disbursements/Expenditures/Payables				
• Payroll				
• Transfers				
• Budgets				
• Working Trial Balances and Adjusting Journal Entries				
• Financial Reporting				
• Other (specify)				
B. Segregation of Duties				
1. Do authorized personnel control who can perform various computer system functions, such as data entry, error correction or on-line edit and update?				
2. Does the Region limit access to programs and functions within programs to those who have a legitimate need?				
3. Are user access rights reviewed periodically?				
4. Are background checks done for new employees? Background checks could involve contacting state authorities to find out if a person has a criminal record.				

MENTAL HEALTH REGION 2017 Audit Programs

June 30, 2017

INTERNAL CONTROL QUESTIONNAIRE
INFORMATION TECHNOLOGY

QUESTION	YES	NO	N/A	REMARKS
5. If the Region makes Electronic Funds Transfers (EFTs), are the personal bank account numbers of the employee making the EFTs restricted? (The System Administrator would set the Region's computer software to restrict the entry of the personal bank account numbers of the employee making the EFTs.)				
6. If the Region utilizes internal Information Technology (IT) programmers to develop software, is there a written policy the software developed by the programmers is the property of the Region?				
7. If the Region utilizes an IT department which develops software, are the following functions segregated WITHIN the IT department:				
a. Programming? (Computer programmers and those performing programming duties.)				
b. Computer operations/data input?				
8. If the Region 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 Region purchases software from a vendor, are the following functions performed only by the Region (no IT department):				
a. Placing programs into production (loading the programs into the Region's computer system)?				
b. Initiation of transactions?				
c. Preparation of source documents?				
d. Changes to master files?				
e. Error correction?				
C. Procedural Controls				
1. Are employees trained to challenge an unknown person using computer terminals or PCs?				
2. Is there a time out and/or log off function which will protect a terminal or PC if left unattended? If no, does the Region have a written policy for logging off unattended terminals or PCs?				

QUESTION	YES	NO	N/A	REMARKS
3. If the above procedure is not done, does the Region use a screen saver password which will protect a terminal or PC if left unattended?				
4. Are the computer terminals or PCs always logged off before being left unattended for extended periods of time during work hours?				
5. Do procedures exist to keep the computer terminal or PC from being left logged on overnight or over the weekend? (Such as timed automatic log off.)				
6. 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/Security Administrator)				
c. Are employee login identification numbers (IDs) removed immediately when their employment terminates?				
d. Do consultants have login access to the computer system? If so, is their access removed when their work is completed?				
e. Are users restricted to those programs and functions within programs for which they have legitimate needs?				
f. 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?				
g. 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?				
h. Does the Region have a written policy instructing employees on their responsibilities to maintain password privacy and confidentiality, including not sharing their password?				
i. Are passwords changed every 60 to 90 days, or sooner?				
j. Does the software require the user to change their password after every 60 to 90 days? (Recommended the software require the user to change their password.)				

MENTAL HEALTH REGION 2017 Audit Programs

June 30, 2017

INTERNAL CONTROL QUESTIONNAIRE
INFORMATION TECHNOLOGY

QUESTION	YES	NO	N/A	REMARKS
k. Is the password length set at a minimum of at least 6 characters? (Preferably 8 or more. The more characters in a password, the more difficult it is for someone to determine the password.)				
l. Are the characters allowed to be used in a password set to all characters on the keyboard? (The System/Security 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 after first use.)				
n. Is password history used to prevent someone from using the same password repeatedly?				
o. If an employee incorrectly enters their password three times in a row (within a 24-hour time period), does the computer system deny the employee access to the computer system for 24 hours?				
7. System backup procedures for mainframe:				
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 on a daily basis in a secured off-site location? Recommend backup tapes be stored in a fireproof vault or safe.				
c. Is a complete system backup done at month end? (Backup would include all transactions plus programs.)				
d. Is a complete system backup done at fiscal year end? (Backup would include all transactions plus programs.)				

QUESTION	YES	NO	N/A	REMARKS
e. Are critical files which reside on a LAN (Local Area Network) backed up using the same procedures as the main frame computer?				
f. Are critical files which reside on a stand-alone PC (not on a LAN) backed up using the same procedures as the main frame computer?				
8. Is the computer system capable of remote data communications (i.e. dial-in-remote access)? If yes, are there appropriate controls?				
D. Data Center Protection				
1. Do hardware controls include:				
a. Suitable physical environment, as follows:				
• Temperature and humidity control?				
• Sufficient power (Voltage Regulator)?				
• UPS (Uninterrupted Power Supply)?				
• Surge Protection?				
b. Does the Region have adequate fire protection as follows:				
• Fire extinguishers?				
• Fire alarms?				
• Smoke detectors?				
• Water sprinklers or Halon gas?				
• Water sensor devices?				
c. Are annual inspections of fire extinguishers being performed?				
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)?				

MENTAL HEALTH REGION 2017 Audit Programs

June 30, 2017

INTERNAL CONTROL QUESTIONNAIRE
INFORMATION TECHNOLOGY

QUESTION	YES	NO	N/A	REMARKS
E. If the Region utilizes an IT department to develop its IN-HOUSE software, are these procedures established for Systems Development and Software Program Change Control:				
1. Is a uniform systems development policy (including acceptance testing) 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 "quick 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 the following, up-to-date documentation for each application:				
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 Region purchases software from a VENDOR:				
1. Is a uniform policy (including acceptance testing) 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 "quick 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 systems development policies require the active participation of users in important phases of development or change, including final approval?				
6. Is a user manual available to describe the operation of the software?				

QUESTION	YES	NO	N/A	REMARKS
G. Personal Computers (PCs) and Local Area Networks (LANs)				
1. Anti-Virus Programs:				
a. Is the Region using an anti-virus program?				
b. Does the Region have a policy and procedure for employees to run the anti-virus program on a regular basis?				
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. Document how often virus definitions are obtained. (Ideally, virus definitions should be updated on a live basis.)				
d. Are there policies and procedures to scan media (disk, tape, file from internet) or upgrade programs before loading on to the system?				
e. Are there policies and procedures for employees 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.				
2. Are there policies to ensure software not licensed to the Region is not installed on a PC? If employee owned software is installed on the Region's computer, the Region may not be in compliance with copyright laws.				
3. Is the Region monitoring software-licensing requirements to determine if they are in compliance? The Region should read and understand the software licensing requirements for purchased software so they are not illegally copying software. The Software Publishers Association (SPA) monitors the illegal copying of software. The internet site is "www.spa.org".				
4. If the Region has an internet service provider, is there a written policy on the usage of the internet?				
5. If the Region has an internet web page:				
a. Does the Region or the internet service provider have a firewall established? A firewall could prevent a person who accesses the web page from making changes to the Region's computer system.				
b. If the Region is doing electronic business through its web page, are adequate safeguards established?				
H. Contingency Planning (Disaster Recovery Controls)				

MENTAL HEALTH REGION 2017 Audit Programs

June 30, 2017

INTERNAL CONTROL QUESTIONNAIRE
INFORMATION TECHNOLOGY

QUESTION	YES	NO	N/A	REMARKS
1. Is there a written disaster recovery plan?				
2. 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.				
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 is 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. A determination of whether the disaster recovery plan is adequately tested.				
3. Are all employees trained for appropriate responses to emergency situations?				
4. Have suppliers provided written confirmation they can replace hardware and supplies fast enough for the continued operation of the Region?				
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?				