CHAPTER 2

COMPUTER SYSTEMS

The following is a general outline of steps to follow when contemplating the purchase of data processing hardware and/or software. The State Board of Accounts has an Information Technology Services Division (ITS) available to assist in evaluating ITS requirements.

Basic Questions.

1. Is this purchase cost effective?
2. Are sufficient funds available to purchase desired hardware and software?
3. What applications are needed? Payroll? Financial and Appropriation Ledger? Accounts Payable?
4. What is the current and future volume of transactions to be processed per application?
5. Are qualified personnel available to operate the new system? How will they be trained?
6. How will software be maintained?
7. Can the vendor provide a list of users as references?
8. Where is hardware/software maintenance staff located?
9. What services are provided by vendor when system is down? How long before these services are available?
10. What is the estimated maintenance costs?
11. What is the cost to upgrade the system in the future?
12. If the source code is not purchased, the vendor must allow access to the source code for audit purposes by representatives of the State Board of Accounts.

Software.

1. Should provide extensive editing of data and change capability upon input and before a transaction is posted to an account, but no ability to change data after it is posted. If an error is discovered after the transaction is posted, a separate correcting transaction must be made.
2. Capable of providing hard copy of entire file or of selected screens.

3. A detailed transaction history (similar to a manually posted ledger page) should be maintained supporting each account. We would generally recommend a twelve month history. However, in small systems this may not be cost effective due to limited storage and require the use of a hard copy listing. Each transaction should be identified with the individual processing the transaction as well as the date of transaction.

4. Copyright restrictions and documentation of all programs should be reviewed before purchase.

5. If purchased separately, software must be compatible with hardware.

Hardware.

1. If purchased separately, hardware must be compatible with software.

2. Should have expansion capability to meet possible additional applications and future growth.

3. Review vendor service agreements carefully for cost and completeness.

Steps to Take Prior to Bidding.

1. Communicate with all potential in-house users to ensure that their demands on the system are fully understood.

2. Be sure record requirements in ITS environment are the same as those of the manual accounting system prescribed by the State Board of Accounts.

3. Observe hardware and software in operation at other units within the State and discuss with their users possible problems and/or suggestions, particularly service and maintenance.

Other Requirements.

1. Provisions must be made to "back-up" records in case originals are destroyed. Store "backups" off site or in fire proof vault. In addition, a disaster recovery plan must be developed and tested when the system is installed.

2. Review temperature, humidity and dust control requirements at computer location.

3. Review insurance coverage for hardware, software and file reconstruction.

4. Appropriate procedures should be used in implementing the new system. For example, control totals during conversion of data and a parallel processing period.

Possible Applications

The following is a list of possible applications with generalized minimum requirements.

Basically, output requirements in an ITS environment are the same as the records of the manual accounting system prescribed by the State Board of Accounts.

Payroll.

1. Properly authorized, edited and extended before input.
2. Record kept by individual.
3. Year to date totals available.
4. Generate monthly and quarterly reports.
5. Totals by department.
6. Overtime kept separately.
7. Hard copy of each payroll.
8. Generate annual reports - W-2's, WH-2's, 1099's, etc.

Purchase Orders.

1. Properly authorized, edited and extended before input.
2. Reduce purchase order balance when claim paid.
3. Adjust for partial paid claim.
4. Adjust for change in purchase order.
5. Update appropriation ledger for encumbrances and payments.
6. Update vendor record if applicable.

INTERNAL CONTROL REQUIREMENTS FOR ACCOUNTING SYSTEMS
INFORMATION TECHNOLOGY PROCESSING CONTROLS

In accordance with Statement on Auditing Standards Number 78, the Board of Accounts will review all computers that process accounting data. The scope of the review will be based on the following criteria: total dollars processed by the computer system, the materiality of those dollars to the unit's financial statements, the complexity of the processing, the availability of alternate sources for audit information, and the criticality of non-financial information processed. The ITS controls reviewed will be based primarily on the Control Objectives for Information and Related Technology and other publications of the Information System Audit and Control Association. Additional sources of information used in Board of Accounts Information Technology Services (ITS) reviews include but are not limited to publications of the AICPA, the Internal Auditor's Association, the General Accounting Office, the Department of Defense, the National Computer Security Association, and hardware and software vendors.

Governmental units should have internal controls in effect which provide reasonable assurance regarding the reliability of financial information and records, effectiveness and efficiency of operations, proper execution of managements' objectives, and compliance with laws and regulations. Among other things, segregation of duties, safeguarding controls over cash and all other assets and all forms of information processing are necessary for proper internal control.

The following requirements have been established for all computer systems processing accounting information.

Disaster Recovery

A written Disaster Recovery Plan is required to ensure that critical accounting information will be processed in the event of interruption of computer processing capability. The plan must be updated and tested annually or when significant modifications to computer hardware, software or application systems occur. One copy of the Plan must be retained off site.

Back Up Processing

All computer application programs and operating system software must be backed up on a periodic basis and after modification. Accounting information must be backed up on a periodic basis sufficient to allow restoration of the information in a timely manner. Periodically the back up media must be tested to assure restoration will occur accurately. One copy of the back up information must be retained off site. A log of back-ups and their contents should be maintained to assist in the timely restoration of information.

Physical Security

The computer system and the associated telecommunications equipment must be adequately protected from environmental damage including, but not limited to, fire, water, and physical damage by individuals. In addition, the computer must be protected from unauthorized access, terminals must be inoperable when not attended by an authorized employee, and terminals utilized to enter sensitive commands must not be positioned where unauthorized individuals may view the contents of the video display terminal. Procedures must exist to assure sufficient computer processing capacity will continue to be available to process accounting information.

Logical Security

Access to information stored on the computer must be protected through the use of user identification codes and confidential passwords. These passwords must meet the following criteria:

Each user must have a unique user identification code and password.

Passwords must be changed every 30 days.

Passwords must be a minimum of six (6) characters in length.

Passwords must be a combination of alphabetic and numeric characters.

Passwords may not be the same for a user identification code as the last five (5) passwords used by this user identification code.

Individuals must assign their own passwords.

Passwords must be encrypted while stored on the computer.

User identification codes and passwords may not be shared.

Users other than System Administrators and Security Administrators must be prevented from accessing sensitive operating system commands.

Users must not be allowed to be active on multiple terminals at the same time with the same user identification code.

User identification codes must be deactivated after three unsuccessful attempts to sign on to the computer.

A display of the last attempted sign on for a user identification code must be displayed when a user signs on the computer.

For inactive terminals, the user must be automatically prevented from accessing the computer after 15 minutes of no activity until the user password is entered.

Users must be prevented from accessing operating system and computer program files.

Users must be prevented from accessing accounting information except through authorized transactions within the computerized accounting application system.

Reporting of security definitions and user access rights to information must be available and easily understood by Field Examiners during the course of a regularly scheduled audit. These security definitions and user access rights must enforce adequate segregation of duties for the accounting system. User access rights must be eliminated or revised upon termination of employment and transfers of employee responsibility.

Computerized audit trails must be protected from modification and destruction.

Change Controls

Computer programmers must not have access to production accounting information.

Accounting information must not be modified by computer utility programs which are not contained in the accounting application system.

Changes to the computer application system programs for the accounting systems must be adequately controlled including the following requirements:

> Computer source (human readable) and load (machine readable) modules must be stored in computer datasets protected from unauthorized modification.
>
> Modifications to computer source code must occur in a test environment and not affect production source code.
>
> All modifications to computer source code must be adequately tested. Modifications must be approved by management.
>
> Individuals responsible for modifying computer source code in a test environment must be prohibited from accessing computer code in the production environment. Movement of computer source and load modules from the test to production environments must be completed by authorized employees not responsible for modification of computer source or load modules.

Audit Trails

The computerized accounting system must maintain electronic audit trails sufficient to trace all transactions from original source of entry into the system, through all system processing, and to the results produced by the system. The audit trails must also maintain sufficient information to trace all transactions from the final results produced by the system, through all system processing, and to the original source of entry into the system. These audit trails must be protected from modification and deletion.

Input Controls

The computerized accounting system must provide input edits and controls to assure that information entered into the system is accurate, that all appropriate information is entered into the system, that information is entered into the system only once, and that all information entered into the system is authorized by management.

Output Controls

The computerized accounting system must incorporate features that assure all accounting information is reported accurately and completely. Procedures must also exist to assure that only authorized individuals have access to computer generated output. All receipts or payments generated by the accounting system must include unique document identification numbers preprinted on the form. If the application system prints other numbers on the form (document control numbers) adequate security must be implemented to prevent unauthorized modification of the number sequence. Individuals responsible for computer processing of receipts or payment documents must not have access to the storage locations of these documents. Receipt and payment documents must not include preprinted signatures. All output reports must clearly indicate the effective dates of the information regardless of when the report is generated. Output reports must have appropriate subtotals to allow reconcilement of reports within the system and reconcilement to external documentation.

Interface Controls

Information generated in one computer application system and transferred to another computer application system must be accurate and complete. The adequate transfer of information must be recorded on reports from both systems documenting the number of items of information transferred and the accounting value totals of the information transferred.

Internal Processing

During the course of a regularly scheduled audit, written verification procedures and actual verification results must be provided to the Field Examiners which document the verification of accurate calculating, summarizing, categorizing, and updating of accounting information on a periodic basis and after the modification of accounting system computer programs.

Error Correction

The accounting application system must be supported by computerized and manual procedures to assure the following controls related to error correction:

The type of error condition is recorded.

The original transaction creating the error is retained within the system.

A reversing transaction to eliminate the effect of the error on the appropriate value is entered and retained within the system.

The correct transaction is entered into the system and recorded.

The management approval for this error correction is documented.

Programming Documentation

During the course of a regularly scheduled audit, documentation must be available to the Field Examiners which provide adequate information on the functions performed by each computer program, the definitions of all computer files and records utilized by the computer programs, and a description of the computer processing which relates each computer program to other computer programs to accomplish accounting functions. The documentation must be adequate for the Field Examiners to determine the accuracy of accounting processes by the computer.

Operations Documentation

For each computerized accounting system, documentation must exist to record the processing of computer programs affecting accounting information. This documentation must include logs of when the programs were processed, errors which occurred during processing, error correction activities conducted prior to the continuation of processing, and the restart procedures for reinitiating processing. In addition, written documentation must be available to the Field Examiners during a regularly scheduled audit which provide the instructions to operate the computer hardware, operating system software, and application programs.

User Documentation

Written procedures must be available for all computerized accounting systems which provide instructions on the requirements for the approval of information prior to entry into the computer, as well as the accurate entry, processing, and reporting of information from the accounting system.

Computer Output

Records, financial statement information and supporting information generated through a computer system should be printed out on paper, printed to disk or maintained on-line at the end of each reporting year and retained for audit. Information must be maintained in a manner that will allow access for audit and public inquiry on equipment of the governmental unit.