Information Systems and Technology

As public servants, it is our responsibility to use taxpayers' dollars in the most effective and efficient way possible while adhering to laws and regulations governing those processes. There are many reasons to place controls in various points in these processes that may appear bureaucratic, but are necessary to ensure objectives are met and there is accountability to the citizens. This document does not address all possible circumstances that need to be considered when establishing internal controls or assessing risk. Each entity is responsible for reviewing its business practices and processes to determine where risks exist and where and how controls can be established to mitigate them.

Examples of the results of appropriate controls are as follows:

- Segregation of duties is maintained to the extent staffing constraints allow between the functions for information systems. Specifically, the use, data entry, computer operation, network management, system administration, systems development and maintenance, change management, security administration, and security audit are all properly segregated.
- Unauthorized personnel are prevented from accessing computer resources.
- Authentication and access mechanisms are in place (e.g. regular password changes).
- Operational security is periodically reviewed.
- Internal controls are established and periodically reviewed,
- Data is accurate, complete, and valid.
- Output is routinely reconciled to relevant internal system control totals.
- Audit trails are provided to facilitate the tracing of transaction processing.
- The logical and physical security of the organization's information assets is protected.
- Privacy and security of sensitive data is adequately addressed.
- User accounts are managed in a timely manner.
- Information systems are adequately protected from computer viruses and other system corrupting elements (such as spy-ware, ad-ware, Trojans, worms, etc.).

Control Objectives:

1. Proper design and use of information system documents and records is maintained.
2. Access to and use of the information system, assets and records are reasonable and restricted to authorized individuals.
3. Segregation of duties exists in functions related to the information systems.
4. Transactions and activities related to the information systems are properly authorized.
5. Performance of information system functions is independently verified.

Segregation of Duties:

Segregation of duties is one of the most important features of an internal control plan. The fundamental premise of segregated duties is that an individual or small group of individuals should not be in a position to initiate, approve, undertake, and review the same action. These are called incompatible duties when performed by the same individual.

Examples of incompatible duties include situations where the same individual (or small group of people) is responsible for:

- Managing both the operation of and record keeping for the same activity.
- Managing custodial activities and record keeping for the same assets.
- Authorizing transactions and managing the custody or disposal of the related assets or records.

Stated differently, there are four kinds of functional responsibilities that should be performed by different work units or, at a minimum, by different persons within the same unit:

1. Custody of assets involved: This duty refers to the actual physical possession or effective physical control over/safekeeping of property.

2. Recording transactions: This duty refers to the accounting or record keeping function, which in most organizations, is accomplished by entering data into a computer system.
3. Authorization to execute transactions: This duty belongs to persons with authority and responsibility to initiate and execute transactions.
4. Periodic reviews and reconciliation of existing assets to recorded amounts: This duty refers to making comparisons at regular intervals and taking action to resolve differences.

The advantage derived from proper segregation of duties is twofold:

- Fraud is more difficult to commit because it would require collusion of two or more persons and most people hesitate to seek the help of others to conduct wrongful acts.
- By handling different aspects of the transaction, innocent errors are more likely to be found and flagged for correction.

Example Financial Systems Aligned with IT and Business Strategies Questions:

A.		Yes	No	N/A	Comments
1.	Does the entity have an Information Technology/System strategy with respect to business systems?				
2.	Does the entity's strategy align with statewide IT/IS strategies with respect to business systems?				
3.	Is the entity familiar with statewide IT strategies and/or directives?				
4.	Is the entity aware of state laws, regulations or other pronouncements that apply to IT in relation to business systems?				
5.	Has the entity appointed someone (individual or office) who is responsible for compliance with IT in respect to business systems?				

B.	Organization of the entity IT Function:	Yes	No	N/A	Comments
1.	Is the IT function centralized?				
2.	Is someone in the IT organization responsible for business systems?				
3.	Have there been any significant personnel changes during the year that might affect the amount or quality of support for business systems?				
4.	Does the support of business systems involve external parties, such as outsourcing, vendors, or consultants?				
5.	Does the IT function have a uniform project management model that is followed for all projects, including acquisition of business system applications?				
6.	Do significant projects require a business benefit assessment?				
7.	Are the projects formally controlled against budgets, schedule and quality?				
8.	Do measures for quality exist?				
9.	Is the risk due to any significant business systems activities outside the IT function considered “low”?				
10.	Are subcontractors subject to program development and change control policies and procedures?				

Information Systems and Technology

C.	Effective Use of Technology:	Yes	No	N/A	Comments
1.	Does the entity have a strategy to update technology, including business systems, when needed?				
2.	Does the network and communication structure meet the entity's needs with respect to business systems?				
3.	Has management established a process to manage business systems changes?				
4.	Are policies and procedures to manage business system changes documented?				
5.	Does management monitor progress and ensure that approved changes are implemented on a timely basis?				
6.	Does IT management use reports/statistics to review the operational quality of the business systems?				
7.	Does IT accomplish the installation of infrastructure-related patches for hardware and software?				
8.	Is the risk of using any subcontractors considered “low”?				

D.	Staffing Levels:	Yes	No	N/A	Comments
1.	Is the number of IT staff in line with the entity's business systems requirements?				
2.	Is IT staff’s skill levels in line with the entity's business systems requirements?				
3.	Are the business systems owned and maintained by the users?				
4.	Do the users have the appropriate knowledge to exercise their ownership?				
5.	Is the reliance on key IT staff members or key users acceptable?				

E.	Alignment of Business Systems to Business Strategies and Objectives:	Yes	No	N/A	Comments
1.	Does the business system meet the needs of entity management?				
2.	Is the business system information for the entity accurate and useful?				
3.	Is the risk associated with the age of the business system considered “low”?				
4.	Is the risk associated with any needed business system upgrades or replacements in the near future considered “low”?				
5.	Is there a cost benefit for maintenance, staff, and support to keep the business applications going on a day-to-day basis?				
6.	Is the risk associated with agency reliance on vendors/contractors to perform maintenance considered “low”?				
7.	If vendors/contractors perform system maintenance, do they have sufficient knowledge to support the applications?				
8.	Does the business system provide for a proper audit trail?				

E.	Alignment of Business Systems to Business Strategies and Objectives:	Yes	No	N/A	Comments
9.	Is the risk associated with any business information demands that are not covered by the existing system considered “low”?				
10.	Are steps being taken to meet any unfulfilled demands?				

Example Personnel Policy Questions:

F.	IT Department:	Yes	No	N/A	Comments
1.	Are user profiles reviewed periodically to ensure they have the correct rights for their positions?				
2.	Do personnel policies include reference checks?				
3.	Do personnel policies include security statements?				
4.	Do personnel policies include rotation of duties?				
5.	Do personnel policies include terminated employee security measures?				

G.	Functions within the IT Department:	Yes	No	N/A	Comments
1.	Is system design segregated from operations?				
2.	Is application programming segregated from testing and ongoing operations?				
3.	Is systems programming (operating system/utilities) segregated?				
4.	Are quality assurance/testing segregated?				
5.	Is the approval of changes segregated?				
6.	Is the movement of changes into production segregated?				
7.	Is the computer operations/data input segregated?				

Example Procedural Controls Questions:

H.	Data Integrity Control Activities:	Yes	No	N/A	Comments
1.	Is IT staff prohibited from initiating transactions?				
2.	Are there controls to ensure all approved data is input?				
3.	Are there controls to ensure input is processed correctly through the system?				
4.	Are there controls to ensure duplicative data cannot be processed?				
5.	Are there audit trails tracing the computer output to data source and vice versa?				
6.	Are changes to master files approved by a supervisor in the user department and verified against a printout of changes?				
7.	Is there an audit trail for rejected and/or error transactions?				
8.	Are there processes that reconcile output totals to input totals for all data submitted as well as file balances?				
9.	Does someone review outputs for reasonableness?				
10.	Is there proper control of data between the user and the IT (operations) department?				
11.	Do application controls include editing and validation of input data?				

Information Systems and Technology

H.	Data Integrity Control Activities:	Yes	No	N/A	Comments
12.	Do application controls include data processing controls over rejected transactions?				
13.	Do application controls include balancing transaction and master files?				

Example Development / Implementation Controls Questions:

I.	Overall Control Activities:	Yes	No	N/A	Comments
1.	Are user control objectives clarified and defined within the initial requirements documentation?				
2.	Does the entity have a formal system development life cycle (SDLC) methodology that is followed?				
3.	Are users involved throughout the development life cycle?				
4.	Are application and control objectives clearly defined for new acquisition of purchased software?				
5.	Has a detailed project plan been developed?				
6.	Does the plan include goals and tasks?				
7.	Does the plan include timelines and milestones?				
8.	Does the plan include sponsor/stakeholder approval for each milestone?				
9.	Does the plan include projected roles, responsibilities, and resources?				
10.	Does the management receive project status reports on an ongoing basis?				
11.	Do the status reports include assessments of quality assurance review?				
12.	Do the status reports include actual completion of tasks against the plan?				
13.	Do the status reports include actual delivery dates against milestones and deadlines?				
14.	Has management determined and communicated a method to track costs that are eligible for capitalization under existing accounting standards?				
15.	Do the status reports include actual project costs against budgets?				
16.	Are users performing integration, acceptance, and data volume testing throughout the development life cycle?				

J.	Software Control Activities:	Yes	No	N/A	Comments
1.	If the entity purchases software from a vendor, is the placement of programs into production (loading the programs into the entity's computer system(s)) and changes to master files performed only by the entity (not the vendor)?				
2.	Do system policies and procedures require an up-to-date system flowchart/documentation for each application?				
3.	Are standard coding methodologies employed for internal development?				
4.	Does the entity require up-to-date program source code for each application?				
5.	Are users involved in development and acceptance testing?				

J.	Software Control Activities:	Yes	No	N/A	Comments
6.	Does the entity require up-to-date operator and user instructions for each application?				
7.	Do systems development policies require the active participation of users/stakeholders in important phases of the development or change, including final approval?				
8.	Does the application owner authorize acceptance and implementation of all application changes?				
9.	Are controls in place to prevent and/or detect changes in code after testing was completed but before going live?				
10.	Are procedures in place to ensure that configuration options and parameters meet business objectives and control requirements?				
11.	Do users control who can perform data entry and error correction?				
12.	Is process and data modeling performed?				
13.	Is the risk associated with any necessary data conversion considered “low”?				
14.	Are changes to the original design approved and controlled?				

Example Change Management Controls Questions:

K.	Control Activities Over Approval and Tracking of Change Requests:	Yes	No	N/A	Comments
1.	Are all requests for changes captured and managed centrally?				
2.	Are controls in place to log and track all requests?				
3.	Do changes reflect the priorities of business owners?				
4.	Is there ongoing communication between technical and business staff?				
5.	Are changes documented and approved before developers make program changes to any applications?				
6.	Is there a uniform systems development policy that is followed for all new programs?				
7.	Is business owner approval and acceptance testing required before a change is implemented?				
8.	Is there a uniform policy that is followed for all changes to existing programs to include up-to-date program modification documentation?				
9.	Do “emergency fixes” to a production system follow the same development, testing and approval process as other program changes?				
10.	Do change control processes ensure that superseded programs are segregated from the current version and removed from the production library?				
11.	Are tools used to ensure that all dependencies between integrated applications are identified and considered before changes are made?				

L.	Data Conversion:	Yes	No	N/A	Comments
1.	Are there procedures to ensure that the mapping of data fields from the legacy system to the target system is correct?				

L.	Data Conversion:	Yes	No	N/A	Comments
2.	Are there procedures to ensure the converted data is accurate?				
3.	Are there procedures to ensure the converted data is complete?				
4.	Are there procedures to ensure the converted data is accessible?				
5.	Are there procedures to ensure that critical system interfaces are modified to accept the new data model?				

M.	Testing and Quality Assurance:	Yes	No	N/A	Comments
1.	Are separate development, testing and production environments maintained?				
2.	Are users involved in the testing?				
3.	Do business owners authorize system acceptance?				
4.	Are code changes to production executed by staff other than those developing the software?				
5.	Are there processes in place to ensure that changes do not compromise security controls (e.g., checking software to ensure it does not contain malicious code, such as Trojans, Worms, or other viruses)?				
6.	Are there procedures in place to ensure that all changes have adequate backup and recovery procedures defined with management-approved escalation lists?				

N.	Going Live with System Changes:	Yes	No	N/A	Comments
1.	Are all changes approved migrated into the production environment?				
2.	If developers have “write” access to the production environment, does management have processes to ensure all changes are authorized?				
3.	Is formal approval from the project sponsor/owner and IT management required for authorizing the go-live decision?				
4.	Are quality assurance reviews required as part of the go-live decision making process?				
5.	Is there a go/no go-live checklist?				
6.	Is there a process to ensure that only the properly tested, reviewed, and approved version of the system is transferred to the live environment?				
7.	Is there a process to communicate the specifics of the go-live process?				
8.	Have individuals from both the business and IT organizations been designated to support the new system during the go-live period?				
9.	Is a post-implementation review planned?				

O.	Documentation and Training:	Yes	No	N/A	Comments
1.	Are user and technical documentation/procedures updated for all implemented system changes?				
2.	Are technical documentation/procedures updated when any changes to systems occur?				

O.	Documentation and Training:	Yes	No	N/A	Comments
3.	Have the users and computer operators received adequate training on new systems?				
4.	Is there a formal training program?				

Example Security Control Activities Questions:

P.	Security Organization and Management:	Yes	No	N/A	Comments
1.	Does the organization have an IT security coordinator?				
2.	Have user roles and responsibilities been clearly defined and communicated?				
3.	Have developer roles and responsibilities been clearly defined and communicated?				
4.	Have owner roles and responsibilities been clearly defined and communicated?				
5.	Is the business owner involved in the design of IT staff security access?				
6.	Are unsuccessful access attempts recorded?				
7.	Are unsuccessful access attempts reported?				
8.	Are unsuccessful access attempts monitored?				
9.	Is there a periodic review of security access?				

Q.	Security Policies and Procedures:	Yes	No	N/A	Comments
1.	Are there published policies and procedures that support the entities information integrity objectives?				
2.	Is there a controlled process to review and, if necessary, to update the security policy and procedure documentation (comprehensive security plan) on a periodic basis?				
3.	Is there a process to ensure that IT and business owners are aware of security policies and procedures, as well as their specific security responsibilities?				
4.	Have security policies relating to computer resources, passwords, etc. been communicated to employees including new hires?				
5.	Are all users required to authenticate with a personally identifiable username and password to access a workstation?				
6.	Are all computers configured to require a locking screen saver that activates when there is not more than 15 minutes of inactivity on the computer?				
7.	Is virus protection software installed and up to date on all computers?				
8.	Is adequately trained IT staff immediately alerted to virus events on computers?				
9.	Does all staff regularly attend security awareness training that covers topics such as password construction and management, web and email security, social engineering and networking, physical security, identity theft, data security, mobile device security, and reporting incidents?				
10.	Are all computers regularly patched for operating system security fixes and third party applications?				

Information Systems and Technology

Q.	Security Policies and Procedures:	Yes	No	N/A	Comments
11.	Are procedures in place for removing all system access when an employee leaves a unit?				
12.	Are non-IT support personnel denied administrative rights to their computer or other computers in the entity?				

R.	Security Over Applications:	Yes	No	N/A	Comments
1.	Is there a documented security administration process to ensure that all network and applications access is approved by management?				
2.	Is system access approved by the business owners?				
3.	Does the centralized security administration provide reports and require periodic reviews of user access by management to ensure that access is commensurate with current job responsibilities?				
4.	Are users required to have complex passwords for all systems?				
5.	Are users required to change their passwords at least every 90 days for all systems?				

S.	Security Over Sensitive and/or Critical Data:	Yes	No	N/A	Comments
1.	Are appropriate monitoring and audit trail controls in place for management to monitor for unauthorized activity?				
2.	Does management periodically review monitoring reports to identify potential unauthorized activity?				
3.	Has management complied with federal and state laws, regulations and rules regarding the privacy and confidentiality of financial data collected from customers, vendors, or employees?				

T.	Physical Environment and Access:	Yes	No	N/A	Comments
1.	Do procedures restrict physical access to computer facilities, including wiring closets, to authorized personnel?				
2.	Are PC systems with hard disks, in areas where they are accessible to the public, controlled/monitored when left unattended?				
3.	Are all laptop hard drives properly encrypted?				
4.	Are public use workstations restricted to read access only?				
5.	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)?				
6.	Are there controls on computer output that ensures only authorized users are receiving the data?				

U.	System Backup Procedures:	Yes	No	N/A	Comments
1.	Are data backup procedures documented and followed?				

Information Systems and Technology

U.	System Backup Procedures:	Yes	No	N/A	Comments
2.	Does the frequency of data backup procedures allow for the economic recovery of data lost due to intentional or accidental destruction?				
3.	Are backups created and saved daily?				
4.	Are backups created and saved weekly?				
5.	Are backups created and saved monthly?				
6.	Are backups created and saved yearly?				
7.	Are all backup data stored in a secured, fireproof vault or safe at an offsite location?				
8.	Are all backup data stored off site daily?				
9.	Is there a complete system backup done at month end?				
10.	Is there a complete system backup done at fiscal year end?				
11.	Are systems periodically restored from back-ups to confirm that the data and process are functional?				
12.	Are employees storing all critical files on network drives rather than workstation drives?				
13.	Are procedures established that requires all critical data to be maintained on devices and drives that are subject to data back-up and recovery policies and procedures?				

V.	Contingency Planning, Disaster Recovery (Restoring core systems):	Yes	No	N/A	Comments
1.	Is there a written disaster recovery plan (DR)?				
2.	Does the plan identify the critical applications?				
3.	Does the plan identify the critical staff responsibilities?				
4.	Does the plan identify steps for system recovery?				
5.	Does the plan identify computer equipment needed for temporary processing?				
6.	Does the plan identify business locations(s) that could be used to process critical applications in an emergency?				
7.	Is there a written agreement with other business locations(s)?				
8.	Does the plan identify the off-site location of the disaster recovery plan?				
9.	Does the plan identify the location and users authorized to access off-site system backups?				
10.	Does the plan identify all hardware and components (e.g. make, model numbers, serial numbers, etc.)?				
11.	Does the plan include an inventory of all software applications (e.g. operating system and software applications, release versions, and vendor names)?				
12.	Does the plan identify the location of all user documentation as well as system procedures manuals?				
13.	Does the plan identify the off-site location of extra stock, such as checks, warrants, purchase orders, etc.?				
14.	Are procedures for emergency purchases spelled out in the plan?				
15.	Does the entity have a Disaster Recovery site where a cold-back-up of software and data resides to ensure an appropriate recovery time (as defined in the plan)?				

V.	Contingency Planning, Disaster Recovery (Restoring core systems):	Yes	No	N/A	Comments
16.	Does the entity have a Disaster Recovery site where a warm-back-up of software and data resides to ensure an appropriate recovery time (as defined in the plan)?				
17.	Does the entity have a Disaster Recovery site where a hot-back-up of software and data resides to ensure an appropriate recovery time (as defined in the plan)?				
18.	Are all employees trained for appropriate responses to emergency situations?				
19.	Does the entity record retention policy require that records be retained for at least as long as they are needed to meet operational and legal requirements?				
20.	Is the plan reviewed and exercised regularly?				
21.	Is the plan updated with lessons learned from the reviews and exercises?				

W.	Contingency Planning, Business Continuity (Ongoing business operations):	Yes	No	N/A	Comments
1.	Is there a written business continuity plan (BCP)?				
2.	Does the BCP identify critical processes?				
3.	Does the BCP identify critical staff responsibilities?				
4.	Does the BCP identify business locations(s) that could be used to process critical applications in an emergency?				
5.	Is there a written agreement with other business location(s)?				
6.	Does the BCP identify the location of all user documentation?				
7.	Does the BCP identify the off-site location of extra stock, such as checks, warrants, purchase orders, etc.?				
8.	Are procedures for emergency purchases spelled out in the BCP?				
9.	Are all employees trained for appropriate responses to emergency situations?				
10.	Does the entity record retention policy require that records be retained for at least as long as they are needed to meet operational and legal requirements?				
11.	Is the plan reviewed and exercised regularly?				
12	Is the BCP updated with lessons learned from the exercises?				